

an American National Standard

ANSI/BICSI 002-2014

**Data Center Design and
Implementation Best Practices**



ANSI/BICSI 002-2014

Data Center Design and Implementation Best Practices

Committee Approval: November 2014

First Published: December 2014



BICSI International Standards

BICSI international standards contain information deemed to be of technical value to the industry and are published at the request of the originating committee. The BICSI International Standards Program subjects all of their draft standards to a rigorous public review and comment resolution process, which is a part of the full development and approval process for any BICSI international standard.

The BICSI International Standards Program reviews its standards at regular intervals. By the end of the fifth year after a standard's publication, the standard will be reaffirmed, rescinded, or revised according to the submitted updates and comments from all interested parties.

Suggestions for revision should be directed to the BICSI International Standards Program, care of BICSI.

Copyright

This BICSI document is a standard and is copyright protected. Except as permitted under the applicable laws of the user's country, neither this BICSI standard nor any extract from it may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, photocopying, recording or otherwise, without prior written permission from BICSI being secured.

Requests for permission to reproduce this document should be addressed to BICSI.

Reproduction may be subject to royalty payments or a licensing agreement.

Violators may be prosecuted.

Published by:



BICSI
8610 Hidden River Parkway
Tampa, FL 33637-1000 USA

All rights reserved
Printed in U.S.A.

Notice of Disclaimer and Limitation of Liability

BICSI standards and publications are designed to serve the public interest by offering information communication and technology systems design guidelines and best practices. Existence of such standards and publications shall not in any respect preclude any member or nonmember of BICSI from manufacturing or selling products not conforming to such standards and publications, nor shall the existence of such standards and publications preclude their voluntary use, whether the standard is to be used either domestically or internationally.

By publication of this standard, BICSI takes no position respecting the validity of any patent rights or copyrights asserted in connection with any item mentioned in this standard. Additionally, BICSI does not assume any liability to any patent owner, nor does it assume any obligation whatever to parties adopting the standard or publication. Users of this standard are expressly advised that determination of any such patent rights or copyrights, and the risk of infringement of such rights, are entirely their own responsibility.

This standard does not purport to address all safety issues or applicable regulatory requirements associated with its use. It is the responsibility of the user of this standard to review any existing codes and other regulations recognized by the national, regional, local, and other recognized authorities having jurisdiction (AHJ) in conjunction with the use of this standard. Where differences occur, those items listed within the codes or regulations of the AHJ supersede any requirement or recommendation of this standard.

All warranties, express or implied, are disclaimed, including without limitation, any and all warranties concerning the accuracy of the contents, its fitness or appropriateness for a particular purpose or use, its merchantability and its non-infringement of any third party's intellectual property rights. BICSI expressly disclaims any and all responsibilities for the accuracy of the contents and makes no representations or warranties regarding the content's compliance with any applicable statute, rule, or regulation.

BICSI shall not be liable for any and all damages, direct or indirect, arising from or relating to any use of the contents contained herein, including without limitation any and all indirect, special, incidental, or consequential damages (including damages for loss of business, loss of profits, litigation, or the like), whether based upon breach of contract, breach of warranty, tort (including negligence), product liability or otherwise, even if advised of the possibility of such damages. The foregoing negation of damages is a fundamental element of the use of the contents hereof, and these contents would not be published by BICSI without such limitations.

TABLE OF CONTENTS

PREFACE	xxvii
1 Introduction	1
1.1 General.....	1
1.2 Purpose	1
1.2.1 Users Within IT	1
1.2.2 Users Within Facilities Group	1
1.2.3 Staff Outside IT and Facilities Groups.....	2
1.3 Categories of Criteria	2
2 Scope	2
3 Required Standards and Documents.....	3
4 Definitions, Acronyms, Abbreviations, and Units of Measurement.....	7
4.1 Definitions.....	7
4.2 Acronyms and Abbreviations	25
4.3 Units of Measurement.....	27
5 Site Selection.....	29
5.1 Introduction.....	29
5.2 Site Evaluation	29
5.2.1 General Requirements	29
5.2.2 General Recommendations	29
5.2.3 Cost Evaluation Recommendations.....	29
5.2.4 Existing Facilities Requirements.....	30
5.3 Natural Hazards.....	30
5.3.1 Introduction	30
5.3.2 General Requirements	30
5.3.3 Seismic Activity	30
5.3.4 Volcanic Activity	32
5.3.5 Wildfire	32
5.3.6 Flood Plains.....	33
5.3.7 Wind.....	33
5.4 Natural Environment.....	34
5.4.1 Introduction	34
5.4.2 Ground Stability	34
5.4.3 Groundwater.....	35
5.4.4 Lightning.....	36
5.4.5 Air Quality	36
5.4.6 Noise	37
5.4.7 Other Topography and Natural Environment Recommendations	37
5.5 Man-Made Hazards.....	37
5.5.1 Introduction	37
5.5.2 Recommended Separation Distances	37
5.5.3 Other Recommendations	37

5.6	Site Access and Location	39
5.6.1	Public Road Access Recommendations	39
5.6.2	Adjacent Property	39
5.6.3	Proximity to Existing or Redundant Data Center.....	39
5.6.4	Security and Emergency Services	40
5.6.5	Proximity to Skilled Labor.....	40
5.7	Utility Services	40
5.7.1	Power and Electrical Service	40
5.7.2	Communications	43
5.7.3	Water Service.....	44
5.7.4	Sanitary Sewer	46
5.7.5	Natural Gas and Other Fuels	46
5.8	Regulations (Local, Regional, Country).....	47
5.8.1	Air Quality Requirements	47
5.8.2	Noise Requirements	47
5.8.3	Towers and Tall Structures Requirements	47
5.8.4	Fuel Tanks Requirements.....	47
5.8.5	Generator Requirements	47
5.8.6	Site Access and Required Parking	48
5.8.7	Setbacks and Sight Lines	48
5.8.8	Environmental Assessment	48
6	Space Planning.....	49
6.1	Overall Facility Capacity	49
6.1.1	General.....	49
6.1.2	Module and Modular Design	49
6.2	Power Systems.....	50
6.2.1	Introduction.....	50
6.2.2	Electric Utility Service Feeds.....	55
6.2.3	Generator Power	56
6.3	Cooling Capacity.....	57
6.3.1	Introduction.....	57
6.3.2	Recommendations	57
6.3.3	Additional Information	59
6.4	Data Center Supporting Spaces.....	59
6.4.1	Adjacencies of Functional Spaces.....	59
6.4.2	Security	61
6.4.3	Telecommunications Entrance Room	62
6.4.4	Command Center	63
6.4.5	Helpdesk	63
6.4.6	Print.....	63
6.4.7	Loading Dock.....	64
6.4.8	Storage	64
6.4.9	Engineering Offices	65
6.4.10	Administrative.....	65
6.4.11	Environmental Design.....	65
6.4.12	Waste/Recycle.....	65
6.5	Placement of Equipment When Using Access Floors	65
6.5.1	Cooling.....	66
6.5.2	Power Distribution.....	67
6.5.3	Fire Protection Systems	67

6.6	Information Technology Equipment Placement in a Computer Room With an Access Floor	67
6.6.1	Telecommunications Spaces	67
6.6.2	Racks, Frames, and Equipment	68
6.6.3	Aisles.....	71
6.6.4	Power and Telecommunications Cable Distribution	75
6.6.5	Airflow Circulation and Equipment Placement Coordination.....	76
6.6.6	Information Technology (IT) Equipment Adjacencies	76
6.6.7	Access Floor Grid Layout and Reference Point	76
6.7	Design For Efficiency	77
6.7.1	Holistic Energy Efficient Data Center Design	77
6.7.2	Data Center Efficiency Metrics	77
6.7.3	Data Center Energy Saving Design Opportunities	78
6.8	Network Architecture	79
6.8.1	Considerations	79
7	Architectural	81
7.1	Facilities Planning	81
7.1.1	General Overview	81
7.1.2	Site Selection.....	81
7.1.3	Location Within a Building.....	82
7.2	General Design Concepts	82
7.2.1	Levels of Reliability	82
7.2.2	Facility Purpose.....	82
7.2.3	Multiuser Versus Single User Groups.....	83
7.2.4	Equipment Change Cycle.....	83
7.2.5	Occupied Versus Unoccupied Data Centers.....	83
7.2.6	Data Center Location Within Building	83
7.2.7	Type of Building	84
7.2.8	Multitenant Buildings.....	84
7.2.9	24/7 Operation Of Data Center	84
7.2.10	Temperature And Relative Humidity Control	84
7.2.11	Materials.....	84
7.3	General Paths of Access.....	85
7.3.1	General Access.....	85
7.3.2	Data Center Access	85
7.3.3	Equipment Access.....	85
7.3.4	Telecommunications Access Provider Entry Into Computer Rooms	85
7.3.5	Vendor Access	86
7.3.6	Support Equipment Service Access	86
7.4	Planning Detail.....	86
7.4.1	Entry.....	86
7.4.2	Command center and Personnel Areas.....	86
7.4.3	Printer Room	86
7.4.4	Media Storage Room.....	86
7.4.5	Restrooms and Break Rooms	87
7.4.6	Computer Room	87
7.4.7	Entrance Rooms	87
7.4.8	Mechanical Equipment Space	87
7.4.9	Electrical Room and UPS Room	88
7.4.10	Battery Room	88
7.4.11	Fire Suppression Room	88
7.4.12	Circulation.....	89
7.4.13	Equipment Staging and Storage	89
7.4.14	Equipment Repair Room.....	89

7.5	Construction Components	89
7.5.1	Data Center Preparation	89
7.5.2	Floor Slab.....	89
7.5.3	Computer Room Envelope Wall Construction.....	90
7.5.4	Nonrated Partitions	90
7.5.5	Vapor/Moisture Seal	90
7.5.6	Door and Glazed Openings	90
7.5.7	Fire-Rated Construction	91
7.5.8	Access Control Systems.....	91
7.5.9	Airborne Particles	92
7.5.10	Access Flooring System.....	92
7.5.11	Ceilings	94
7.5.12	Equipment Bracing System.....	95
7.5.13	Computer Room Finishes.....	95
7.5.14	Roof Systems	95
8	Structural	97
8.1	Building Code Compliance and Coordination	97
8.1.1	Requirements	97
8.1.2	Additional Information	97
8.2	Impact of Site Location on Structural Loading	97
8.2.1	Introduction.....	97
8.2.2	Recommendations	97
8.3	Structural Concerns Specific to Data Center Design.....	97
8.3.1	Floor Load.....	97
8.3.2	Raised Access Floors	98
8.3.3	Mission Critical Equipment	98
8.3.4	Wind.....	99
8.3.5	Earthquake	99
8.3.6	Blast and Terrorist Attack	100
8.3.7	Ice Shard Impact	100
9	Electrical Systems	101
9.1	Overview.....	101
9.1.1	Introduction.....	101
9.1.2	Requirements	101
9.1.3	Availability and Uptime.....	102
9.1.4	Redundancy.....	102
9.1.5	Capacity Versus Utilization Efficiency.....	103
9.1.6	Electrical Class Ratings	104
9.2	Utility Service.....	117
9.2.1	Utility Service Planning.....	117
9.2.2	Low-Voltage Utility Services	118
9.2.3	Medium-Voltage and High-Voltage Utility Services.....	118
9.2.4	Protective Relaying.....	120
9.3	Distribution	120
9.3.1	Requirements	120
9.3.2	UPS Rectifier or Motor Inputs	120
9.3.3	Static Switch Bypass Inputs.....	120
9.3.4	UPS System Bypass.....	120
9.3.5	Power Strips.....	121
9.3.6	Input Source Transfer.....	121
9.3.7	Generator Controls and Paralleling	123
9.3.8	Unit Substations	123
9.3.9	UPS System	124

9.3.10	UPS Output Distribution	134
9.3.11	Power Distribution Units (PDUs).....	135
9.3.12	Automatic Static Transfer Switches	137
9.3.13	Direct Current (DC) Power Systems	139
9.3.14	Computer Room Equipment Power Distribution	142
9.3.15	Emergency Power Off (EPO) Systems	154
9.4	Mechanical Equipment Support.....	156
9.4.1	Introduction	156
9.4.2	Requirements	158
9.4.3	Recommendations	158
9.5	Uninterruptible Power Supply (UPS) Systems.....	159
9.5.1	Introduction	159
9.5.2	Sizing and Application	160
9.5.3	Technologies	162
9.5.4	Paralleling and Controls	164
9.5.5	Batteries and Stored Energy Systems.....	165
9.6	Standby and Emergency Power Systems	170
9.6.1	Sizing and Application	170
9.6.2	Starting Systems.....	172
9.6.3	Fuel System.....	172
9.6.4	Fuel Tank and Piping	173
9.6.5	Exhaust System	173
9.6.6	Cooling System	173
9.6.7	Mounting.....	174
9.7	Automation and Control	174
9.7.1	Introduction	174
9.7.2	Monitoring	174
9.7.3	Control	175
9.7.4	System Integration	175
9.8	Lighting.....	175
9.8.1	Introduction	175
9.8.2	General Recommendations	175
9.8.3	Computer Rooms	176
9.8.4	Support Areas.....	176
9.9	Bonding, Grounding, Lightning Protection, and Surge Suppression.....	177
9.9.1	Introduction	177
9.9.2	General Recommendations	181
9.9.3	Lightning Protection.....	182
9.9.4	Surge Suppression/Surge Protective Devices (SPDs)	183
9.9.5	Telecommunications Surge Protection.....	184
9.9.6	Building Ground (Electrode) Ring.....	185
9.9.7	Supplementary Bonding and Grounding	186
9.9.8	Information Technology Equipment Interconnections.....	191
9.9.9	Power System Bonding and Grounding	194
9.10	Labeling and Signage.....	200
9.10.1	Introduction	200
9.10.2	Requirements	200
9.10.3	Recommendations	200
9.11	Testing and Quality Assurance.....	201
9.11.1	Requirements	201
9.11.2	Recommendations	201
9.12	Ongoing Operations.....	202
9.12.1	Recommendations	202
9.13	Electrical Systems Matrix	202

10	Mechanical	221
10.1	Codes, References, and Terminology	221
10.1.1	Code Compliance and Coordination	221
10.1.2	References	221
10.1.3	Terminology Differences Between Codes and Telecommunications Standards	221
10.2	Typical Heat Rejection and Computer Room Cooling Technologies	221
10.2.1	Introduction	221
10.2.2	Chiller Based Systems	221
10.2.3	Direct Expansion Cooling Systems	229
10.2.4	Dual Coil Cooling Solution	232
10.3	Mechanical Class Ratings	232
10.3.1	Introduction	232
10.3.2	Class F0 and F1 Description	232
10.3.3	Class F2 Description	234
10.3.4	Class F3 Description	236
10.3.5	Class F4 Description	239
10.3.6	Chiller Piping and Valve Redundancy	242
10.4	Environmental Conditions	243
10.4.1	Introduction	243
10.4.2	Normal Operation Versus Loss of Environmental Control	243
10.4.3	Environmental Class Definitions	243
10.4.4	Air Conditioning	245
10.4.5	Ventilation (Outside Air)	246
10.4.6	Airborne Contaminants (Gases and Particles)	247
10.4.7	Environmental Limits	247
10.4.8	Humidity Control	248
10.4.9	Temperature And Humidity Control—Tape Media	248
10.4.10	Maximum Dew Point	248
10.4.11	Altitude	248
10.4.12	Noise Levels	248
10.4.13	Leak Detection	248
10.5	Thermal Management	249
10.5.1	Introduction	249
10.5.2	Use Of Operating Rather Than Nameplate Load	249
10.5.3	Current Equipment Heat Release and Trends	250
10.5.4	Equipment Heat Release Specifications	250
10.5.5	Electronic Equipment Cooling	250
10.5.6	Humidification and Dehumidification Equipment	250
10.5.7	Air-side Economizer Systems	251
10.5.8	Supplemental Cooling	251
10.6	Computer Room Cooling	252
10.6.1	General Considerations	252
10.6.2	Access Floor Versus No Access Floor	252
10.6.3	Hot Aisle/Cold Aisle Concept	253
10.6.4	Access Floor	254
10.6.5	Overhead Air Distribution	255
10.6.6	Row-Integrated Cooling	255
10.6.7	Equipment Layout	255
10.6.8	Supply Air Layout	255
10.6.9	Return Air Layout	256
10.6.10	Cable Management	256

10.7	Mechanical Equipment (Design and Operation).....	256
10.7.1	General Recommendations	256
10.7.2	Computer Room Air Conditioning (CRAC) Units.....	257
10.7.3	Central Air Handlers	257
10.7.4	Supplemental Cooling Systems.....	257
10.7.5	Chilled Water Systems.....	258
10.7.6	Chillers	258
10.7.7	Cooling Towers.....	258
10.7.8	Thermal Storage	258
10.7.9	Piping And Pumps.....	259
10.7.10	Plumbing.....	259
10.8	Materials and Finishes.....	259
10.8.1	Introduction.....	259
10.8.2	Materials in Air Plenums.....	259
11	Fire Protection.....	261
11.1	Introduction.....	261
11.2	Basic Design Elements	261
11.3	General Requirements and Recommendations	261
11.3.1	Requirements	261
11.3.2	Recommendations	261
11.4	Walls, Floors, and Ceilings.....	262
11.4.1	Requirements	262
11.5	Aisle Containment.....	262
11.5.1	Introduction	262
11.5.2	Aisle Containment Construction and Materials	262
11.5.3	Detection Systems In Contained Spaces	263
11.5.4	Suppression Systems In Contained Spaces	263
11.5.5	Additional Information.....	264
11.6	Handheld Fire Extinguishers	265
11.6.1	Requirements	265
11.6.2	Recommendations	265
11.7	Fire Protection.....	265
11.7.1	Water Sprinkler System	265
11.7.2	Gaseous Fire Suppression	267
11.8	Fire Detection	268
11.8.1	Area Requirements.....	268
11.8.2	Detector Technology.....	268
11.8.3	Early Warning Detection Systems	269
11.9	Labeling and Signage.....	270
11.9.1	Requirements	270
11.9.2	Recommendations	270
11.10	Testing and Quality Assurance.....	270
11.10.1	Requirements	270
11.10.2	Recommendations	270
11.11	Ongoing Operations.....	270
11.11.1	Requirements	270
11.11.2	Recommendations	270
12	Security.....	271
12.1	General.....	271
12.1.1	Introduction	271
12.1.2	Requirements	271

12.2	Physical Security Plan	271
12.2.1	Recommendations	271
12.2.2	Additional Information	271
12.3	Risk and Threat Assessment	272
12.3.1	Definitions	272
12.3.2	Recommendations	272
12.4	Regulatory and Insurance Requirements	273
12.4.1	Recommendations	273
12.4.2	Additional Information	273
12.5	Data Center Security Plan	273
12.5.1	Recommendations	273
12.6	Crime Prevention Through Environment Design	278
12.6.1	Recommendations	278
12.7	Access Control	280
12.7.1	Requirements	280
12.7.2	Recommendations	280
12.8	Alarms	287
12.8.1	Introduction	287
12.8.2	Recommendations	287
12.9	Surveillance	289
12.9.1	Introduction	289
12.9.2	Recommendations	289
12.10	Barriers	291
12.10.1	Definitions	291
12.10.2	Introduction	292
12.10.3	Vehicle Barriers	293
12.10.4	Building Exteriors	294
12.10.5	Concrete Walls	294
12.10.6	Building Openings	295
12.10.7	Glazing	296
12.10.8	Fences and Metal Barriers	299
12.10.9	Metal and Welded Wire Barriers	300
12.10.10	Gates	301
12.11	Lighting	301
12.11.1	Introduction	301
12.12	Guards	302
12.12.1	Introduction	302
12.12.2	Recommendations	302
12.13	Disaster Recovery Plan	302
12.13.1	Introduction	302
12.13.2	Requirements	302
12.13.3	Recommendations	302
12.14	Building Site Considerations	304
12.14.1	Introduction	304
12.14.2	General Recommendations	304
12.14.3	Lighting	305
12.14.4	Perimeter Fencing and Barriers	305
12.14.5	Automotive Threats and Concerns	306
12.14.6	Threat History	307
12.14.7	Natural Threats and Concerns	307
12.14.8	Chemical, Biological, Radiological, Nuclear, and Explosives	307
12.14.9	Medical Disasters and Epidemics	308

12.15	Building Shell	308
12.15.1	General Recommendations	308
12.15.2	Doorways And Windows	308
12.15.3	Signage and Displays	309
12.15.4	Construction	309
12.15.5	Elevators.....	309
12.15.6	Emergency Exits	309
12.15.7	Utilities.....	309
12.15.8	Hazardous Material Storage	309
12.16	Data Center Security Design Recommendations.....	309
12.16.1	Site, Personnel, and Non-Critical Areas.....	309
12.16.2	Computer Room and Critical Facility Areas Special Considerations	311
13	Data Center Management and Building Systems.....	315
13.1	Data Center Infrastructure Management.....	315
13.1.1	Introduction	315
13.1.2	Components	315
13.1.3	Communication Protocols, Media and Hardware.....	317
13.1.4	Reporting.....	317
13.1.5	Recommendations and Conclusion	317
13.2	Building Automation Systems.....	318
13.2.1	Introduction	318
13.2.2	Components	318
13.2.3	Cabling Design Considerations	320
13.3	Electronic Safety and Security Systems	322
13.3.1	Introduction	322
13.3.2	Cabling Infrastructure	322
14	Telecommunications Cabling, Infrastructure, Pathways and Spaces	323
14.1	Introduction.....	323
14.2	Telecommunications Cabling Infrastructure Classes	323
14.2.1	Introduction	323
14.2.2	Class C0 and C1 Telecommunications Infrastructure	324
14.2.3	Class C2 Telecommunications Infrastructure	324
14.2.4	Class C3 Telecommunications Infrastructure	327
14.2.5	Class C4 Telecommunications Infrastructure	327
14.3	Cabling Topology.....	330
14.3.1	Introduction	330
14.3.2	Horizontal Cabling Topology.....	330
14.3.3	Backbone Cabling Topology.....	330
14.3.4	Accommodation of Non-Star Configurations	330
14.3.5	Redundant Cabling Topologies	330
14.4	Data Center Spaces for Telecommunications.....	332
14.4.1	Introduction	332
14.4.2	Design and Structural Requirements	332
14.4.3	Entrance Rooms	332
14.4.4	Main Distribution Area (MDA)	333
14.4.5	Intermediate Distribution Area (IDA).....	334
14.4.6	Horizontal Distribution Area (HDA)	334
14.4.7	Zone Distribution Area (ZDA).....	334
14.4.8	Equipment Distribution Area (EDA)	335
14.5	Outside Plant Cabling Infrastructure	335
14.5.1	Underground Service Pathways	335
14.5.2	Aerial Service Pathways.....	336

14.6	Access Providers	336
14.6.1	Access Provider Coordination.....	336
14.6.2	Redundancy.....	337
14.6.3	Access Provider Demarcation	337
14.7	Telecommunications Cabling Pathways	341
14.7.1	General.....	341
14.7.2	Security	342
14.7.3	Separation of Power and Telecommunications Cabling	342
14.7.4	Cable Tray Support Systems	343
14.8	Backbone Cabling.....	345
14.8.1	Introduction.....	345
14.8.2	General Requirements	345
14.8.3	General Recommendations	345
14.8.4	Cabling Types	345
14.8.5	Redundant Backbone Cabling.....	346
14.8.6	Backbone Cabling Length Limitations	346
14.8.7	Centralized Optical Fiber Cabling	347
14.9	Horizontal Cabling	348
14.9.1	Introduction.....	348
14.9.2	Cabling Types	348
14.9.3	Redundant Horizontal Cabling.....	349
14.9.4	Balanced Twisted-Pair Cabling.....	349
14.9.5	Optical Fiber Cabling.....	349
14.9.6	Shared Sheath Guidelines	352
14.9.7	Horizontal Cabling Length Limitations	353
14.10	Cabling Installation	354
14.10.1	General Requirements	354
14.10.2	Cable Management	354
14.10.3	Bend Radius and Pulling Tension Guidelines	356
14.10.4	Abandoned Cable	356
14.11	Field Testing Data Center Telecommunications Cabling.....	357
14.11.1	Introduction.....	357
14.11.2	Installation Conformance	358
14.11.3	100-ohm Balanced Twisted-Pair Cabling Field Testing	358
14.11.4	Optical Fiber Cabling Field Testing.....	361
14.12	Telecommunications and Computer Cabinets and Racks.....	365
14.12.1	Requirements and Recommendations	365
14.12.2	Cabinet and Rack Configurations	366
14.12.3	Cabinet Airflow and Cabling Capacity	368
14.12.4	Cabinet and Rack Installations.....	375
14.12.5	Thermal Management in Cabinets	379
14.13	Telecommunications Cabling, Pathways, and Spaces Administration	380
14.13.1	General.....	380
14.13.2	Identification Conventions for Data Center Components	381
14.13.3	Intelligent Infrastructure Management	385
15	Information Technology	387
15.1	Disaster Recovery	387
15.1.1	Introduction.....	387
15.1.2	Offsite Data Storage.....	387
15.1.3	Colocation Facility.....	387
15.1.4	Onsite Data Center Redundancy	388
15.1.5	HVAC Failure	388
15.1.6	Power Failure	388
15.1.7	Mirroring.....	388

15.1.8	Location of Real-Time Redundant Storage Device.....	389
15.1.9	Physical Connectivity Methods and Devices	389
15.1.10	RAID	389
15.1.11	Distance Between Data Centers	389
15.2	Channel and Console Cabling.....	390
15.2.1	Introduction	390
15.2.2	Mainframe Channel Cabling	390
15.3	Communications	392
15.3.1	Wired/Wireless/Hands-Free Voice Communications	392
15.3.2	Wireless Network for Portable Maintenance Equipment	394
15.3.3	Zone Paging	394
15.4	Computer Room Layout.....	394
15.4.1	Introduction	394
15.4.2	Equipment Configuration for Efficiency	394
15.4.3	Connectivity Panel Distribution	394
15.4.4	Aisle Sizing and Workflow Analyses for Proper Walkways and Egress Pathways	397
15.5	Operations Center.....	397
15.5.1	Monitoring of Building Systems	397
15.5.2	Location	397
15.6	Network Infrastructure Reliability	397
15.6.1	Overview	397
15.6.2	Network Infrastructure Availability Classes	398
15.7	Network Security for Facility and IT Networks.....	404
15.7.1	Overview	404
15.7.2	Requirements	404
15.7.3	Recommendations	404
15.7.4	Additional Information.....	404
16	Commissioning	407
16.1	General.....	407
16.1.1	Introduction	407
16.1.2	Recommendations	407
16.2	Phases of the Commissioning Process	407
16.2.1	Overview	407
16.2.2	Program Phase.....	408
16.2.3	Design Phase	408
16.2.4	Construction Phase.....	408
16.2.5	Acceptance Phase.....	408
16.2.6	Post-Acceptance Phase.....	409
16.3	Types of Commissioning.....	409
16.3.1	New Building	409
16.3.2	Existing Building	409
16.4	Testing.....	410
16.4.1	Introduction	410
16.4.2	Functional Testing Components.....	410
16.4.3	Functional Testing Procedures	410
16.4.4	Testing Equipment	410
16.4.5	System Testing.....	410
16.4.6	Acceptance Testing	411
16.4.7	Electrical System Testing Example.....	412

16.5	Commissioning Documents	412
16.5.1	Introduction	412
16.5.2	Design Documents	412
16.5.3	Process Documents	413
16.5.4	Verification Documents	413
16.5.5	Operation and Maintenance Documents	413
16.6	System Training for Client Staff	413
16.6.1	Recommendations	413
16.7	Final Commissioning Report	414
17	Data Center Maintenance	415
17.1	Introduction	415
17.2	System Maintenance General Requirements and Recommendations	415
17.2.1	Requirements	415
17.2.2	Recommendations	415
17.3	Maintenance Plans	416
17.3.1	Recommendations	416
17.4	Cabling Systems Maintenance	417
17.4.1	Introduction	417
17.4.2	Recommendations	417
17.5	Electrical Systems Maintenance	417
17.5.1	Introduction	417
17.5.2	Requirements	418
17.5.3	General Recommendations	418
17.5.4	Battery Recommendations	418
17.5.5	Additional Information	420
17.6	HVAC Systems Maintenance	420
17.6.1	Introduction	420
17.6.2	Recommendations	420
17.7	IT and Telecommunications Systems Maintenance	421
17.7.1	Introduction	421
17.7.2	Recommendations	423
17.8	Access Floor System Maintenance	423
17.8.1	Introduction	423
17.8.2	Recommendations	424
17.9	Fire Protection and Suppression System Maintenance	431
17.9.1	Introduction	431
17.9.2	Recommendations	431
17.10	Security Systems Maintenance	431
17.10.1	Introduction	431
17.10.2	Recommendations	431
17.11	Monitoring and Management Systems Maintenance	432
17.11.1	Overview	432
17.11.2	Recommendations	432
17.12	Maintenance Recordkeeping	432
17.12.1	Recommendations	432
17.13	Service Contracts	432
17.13.1	Recommendations	432
17.13.2	Example ESS Service Contract Provisions	433

Appendix A	Design Process (Informative)	435
A.1	Introduction.....	435
A.2	Project Delivery Methods.....	437
A.3	Facility Design Phases.....	438
A.4	Technology Design Phases.....	440
A.5	Commissioning	441
A.6	Data Center Documentation	441
Appendix B	Reliability and Availability (Informative)	443
B.1	Introduction.....	443
B.2	Creating Mission-Critical Data Centers Overview	444
B.3	Risk Analysis	445
B.4	Availability	445
B.5	Determining the Data Center Availability Class.....	446
B.6	Data Center Availability Classes	449
B.7	Availability Class Sub Groups	452
B.8	Reliability Aspects of Availability Planning	453
B.9	Other Factors	454
B.10	Other Reliability Alternatives.....	455
B.11	Reliability Planning Worksheet.....	455
Appendix C	Alignment of Data Center Services Reliability with Application and System Architecture (Informative)	459
C.1	Overview.....	459
C.2	Application Reliability.....	459
C.3	Data Processing and Storage Systems Reliability	463
Appendix D	Data Center Services Outsourcing Models (Informative)	469
D.1	Data Center Services Outsourcing Models.....	469
D.2	Data Center Services Outsourcing Model Comparison.....	469
D.3	Public Cloud Services	470
D.4	Outsourcing Model Decision Tree.....	471
Appendix E	Multi-Data Center Architecture (Informative)	473
E.1	Overview.....	473
E.2	High Availability In-House Multi-Data Center Architecture Example	474
E.3	Private Cloud Multi-Data Center Architecture Examples.....	475
Appendix F	Examples of Testing Documentation (Informative)	477
F.1	Introduction.....	477
F.2	Example of PDU Testing	477
F.3	Example of UPS and Diesel Generator Testing.....	482
Appendix G	Design for Energy Efficiency (Informative)	497
G.1	Introduction.....	497
G.2	Design for Efficiency.....	498
G.3	Efficiency Content of BICSI 002-2014	499
Appendix H	Related Documents (Informative)	501

This page intentionally left blank

INDEX OF FIGURES

Section 5	Site Selection	
Figure 5-1	Global Seismic Hazard Map	31
Figure 5-2	Example Volcano Hazard Map.....	32
Figure 5-3	Global Flooding Hazard.....	33
Figure 5-4	Global Tornado Risk Areas	34
Figure 5-5	Example Ground Permeability Chart.....	35
Figure 5-6	Example Map of Lightning Flash Data.....	36
Figure 5-7	AC Electricity Distribution from Generation Stations to Data Centers	41
Section 6	Space Planning	
Figure 6-1	Example Module Size Decision Tree	51
Figure 6-2	Space Adjacencies of a Traditional Data Center	60
Figure 6-3	Space Adjacencies of Modular or Containerized Data Centers	61
Figure 6-4	Example of Aisle Width With Different Cabinet Sizes	73
Section 9	Electrical Systems	
Figure 9-1	Class F0 Electrical Concept Diagram (Configuration Without Backup/Alternate Power)	106
Figure 9-2	Class F1 Electrical Concept Diagram	107
Figure 9-3	Class F2 Concept Diagram	108
Figure 9-4	Class F3 Single Utility Source with Two Utility Inputs	109
Figure 9-5	Class F3 Single Utility Source with Single Utility Input.....	110
Figure 9-6	Class F4 Electrical Topology (System-Plus-System)	112
Figure 9-7	Class F4 Electrical Topology (xN Or Distributed Redundant)	113
Figure 9-8	Class F3 Single Utility Source with Two Utility Inputs “Catcher” System.....	115
Figure 9-9	Class F4 2(N+1) Electrical Topology with Dual Utility Inputs	116
Figure 9-10	Example of a Power Strip for Mounting in ITE Cabinets.....	121
Figure 9-11	Example ATS Sizes and Locations.....	122
Figure 9-12	Single-Module UPS with Internal Static Bypass and Maintenance Bypass from the Same Source	125
Figure 9-13	Single-Module UPS with Inputs to Rectifier, Static Bypass, and Maintenance Bypass from the Same Source	126
Figure 9-14	Multiple-Module UPS with Inputs to Rectifier and Maintenance Bypass from Same Source – Centralized Static Bypass	127
Figure 9-15	Multiple-Module UPS with Inputs to Rectifier and Maintenance Bypass from Same Source – Paralleled Installation	128
Figure 9-16	Single-Module UPS Bypass – Alternate Bypass Source - Input to Rectifier from Primary Source; Inputs to Static Bypass and Maintenance Bypass from a Second Source.....	129
Figure 9-17	Multiple-Module UPS Bypass – Alternate Bypass Sources - Inputs to Rectifiers from Primary Source; Inputs to Static Bypass and Maintenance Bypass from a Second Source	130
Figure 9-18	Single-Module UPS Bypass – Multiple Bypass Sources - Inputs to Rectifier and Static Bypass from Primary Source, and Input to Maintenance Bypass from a Second Source.....	131
Figure 9-19	Multiple-Module UPS Bypass – Multiple Bypass Sources - Inputs to Rectifiers and Static Bypass from Primary Source, and Input to Maintenance Bypass from a Second Source.....	131
Figure 9-20	Topology Inside an UPS Unit (Ref Figures	132

Figure 9-21	An Example of an Approach to UPS Output Switchboard Load Management	136
Figure 9-22	PDU Configuration: Single-Corded and Poly-Corded Devices	137
Figure 9-23	Automatic Static Transfer Switches	138
Figure 9-24	System Capacities at Various Stages of the Electrical Distribution System	145
Figure 9-25	Class F0 and F1 Circuit Mapping	146
Figure 9-26	Class F2 Circuit Mapping	147
Figure 9-27	Class F3 Circuit Mapping (Manual Operations)	149
Figure 9-28	Class F3 Circuit Mapping (Automated Operations)	150
Figure 9-29	Class F4 Circuit Mapping	151
Figure 9-30	Class F3 50 to 600 V _{DC} Circuit Mapping	152
Figure 9-31	Class F4 50 to 600 V _{DC} Circuit Mapping	153
Figure 9-32	EPO System	155
Figure 9-33	Sample Power Circuits For a Class F3 Mechanical System	157
Figure 9-34	Sample Power Circuits For a Class F4 Mechanical System	157
Figure 9-35	Example Critical Facility Bonding and Grounding Diagram for Class F2 and Lower	178
Figure 9-36	Example Critical Facility Bonding and Grounding Diagram For Class F3	179
Figure 9-37	Example Class F4 Bonding and Grounding Diagram (Two MGB and Two Entrance Facilities)	180
Figure 9-38	Typical Data Center Grounding Schema (shown with raised floor)	187
Figure 9-39	Typical Configuration of Flat Strip-Type SBG Within a Mesh-BN	188
Figure 9-40	Adjacent Rolls Of Flat-Strip-Type SBG Being Exothermically-Welded Together	189
Figure 9-41	Data Center Grounding Infrastructure (Room Level) Example	189
Figure 9-42	Examples of a Rack Bonding Conductor and Rack Grounding Busbar Mounting	192
Figure 9-43	Example of Bonding of Cabinet Side Panel and Door	193
Figure 9-44	Telecommunications Bonding and Grounding Infrastructure	195
Figure 9-45	Similarity of Recommended Grounding for AC and DC Power Systems and Load Equipment	197
Figure 9-46	DC Power System Showing a Single-Point Grounded Return	197
Figure 9-47	Information Technology Equipment Showing Grounding of DC Power Input (Return Is Insulated)	198
Figure 9-48	Common Bonding Network	198
Figure 9-49	Isolated (Insulated) Bonding Network	199
Figure 9-50	Sample Equipment Nameplate	201
Figure 9-51	Arc Flash Warning Label	201
Section 10	Mechanical	
Figure 10-1	Evaporative Condenser Heat Rejection System	222
Figure 10-2	Air-Cooled Condenser Heat Rejection System	223
Figure 10-3	Air-Cooled Chiller Heat Rejection System	224
Figure 10-4	Computer Room Air Handler Cooling System	225
Figure 10-5	Liquid Cooling ITE Cooling System	226
Figure 10-6	Closed Cabinet Cooling System	227
Figure 10-7	Row Integrated Cooling Systems	228
Figure 10-8	Direct Expansion Computer Room Air Handler Cooling System	229
Figure 10-9	Direct Expansion Integrated Cooling System	230
Figure 10-10	Direct Expansion Closed Cabinet Cooling System	231

Figure 10-11	Class F0 and F1 Chiller System Example.....	233
Figure 10-12	Class F0 and F1 Direct Expansion System Example.....	234
Figure 10-13	Class F2 Chiller System Example.....	235
Figure 10-14	Class F2 Direct Expansion System Example.....	236
Figure 10-15	Class F3 Direct Expansion System Example.....	237
Figure 10-16	Class F3 Chiller System Example.....	238
Figure 10-17	Class F4 Chiller System Example.....	240
Figure 10-18	Valve Configuration Example for Pumps in Class F4 System (Figure 10-17).....	241
Figure 10-19	Class F4 Direct Expansion System Example.....	241
Figure 10-20	Class F3 Piping and Valve Redundancy Example.....	242
Figure 10-21	Class F4 Piping and Valve Redundancy Example.....	244
Section 11	Fire Protection	
Figure 11-1	Variations of Air Flow in a Data Center with Aisle Containment.....	264
Section 12	Security	
Figure 12-1	Security Measures.....	271
Figure 12-2	Example of a Visually Distinctive Expired Badge	287
Figure 12-3	Security Layers	292
Section 13	Data Center Management and Building Systems	
Figure 13-1	Example DCIM Architecture.....	316
Section 14	Telecommunications Cabling, Infrastructure, Pathways and Spaces	
Figure 14-1	Class C0 and C1 Concept Diagram	325
Figure 14-2	Class C2 Concept Diagram.....	326
Figure 14-3	Class C3 Concept Diagram.....	328
Figure 14-4	Class C4 Concept Diagram.....	329
Figure 14-5	Data Center Cabling Topology Example	331
Figure 14-6	Cross-Connection Circuits to IDC Connecting Hardware Cabled to Modular Jacks in the T568A 8-Pin Sequence	338
Figure 14-7	Cross-Connection Circuits to IDC Connecting Hardware Cabled to Modular Jacks in the T568B 8-Pin Sequence	338
Figure 14-8	Centralized Optical Fiber Cabling Example	347
Figure 14-9	Permanent Link Example.....	359
Figure 14-10	Channel Model Example	359
Figure 14-11	Blank Panels Installed in Empty RUs	367
Figure 14-12	Cabinet Aperture Opening.....	369
Figure 14-13	Illustration of Components for Cable Capacity Formulae	370
Figure 14-14	Cabinets Are Identified and Labeled	375
Figure 14-15	Example of Labeled Termination Ports and Equipment Cords.....	375
Figure 14-16	Effect Of Internal Hot Air Recirculation	376
Figure 14-17	How Reducing Internal Hot Air Recirculation Reduces Input Air Temperature.....	376
Figure 14-18	Gasket Seals Off Access Floor Tile Cutout In Vertical Cable Manager.....	377
Figure 14-19	Brush Grommet Seals Access Floor Tile Cutout	377
Figure 14-20	Illustration of Securing Cabinets and Racks on an Access Floor to a Concrete Slab Using Threaded Rod and Steel Channel.....	378
Figure 14-21	Hot Aisle/Cold Aisle Cabinet Layout	379

Figure 14-22	Room Grid Coordinate System Example.....	382
Figure 14-23	Intelligent Infrastructure Management Interconnection Configuration Example	386
Figure 14-24	Intelligent Infrastructure Management Cross-Connection Configuration Example	386
Section 15	Information Technology	
Figure 15-1	No Radio Zone Around Suppression Tank Room	393
Figure 15-2	Simple Connection Topology	395
Figure 15-3	Sample Zone Distribution Topology	396
Figure 15-4	Sample Redundant Topology	396
Figure 15-5	Class N0 and N1 Network Infrastructure	399
Figure 15-6	Class N2 Network Infrastructure	400
Figure 15-7	Class N3 Network Infrastructure	402
Figure 15-8	Class N4 Network Infrastructure	403
Figure 15-9	Example of Facility & IT Network Topology	405
Section 17	Data Center Maintenance	
Figure 17-1	One Rack Unit (1 RU) 48 Port Ethernet Switch	422
Figure 17-2	Twenty Rack Unit (20 RU) Network Switch Chassis with Installed Switches	422
Appendix A	Design Process (Informative)Space Planning	
Figure A-1	Traditional A/E Design Process.....	435
Figure A-2	Data Center A/E Design Process	436
Appendix B	Reliability and Availability (Informative)	
Figure B-1	Planning Process for a Mission-Critical Facility	444
Figure B-2	Relationship of Factors in Data Center Services Availability Class.....	447
Figure B-3	Sample Reliability Calculation	453
Figure B-4	Continuous Improvement Cycle	454
Appendix C	Alignment of Data Center Services Reliability with Application and System Architecture (Informative)	
Figure C-1	Class A0 and A1 Application Architecture	460
Figure C-2	Class A2 Application Architecture	461
Figure C-3	Class A3 and A4 Application Architecture	462
Figure C-4	Class S0 and S1 Systems Architecture	464
Figure C-5	Class S2 Systems Architecture	465
Figure C-6	Class S3 Systems Architecture	466
Figure C-7	Class S4 Systems Architecture	467
Appendix D	Data Center Services Outsourcing Models (Informative)	
Figure D-1	Outsourcing Model Matrix	470
Figure D-2	Outsourcing Decision Tree.....	472

Appendix E Multi-Data Center Architecture (Informative)

Figure E-1	Reliability Framework Across All Service Layers	473
Figure E-2	Multi-Data Center Class 3 Example	474
Figure E-3	Multi-Data Center Class 3 Example With Three Class 2 Facilities	475
Figure E-4	Multi-Data Center Class 4 Example with Four Class 2 Facilities.....	476

Appendix G Design for Energy Efficiency (Informative)

Figure G-1	Data Center Electricity Utilization.....	497

This page intentionally left blank

INDEX OF TABLES

Section 5	Site Selection	
Table 5-1	Recommended Distances from Man-Made Elements	38
Table 5-2	Utility Reliability Examples	42
Table 5-3	Recommended On-Site Supply of Services for Data Center Facility Classes	46
Section 6	Space Planning	
Table 6-1	Example of a Module Size Design Checklist.....	52
Table 6-2	Liquid and Air-Cooled System Options and Primary Design Parameters	58
Table 6-3	Data Center Energy Saving Opportunities.....	79
Section 7	Architectural	
Table 7-1	Minimum Fire Rating of Spaces	91
Table 7-2	Computer Room Access Floor Performance Specifications	93
Section 9	Electrical Systems	
Table 9-1	Design Efficiency Ratios	103
Table 9-2	Class F0 Electrical System Overview	105
Table 9-3	Class F1 Electrical System Overview	106
Table 9-4	Class F2 Electrical System Overview	107
Table 9-5	Class F3 Electrical System Overview	109
Table 9-6	Class F4 Electrical System Overview	111
Table 9-7	Low-Voltage Distribution Voltages in Some Major Data Center Locations	119
Table 9-8	Static Bypass Switch Input, By Availability Class	133
Table 9-9	Summary of UPS Output Switchboard Counts for Classes	134
Table 9-10	Transformer Wirings and Output Voltages Commonly Used in Data Centers	137
Table 9-11	Multipliers for Electrical Distribution System Components.....	144
Table 9-12	Battery Standards Cross-Reference Table (IEEE Standard Number)	170
Table 9-13	SPD Locations as per Class	184
Table 9-14	Grounding and Bonding Connection Schedule.....	190
Table 9-15	Electrical Systems Availability Classes.....	202
Section 10	Mechanical	
Table 10-1	Section 10 Text References	221
Table 10-2	Class F0 and F1 Mechanical System Overview.....	232
Table 10-3	Class F2 Mechanical System Overview	234
Table 10-4	Class F3 Mechanical System Overview	237
Table 10-5	Class F4 Mechanical System Overview	239
Section 11	Fire Protection	
Table 11-1	Recommended Sprinkler Systems for Data Center Spaces.....	265
Table 11-2	Recommended Detection Systems for Data Center Spaces	268

Section 12 Security

Table 12-1	Thickness of Concrete Wall for Projectile Protection	293
Table 12-2	Vehicle Barrier Comparison	294
Table 12-3	Speed Of Concrete Wall Penetration	295
Table 12-4	Time to Penetrate Industrial Pedestrian Doors	296
Table 12-5	Time to Penetrate Windows.....	297
Table 12-6	Minimum Lighting Levels	305

Section 14 Telecommunications Cabling, Infrastructure, Pathways and Spaces

Table 14-1	Class C0 and C1 Overview.....	324
Table 14-2	Class C2 Overview	324
Table 14-3	Class C3 Overview	327
Table 14-4	Class C4 Overview	327
Table 14-5	Maximum Cable Stacking Height in Cabling Pathways.....	341
Table 14-6	Balanced Twisted-Pair Cabling Channel Performance.....	350
Table 14-7	Optical Fiber Cable Performance By Type.....	350
Table 14-8	Advantages and Disadvantages of Trunk Cabling Assemblies.....	353
Table 14-9	Balanced Twisted-Pair Cable Bend Radius and Pulling Tension	356
Table 14-10	Optical Fiber Cable Bend Radius and Pulling Tension	357
Table 14-11	Balanced Twisted-Pair Field Testing.....	360
Table 14-12	Common Applications Using Optical Fiber Cabling.....	363
Table 14-13	Reference Jumper Repeatability Allowance.....	363
Table 14-14	Example of Cabinet Depth Guidelines	369
Table 14-15	Available Space for Calculating Cabinet Vertical Cable Capacity.....	374

Section 15 Information Technology

Table 15-1	Tactics for Class N0 and N1	399
Table 15-2	Tactics for Class N2	400
Table 15-3	Tactics for Class N3	401
Table 15-4	Tactics for Class N4	401

Appendix B Reliability and Availability (Informative)

Table B-1	Identifying Operational Requirements: Time Available For Planned Maintenance Shutdown...	447
Table B-2	Identifying Operational Availability Rating: Maximum Annual Downtime (Availability %)	448
Table B-3	Classifying the Impact of Downtime on the Mission	449
Table B-4	Determining Data Center Services Availability Class	449
Table B-5	Tactics for Class 0	450
Table B-6	Tactics for Class 1	450
Table B-7	Tactics for Class 2	451
Table B-8	Tactics for Class 3	451
Table B-9	Tactics for Class 4	452
Table B-10	Relationship Between Availability Percentage and Allowable Downtime.....	454

Appendix C Alignment of Data Center Services Reliability with Application and System Architecture (Informative)

Table C-1	Tactics for Class A0 and A1	460
Table C-2	Tactics for Class A2.....	461
Table C-3	Tactics for Class A3 and A4	462
Table C-4	Tactics for Class S0 and S1	464
Table C-5	Tactics for Class S2	465
Table C-6	Tactics for Class S3	466
Table C-7	Tactics for Class S4	467

This page intentionally left blank

PREFACE

Revision History

June 18, 2010 First publication of this standard, titled BICSI 002-2010, *Data Center Design and Implementation Best Practices*

March 15, 2011 Revision of BICSI 002-2010 published as ANSI/BICSI 002-2011, *Data Center Design and Implementation Best Practices*

Major revisions include:

- Addition of Section 9, *Electrical*
- Addition of Section 14, *Telecommunications*

Minor revisions include: definitions, updating of graphics for printing and readability, other editorial corrections

December 9, 2014 Revision of ANSI/BICSI 002-2011 published as ANSI/BICSI 002-2014, *Data Center Design and Implementation Best Practices*

Major revisions include:

- Revision of Class F0 – F4 electrical infrastructure, including the removal of the requirement for a second power utility connection in Section 9, *Electrical*.
- Revised telecommunications Availability Classes C3 and C4 concerning the redundancy of main and horizontal distributors in Section 14, *Telecommunications*.
- Added, expanded and revised Availability Class structure to mechanical, telecommunications and network infrastructure (see Sections 9, 14, and 15 respectively).
- Addition of Appendix C, *Alignment of Data Center Services Reliability with Application and System Architecture*.
- Addition and revision of content for modular and containerized data centers in Section 6, *Space Planning* and Section 9, *Electrical*.
- Introduced content on DCIM and renamed Section 13 to *Data Center Management and Building Systems*.
- Expanded content regarding DC power and safety in Section 9, *Electrical*.
- Addition of hot and cold aisle containment in Section 6, *Space Planning* and Section 11, *Fire Protection*.
- Added and expanded content regarding designing for energy efficiency in multiple sections and added Appendix G, *Design for Energy Efficiency*.
- Addition of Appendix D, *Data Center Services Outsourcing Models*.
- Addition of Appendix E, *Multi-Data Center Architecture*.
- Updated cabinet door air flow and cable capacity calculations in Section 14, *Telecommunications*.

Minor revisions include:

- Moved former Section 5, *Space Planning* to directly after former Section 6, *Site Planning*.
- Restructuring of Section 5, *Site Planning*, Section 14, *Telecommunications*, and Section 16, *Commissioning*.
- Expansion of content to reflect both new and international design practices.
- Revisions to Appendix B, *Reliability and Availability*, to accommodate extension of availability classes.
- Update Section 8, *Structural*, to align with revisions to the *IBC* and related standards.

<List continues on next page>

- Updated Section 10, *Mechanical*, to reflect expanded ASHRAE guidelines for temperature and humidity.
- Updated Section 11, *Fire Protection* section to reflect changes in NFPA 75 and NFPA 76.
- Updated Section 14, *Telecommunications*, to reflect updates to ISO, TIA, and CENELEC data center cabling standards including cable types (removed OM1 and OM2, recommend OM4, added Category 8) and addition of intermediate distributor.
- Revised content regarding zinc whiskers and moved to Section 7, *Architectural*.
- Added content on testing equipment, system testing, acceptance testing, equipment operations and maintenance manuals, and system training to Section 16, *Commissioning*.
- Revised and moved system availability information to Appendix B, *Reliability and Availability*. (content formerly in Section 17, *Maintenance*).
- Added new content on maintenance plans and service contracts in Section 17, *Maintenance*.
- General content relocation and editorial corrections to improve readability and reduce ambiguity.

Document Format (Usability Features)

This standard has the following usability features as aids to the user:

- Additions and changes, other than those for editorial purposes, are indicated with a vertical rule within the left page margin.
- Deletion of one or more paragraphs is indicated with a bullet (•) between the content that remains

NOTE: The relocation of content, within or between sections (e.g., Section 5, *Site Selection* and Section 6, *Space Planning*), due to structure, readability, or content alignment is not indicated.

Translation Notice

This standard may have one or more translations available as a reference for the convenience of its readers. As that act of translation may contain inconsistencies with the original text, if differences between the translation and the published English version exist, the English text shall be used as the official and authoritative version.

1 Introduction

1.1 General

This standard is written with the expectation that the reader is familiar with the different facets of the design process (See Appendix A). The reader should understand from which role and point of view he or she intends to use this document (e.g., information technology, facilities, other corporate internal or external to the owner). Refer to Sections 1.2.1 – 1.2.3 below.

1.2 Purpose

This standard provides a reference of common terminology and design practice. It is not intended to be used by architects and engineers as their sole reference or as a step-by-step design guide, but may be used by such persons to determine design requirements in conjunction with the data center owner, occupant, or consultant.

This standard is intended primarily for:

- Data center owners and operators
- Telecommunications and information technology (IT) consultants and project managers
- Telecommunications and IT technology installers

Additionally, individuals in the following groups are also served by this standard.

1.2.1 Users Within IT

1.2.1.1 IT and Telecommunications Designers

IT and telecommunications designers and consultants may use BICSI 002 in conjunction with the appropriate local telecommunications infrastructure standard (e.g., ANSI/TIA-942-A, AS/NZS 2834-1995 Computer Accommodation, CENELEC EN 50173 Series, ISO/IEC 24764) to design the telecommunications pathways, spaces, and cabling system for the data center. The telecommunications designer/consultant should work with the data center architects and engineers to develop the IT and telecommunications equipment floor plan using guidelines specified in this standard.

1.2.1.2 IT and Telecommunications Management

IT and telecommunications management may use BICSI 002 as an aid in defining initial data center design requirements based on required levels of security, reliability, and availability. IT and telecommunications should work with information protection management, the business continuity group, and end user departments to determine the required levels of security, reliability, and availability.

1.2.1.3 IT Operations Management

Working with facilities groups, IT operations managers may use BICSI 002 to guide the requirements they specify to outsource suppliers who provide computing services and server room IT operations.

1.2.1.4 Information Security

Information security personnel may use BICSI 002 as a guide in defining and implementing information protection and security and assisting in the development of standard policies and operating procedures.

1.2.2 Users Within Facilities Group

1.2.2.1 Technical Representatives Within Facilities Group Capital Projects

Facilities group technical representatives may use BICSI 002 as a guide during the project planning phase as they estimate costs, prepare preliminary design and construction schedules, and prepare requests for professional services (RFPS) for the design and construction of new or renovated IT facilities. Thus, after the method of project delivery is determined, BICSI 002 becomes a referenced document in the RFPS that the facilities group prepares and issues to architecture and engineering (A/E) and design-build (D/B) firms. These companies, in turn, bid on the design and construction of the IT facilities.

1.2.2.2 Facilities Management Representatives Within Facilities Group

Facilities operations and management may use BICSI 002 as a guide in planning the operation and maintenance of corporate IT facilities so that these facilities maintain defined levels of reliability and availability. For example, BICSI 002 provides guidance in defining training needs and maintenance schedules of critical equipment for operations and maintenance personnel.

1.2.3 Staff Outside IT and Facilities Groups

1.2.3.1 Physical Security Management

Security staff responsible for physical security management may use BICSI 002 as a guide in determining physical security and fire protection system requirements for IT facilities.

1.2.3.2 External Resources

1.2.3.2.1 Telecommunications Consulting Firms

BICSI 002 is useful to telecommunications consulting firms or design/build installation firms by providing guidance in the design and construction of IT facilities for the corporation.

1.2.3.2.2 A&E and Construction Firms

BICSI 002 is useful to A&E and construction firms to guide them in the process of design and construction of IT facilities. It provides a reference of common terminology and reliability topologies. It is not intended to be used by A&E and construction firms as their sole reference, and it is not meant to provide a step-by-step design guide for the A&E or D/B firms; however, it may be used by such persons to guide design requirements in conjunction with the data center owner, occupant, or consultant.

1.3 Categories of Criteria

Two categories of criteria are specified — mandatory and advisory:

- Mandatory criteria generally apply to protection, performance, administration and compatibility; they specify the absolute minimum acceptable requirements.
- Advisory or desirable criteria are presented when their attainment will enhance the general performance of the data center infrastructure in all its contemplated applications.

Mandatory requirements are designated by the word *shall*; advisory recommendations are designated by the words *should*, *may*, or *desirable*, which are used interchangeably in this standard. Where possible, requirements and recommendations were separated to aid in clarity.

Notes, cautions and warnings found in the text, tables, or figures are used for emphasis or for offering informative suggestions.

2 Scope

This standard provides best practices and implementation methods that complement TIA, CENELEC, ISO/IEC and other published data center standards and documents. It is primarily a design standard, with installation requirements and guidelines related to implementing a design. The standard includes other installation requirements and guidelines for data centers where appropriate.

3 Required Standards and Documents

The following standards and documents contain provisions that constitute requirements listed within this standard. Unless otherwise indicated, all standards and documents listed are the latest published version prior to the initial publication of this standard. Parties to agreement based on this standard are encouraged to investigate the possibility of applying a more recent version as applicable.

Where equivalent local codes and standards exist, requirements from these local specifications shall apply. Where reference is made to a requirement that exceeds minimum code requirements, the specification requirement shall take precedence over any apparent conflict with applicable codes.

Alliance for Telecommunication Industry Solutions (ATIS)

- ATIS 0600336, *Engineering Requirements for a Universal Telecommunications Framework*

American Society of Civil Engineers (ASCE)

- ASCE/SEI 7, *Minimum Design Loads For Buildings and Other Structures*

American Society of Heating, Refrigerating, and Air-Conditioning Engineers (ASHRAE)

- ANSI/ASHRAE 62.1, *Ventilation for Acceptable Indoor Air Quality*
- *Best Practices for Datacom Facility Energy Efficiency*
- *Datacom Equipment Power Trends and Cooling Applications*
- *Design Considerations for Datacom Equipment Centers*
- *Particulate and Gaseous Contamination in Datacom Environments*
- *Structural and Vibration Guidelines for Datacom Equipment Centers*
- *Thermal Guidelines for Data Processing Environments*

ASTM International

- ASTM E84, *Standard Test Method for Surface Burning Characteristics of Building Materials*

BICSI

- ANSI/BICSI 005, *Electronic Safety and Security (ESS) System Design and Implementation Best Practices*

Electronic Components Industry Association (ECIA)

- EIA/ECA-310-E, *Cabinets, Racks, Panels, and Associated Equipment*

European Committee for Electrotechnical Standardization (CENELEC)

- CENELEC EN 50173-1, *Information technology – Generic cabling systems – Part 1: General requirements*
- CENELEC EN 50173-5, *Information technology – Generic cabling systems – Part 5: Data centres*
- CENELEC EN 50174-2, *Information technology – Cabling installation – Installation planning and practices inside buildings*

European Telecommunications Standards Institute (ETSI)

- ETSI EN 300-019, *Equipment Engineering (EE); Environmental conditions and environmental tests for telecommunications equipment*

International Code Council (ICC)

- *International Building Code (IBC)*
- *International Fuel Gas Code (IFGC)*
- *International Mechanical Code (IMC)*
- *International Plumbing Code (IPC)*

Institute of Electrical and Electronics Engineers (IEEE)

- IEEE 142 (The IEEE Green Book), *IEEE Recommended Practice for Grounding of Industrial and Commercial Power Systems*
- IEEE 450, *IEEE Recommended Practice for Maintenance, Testing, and Replacement of Vented Lead-Acid Batteries for Stationary Application*
- IEEE 484, *IEEE Recommended Practice for Installation Design and Installation of Vented Lead-Acid Batteries for Stationary Applications*
- IEEE 493 (The IEEE Gold Book), *IEEE Recommended Practice for the Design of Reliable Industrial and Commercial Power Systems*
- IEEE 1100 (The IEEE Emerald Book), *IEEE Recommended Practice for Powering and Grounding Electronic Equipment*
- IEEE 1106, *IEEE Recommended Practice for Installation, Maintenance, Testing, and Replacement of Vented Nickel-Cadmium Batteries for Stationary Applications*
- IEEE 1115, *IEEE Recommended Practice for Sizing Nickel-Cadmium Batteries for Stationary Applications*
- IEEE 1184, *IEEE Guide for Batteries for Uninterruptible Power Supply Systems*
- IEEE 1187, *IEEE Recommended Practice for Installation Design and Installation of Valve-Regulated Lead-Acid Batteries for Stationary Applications*
- IEEE 1188, *IEEE Recommended Practice for Maintenance, Testing, and Replacement of Valve-Regulated Lead-Acid (VRLA) Batteries for Stationary Applications*
- IEEE 1189, *IEEE Guide for the Selection of Valve-Regulated Lead-Acid (VRLA) Batteries for Stationary Applications*
- IEEE 1491, *IEEE Guide for Selection and Use of Battery Monitoring Equipment in Stationary Applications*
- IEEE 1578, *IEEE Recommended Practice for Stationary Battery Electrolyte Spill Containment and Management*

International Electrotechnical Commission (IEC)

- IEC 61280-4-1, *Fibre-optic communication subsystem test procedures - Part 4-1: Installed cable plant - Multimode attenuation measurement*
- IEC 61280-4-2, *Fibre optic communication subsystem basic test procedures - Part 4-2: Fibre optic cable plant - Single-mode fibre optic cable plant attenuation*
- IEC 61300-3-35, *Fibre optic interconnecting devices and passive components - Basic test and measurement procedures - Part 3-35: Examinations and measurements - Fibre optic connector endface visual and automated inspection*
- IEC 61935-1, *Specification for the testing of balanced and coaxial information technology cabling - Part 1: Installed balanced cabling as specified in ISO/IEC 11801 and related standards*
- IEC 62305-3, *Protection against lightning - Part 3: Physical damage to structures and life hazard*

International Organization for Standardization (ISO)

- ISO 7240, *Fire detection and alarm systems*
- ISO/IEC 11801, *Information technology – Generic cabling for customer premises*
- ISO 14520, *Gaseous fire-extinguishing systems – Physical properties and system design*
- ISO/IEC 14763-2, *Information technology – Implementation and operation of customer premises cabling – Part 2: Planning and installation*
- ISO/IEC 14763-3, *Information technology – Implementation and operation of customer premises cabling – Part 3: Testing of optical fibre cabling*
- ISO/IEC 24764, *Information technology – Generic cabling systems for data centres*

National Electrical Contractors Association (NECA)

- ANSI/NECA/BICSI 607, *Telecommunications Bonding and Grounding Planning and Installation Methods for Commercial Buildings*

National Fire Protection Association (NFPA)

- NFPA 12, *Carbon Dioxide Fire Extinguishing Systems*
- NFPA 12A, *Halon 1301 Fire Extinguishing Systems*
- NFPA 13, *Standard for the Installation of Sprinkler Systems*
- NFPA 20, *Installation of Stationary Pumps for Fire Protection*
- NFPA 70®, *National Electrical Code® (NEC®)*
- NFPA 70E, *Standard for Electrical Safety in the Workplace*
- NFPA 72®, *National Fire Alarm and Signaling Code*
- NFPA 75, *Standard for the Protection of Information Technology Equipment*
- NFPA 76, *Recommended Practice for the Fire Protection of Telecommunications Facilities*
- NFPA 1600, *Standard on Disaster/Emergency Management Business Continuity Programs*
- NFPA 2001, *Standard on Clean Agent Fire Extinguishing Systems*
- *NFPA Fire Protection Handbook*

Telcordia

- Telcordia GR-63-CORE, *NEBS Requirements: Physical Protection*
- Telcordia GR-139, *Generic Requirements for Central Office Coaxial Cable*
- Telcordia GR-3028-CORE, *Thermal Management in Telecommunications Central Offices*

Telecommunication Industry Association (TIA)

- ANSI/TIA-526-7, *OFSTP-7, Measurement of Optical Power Loss of Installed Single-Mode Fiber Cable Plant*
- ANSI/TIA-526-14-B, *Optical Power Loss Measurements of Installed Multimode Fiber Cable Plant; IEC 61280-4-1 edition 2, Fibre-Optic Communications Subsystem Test Procedure – Part 4-1: Installed cable plant- Multimode attenuation measurement*
- ANSI/TIA-568-C.2, *Balanced Twisted-Pair Telecommunications Cabling and Components Standard*
- ANSI/TIA-568-C.3, *Optical Fiber Cabling Components Standard*
- ANSI/TIA-569-C, *Telecommunications Pathways and Spaces*
- ANSI/TIA-606-B, *Administration Standard for Telecommunications Infrastructure*
- ANSI/TIA-607-B, *Generic Telecommunications Bonding and Grounding (Earthing) for Customer Premises*
- ANSI/TIA-862-A, *Building Automation Systems Cabling Standard*
- ANSI/TIA-942-A, *Telecommunications Infrastructure Standard for Data Centers*
- TIA TSB-155-A, *Guidelines for the Assessment and Mitigation of Installed Category 6 Cabling to Support 10GBASE-T*

Underwriters Laboratories (UL)

- ANSI/UL 497, *Standard for Safety Protectors for Paired-Conductor Communications Circuits*
- UL 723, *Standard for Test for Surface Burning Characteristics of Building Materials*
- UL 1449, *Surge Protective Devices*
- UL 60950-1, *Information Technology Equipment - Safety - Part 1: General Requirements*

Other Standards and Documents

- *EU Code of Conduct on Data Centres Energy Efficiency, version 1.0*
- *EU Best Practices for EU Code of Conduct on Data Centres, version 3.08*

This page intentionally left blank

4 Definitions, Acronyms, Abbreviations, and Units of Measurement

For the purpose of this standard, the following definitions, acronyms, abbreviations and units of measurement apply.

4.1 Definitions

A-C-rated fire-retardant plywood	Plywood treated with a fire-retardant that has a well-finished A grade side that typically faces outward and a less finished C grade side that typically faces the wall.
abandoned cable	Installed cables that are not terminated at both ends at a connector or other equipment and not identified 'For Future Use' with a tag.
access block	A single access switch or group of switches sharing one trunk/uplink or set of redundant uplinks to the distribution layer. Generally confined to one telecommunications room (TR). In a large TR, it is possible to have more than one access block.
access floor	A system consisting of completely removable and interchangeable floor panels that are supported on adjustable pedestals or stringers (or both) to allow access to the area beneath the floor (also known as raised floor).
access layer	The point at which local end users are allowed into the network. In a LAN environment, this connection point is typically a switched Ethernet port that is assigned to a VLAN.
access provider	The operator of any facility that is used to convey telecommunications signals to and from a customer premises.
adapter	A device that converts attributes of one device or system to those of an otherwise incompatible device or system. The use of an adaptor may allow actions such as (a) the connection of different sizes or types of plugs (b) the rearrangement of leads or segmentation of cables with numerous conductors into smaller group (c) interconnection between cables (d) connection of systems with differing voltage, polarity or waveform.
administration	The method for labeling, identification, documentation and usage needed to implement moves, additions and changes of the telecommunications infrastructure
alarm	An electrical, electronic, or mechanical signal that serves to warn of danger or abnormal condition by means of an audible sound or visual signal.
alien crosstalk	Unwanted coupling of signals into a balanced twisted-pair in a given cable from one or more balanced twisted-pair(s) external to the given cable.
alien far-end crosstalk	The unwanted signal coupling from a disturbing pair of a 4-pair channel, permanent link, or component to a disturbed pair of another 4-pair channel, permanent link or component, measured at the far end.
alien near-end crosstalk	Unwanted signal coupling from a disturbing pair of a 4-pair channel, permanent link, or component to a disturbed pair of another 4-pair channel, permanent link, or component, measured at the near end.
asset	Anything tangible or intangible that has value.
attenuation	The decrease in magnitude of transmission signal strength between points, expressed in units of decibels (dB) from the ratio of output to input signal level. See also <i>insertion loss</i> .
attenuation to crosstalk	Crosstalk measured at the opposite end from which the disturbing signal is transmitted normalized by the attenuation contribution of the cable or cabling.
automatic transfer switch	See <i>transfer switch, automatic</i> .

availability	The probability that a component or system is in a condition to perform its intended function, which is calculated as the ratio of the total time a system or component is functional within a specified time interval divided by the length of the specified time interval.
backboard	A panel (e.g., wood or metal) used for mounting connecting hardware and equipment.
backbone	(1) A facility (e.g., pathway, cable, conductors) between any of the following space telecommunications rooms (TRs), common TRs, floor-serving terminals, entrance facilities, equipment rooms, and common equipment rooms. (2) In a data center, a facility (e.g., pathway, cable, conductors) between any of the following spaces entrance rooms or spaces, main distribution areas, horizontal distribution areas, and TRs.
backbone cable	See <i>backbone</i> .
blanking panel (or filler panel)	(1) A panel that may be plastic or finished metal and is not integral to any discrete electronic component or system. (2) A barrier installed in information technology equipment cabinets, racks, or enclosures for maximizing segregation for optimized cooling effectiveness.
bonding	The permanent joining of metallic parts to form an electrically conductive path that will ensure electrical continuity and the capacity to conduct safely any current likely to be imposed.
bonding conductor (jumper)	A reliable conductor to ensure the required electrical conductivity between metal parts required to be electrically connected.
bonding conductor for telecommunications	A conductor that interconnects the telecommunications bonding infrastructure to the building's service equipment (power) ground.
bonding network	A set of interconnected conductive structures that provides, in varying degrees based upon the design topology and installation, an electromagnetic shield for electronic systems and personnel at frequencies to tens of megahertz (MHz). NOTE: The term <i>electromagnetic shield</i> denotes any structure used to divert, block or impede the passage of electromagnetic energy. In general, a bonding network need not be connected to ground but all bonding networks considered in the standard will have a ground connection. Typical energy sources of concern are lightning, and alternating current (AC) and direct current (DC) power faults. Of generally lesser concern are quasi steady-state sources such as AC power harmonics, and "function sources" such as clock signals from digital equipment.
building commissioning	In the broadest sense, a process for achieving, verifying, and documenting that the performance of a building and its various systems meet design intent and the owner and occupants' operational needs. The process ideally extends through all phases of a project, from concept to occupancy and operations.
building systems	The architectural, mechanical, electrical, and control system along with their respective subsystems, equipment, and components.
built-in-place	A traditional construction method that may be employed for the data center space or supporting infrastructure. It can be extrapolated to also indicate hand-configured cabinets, networks and information technology equipment and systems. It is synonymous with the phrase <i>stick built</i> .
bundled cable	An assembly consisting of two or more cables, of the same or different types of cable media, continuously bound together to form a single unit. Bundled cable may be created by the original cable manufacturer, a third party facility, or during installation. See also <i>hybrid cable</i>

bus topology	(1) Networking topology where each communications device or network has a single connection to a shared medium that serves as the communications channel. Also called a <i>point-to-multipoint topology</i> . (2) A linear configuration where all network devices are connected using a single length of cable. It requires one backbone cable to which all network devices are connected.
cabinet	A container with a hinged cover that may enclose telecommunications connection devices, terminations, apparatus, wiring, and equipment.
cable management	Physical structures attached to, within, or between cabinets and racks to provide horizontal and vertical pathways for guiding and managing cabling infrastructure.
cable plant	Cable, raceways, vaults, junction/pull boxes, racks, equipment, patch bays/blocks, and other infrastructure required to provide physical, electrical, optical connectivity between buildings of the owner or between buildings on the owner's property.
• cable sheath	A covering over the optical fiber or conductor assembly that may include one or more metallic members, strength members, or jackets.
cable tray system	A cable tray unit or assembly of cable tray units or sections and associated fittings forming a rigid structural system used to securely fasten or support cables and raceway.
cable tray	A support mechanism used to route and support telecommunications and other cable. Cable trays may be equipped with side walls or barriers to constrain a cable's horizontal placement or movement.
cable	(1) An assembly of one or more insulated conductors or optical fibers within an enveloping sheath. (2) An assembly of one or more cable units of the same type and category in an overall sheath. It may include overall screen. (3) The act of installing cable.
cabling	A combination of all cables, jumpers, cords, and connecting hardware.
campus	(1) The buildings and grounds having legal contiguous interconnection (e.g., college, university, industrial park, military installation). (2) A premises containing one or more buildings.
central office	A building that functions as a network or telecommunication service provider's switching center. A central office typical serves a defined geographical area and utilizes outside plant cabling infrastructure to connect the central office to one or more customers. A central office may also be termed a <i>telco exchange</i> or <i>public exchange</i> .
centralized cabling	A cabling configuration from the work area to a centralized cross-connect using pull through cables and an interconnect or splice in the telecommunications room.
change of state	A change from the normal operating stance of a system, whether required by maintenance or a failure, resulting from an automatic or a manual response to some form of system input or response.
channel	The end-to-end transmission path between two points at which application-specific equipment is connected.
Class	An abbreviation of Data Center Facility Availability Class—the characteristic uptime performance of one component of the critical IT infrastructure. A quantitative measure of the total uptime needed in a facility without regard to the level of quality required in the IT functions carried on during that uptime. As used in this standard, it applies to scheduled uptime. Class is expressed in terms of one of five Data Center Facility Availability Classes. This classification reflects the interaction between the level of criticality and the availability of operation time.
clean agent	An electrically nonconductive, volatile, or gaseous fire extinguishant that does not leave a residue upon evaporation.

clean agent fire suppression	A fire extinguishing system using a total flooding clean agent.
clear zone	An area separating an outdoor barrier from buildings or any form of natural or fabricated concealment.
client	(1) An internal or external customer. (2) A hardware or software entity, as in “client/server.”
closed transition	A change of state or transfer where the electrical circuit connection is maintained during the transfer. This is also known as <i>make before break</i> .
colocation	A data center, managed by a vendor, that provides one or more services (e.g., space, power, network connectivity, cooling, physical security) for the server, storage, and networking equipment of one or more customers. A colocation data center is often called a <i>colo</i> .
command center	A location where network and IT systems are managed and monitored. A command center is commonly referred to as a network operations center (NOC).
commissioning authority	The qualified person, company, or agency that plans, coordinates, and oversees the entire commissioning process. The Commissioning Authority may also be known as the Commissioning Agent.
commissioning plan	The document prepared for each project that describes all aspects of the commissioning process, including schedules, responsibilities, documentation requirements, and functional performance test requirements.
commissioning test plan	The document that details the prefunctional performance test, functional performance test, and the necessary information for carrying out the testing process for each system, piece of equipment, or energy efficiency measure.
common bonding network	The principal means for effecting bonding and grounding inside a telecommunication building. It is the set of metallic components that are intentionally or incidentally interconnected to form the principal bonding network (BN) in a building. These components include structural steel or reinforcing rods, plumbing, alternating current (AC) power conduit, AC equipment grounding conductors (ACEGs), cable racks, and bonding conductors. The CBN always has a mesh topology and is connected to the grounding electrode system.
common equipment room (telecommunications)	An enclosed space used for equipment and backbone interconnections for more than one tenant in a building or campus.
common grounding electrode	(1) An electrode in or at a building structure that is used to ground an AC system as well as equipment and conductor enclosures. (2) A single electrode connected to separate services, feeders, or branch circuits supplying a building. (3) Two or more grounding electrodes that are bonded together.
compartmentalization	The segregation of components, programs, and information. This provides isolation and protection from compromise, contamination, or unauthorized access.
component redundancy	A configuration designed into a system to increase the likelihood of continuous function despite the failure of a component. Component redundancy is achieved by designing and deploying a secondary component so that it replaces an associated primary component when the primary component fails.
computer room	An architectural space with the primary function of accommodating data processing equipment.
concurrently maintainable and operable	A configuration where system components may be removed from service for maintenance or may fail in a manner transparent to the load. There will be some form of state change, and redundancy will be lost while a component or system is out of commission. This is a prime requirement for a Class 3 facility.

conduit	(1) A raceway of circular cross section. (2) A structure containing one or more ducts.
connecting hardware	A device providing mechanical cable terminations.
connectivity	Patch panels, cabling, connectors, and cable management used to create and maintain electrical and optical circuits.
consolidation point	A location for interconnection between horizontal cables extending from building pathways and horizontal cables extending into furniture pathways.
construction manager	An organization or individual assigned to manage the construction team and various contractors to build and test the building systems for the project.
containerized	An information technology equipment (ITE) or infrastructure solution offered in a cargo shipping container, typically 12 m long by 2.4 m wide by 2.4 m high (40 ft by 8 ft by 8 ft). A container solution may offer combined electrical, mechanical and data center space as part of the solution or may offer space for a singular service (e.g., electrical or mechanical solutions).
cord	A length of cable with connectors on one or both ends used to join equipment with cabling infrastructure (i.e., patch panel or cross-connect), a component of cabling infrastructure to another component of cabling infrastructure, or active equipment directly to active equipment.
core layer	The high-speed switching backbone of the network. Its primary purpose is to allow the distribution layer access to critical enterprise computing resources by switching packets as fast as possible.
countermeasures	The procedures, technologies, devices or organisms (e.g., dogs, humans) put into place to deter, delay or detect damage from a threat.
critical distribution board	A power distribution board that feeds critical loads.
criticality	The relative importance of a function or process as measured by the consequences of its failure or inability to function.
cross-connect	A facility enabling the termination of cable elements and their interconnection or cross-connection.
cross-connection	A connection scheme between cabling runs, subsystems, and equipment using patch cords or jumpers that attach to connecting hardware on each end.
dark fiber	Unused installed optical fiber cable. When optical fiber cable is carrying a light signal, it is referred to as <i>lit fiber</i> .
data center	A building or portion of a building with the primary function to house a computer room and its support areas.
data center infrastructure efficiency	Typically expressed as <i>DCIE</i> , data center infrastructure efficiency is a metric for an entire data center, calculated as the reciprocal of power usage effectiveness (PUE), where $1/PUE = IT\ equipment\ power / Total\ facility\ power \times 100\%$.
delay skew	The difference in propagation delay between the pair with the highest and the pair with the lowest propagation delay value within the same cable sheath.
demarc	See <i>demarcation point</i> .
demarcation point	A point where the operational control or ownership changes, typically between the service provider and the customer.
design document	The record that details the design intent.
design intent	Design intent is a detailed technical description of the ideas, concepts, and criteria defined by the building owner to be important.

designation strips	A type of label designated for insertion into a termination frame, comprised of paper or plastic strips, which are usually contained in a clear or color-tinted plastic carrier. Designation strips are usually imprinted with the adjacent terminal number and are used to aid in locating a specific pair, group of pairs, or information outlet or for delineating a termination field.
detection, (fire protection)	The means of detecting the occurrence of heat, smoke or other particles or products of combustion.
distribution layer	Collection of switches between the core and access layer. Distribution switches may be a switch and external router combination or a multilayer switch.
domain	A portion of the naming hierarchy tree that refers to general groupings of networks based on organization type or geography.
double ended	A power distribution switchboard with two power source inputs with an interposing tiebreaker between the sources where either input source of the switchboard can supply 100% of the load. The double-ended system constitutes an N + 1 or 2N system. This type of system may be used for dual utility systems or a single utility system split into redundant feeds and may possess the circuit breaker transfer system with the generator.
earthing	See <i>grounding</i> .
electromagnetic interference	Radiated or conducted electromagnetic energy that has an undesirable effect on electronic equipment or signal transmissions.
emergency systems	Those systems legally required and classed as emergency by municipal, state, federal, or other codes or by any governmental agency having jurisdiction. These systems are intended to automatically supply illumination, power, or both to designated areas and equipment in the event of failure of the normal supply or in the event of accident to elements of a system intended to supply, distribute, and control power and illumination essential for safety to human life.
energy efficiency measure	Any equipment, system, or control strategy installed in a building for the purpose of reducing energy consumption and enhancing building performance.
entrance conduit	Conduit that connects the outside underground infrastructure with the building's entrance room.
entrance facility (telecommunications)	(1) An entrance to a building for both public and private network service cables (including wireless), including the entrance point of the building and continuing to the entrance room or space. (2) A facility that provides all necessary mechanical and electrical services for the entry of telecommunications cables into a building and that complies with all relevant regulations.
entrance point (telecommunications)	The point of emergence for telecommunications cabling through an exterior wall, a floor, or from a conduit.
entrance room or space (telecommunications)	A space in which the joining of inter or intra building telecommunications backbone facilities takes place. Examples include computer rooms and server rooms.
equipment cord	See <i>cord</i> .
equipment distribution area	The computer room space occupied by equipment cabinets or racks.
equipment grounding conductor	The conductive path installed to connect normally non-current carrying metal parts of equipment together and to the system grounded conductor or to the grounding electrode conductor or both.
equipment room (telecommunications)	An environmentally controlled centralized space for telecommunications and data processing equipment with supporting communications connectivity infrastructure.

equipotential bonding	Properly designed and installed electrical connections(s) putting various exposed conductive parts and extraneous conductive parts at a substantially equal potential, especially during normal (non-transient) conditions.
event	Typically, a message generated by a device for informational or error purposes.
failure mode	A system state resulting from an unanticipated system outage and typically an automatic system response to that failure.
Faraday cage	A metallic enclosure that is designed to prevent the entry or escape of electromagnetic fields. An ideal Faraday cage consists of an unbroken perfectly conducting shell. This ideal cannot be achieved in practice but it can be approached.
fault tolerant	The attribute of a concurrently maintainable and operable system or facility where redundancy is not lost during failure or maintenance mode of operation.
fiber management	Hardware designed and manufactured for keeping optical fiber patch cords neat and orderly. Most termination frame manufacturers provide optical fiber management components designed to work in conjunction with their termination frames. Fiber management may also refer to other types of hardware for securing optical fiber cable to the building.
fiber optic	See <i>optical fiber</i> .
fire	The presence of a flame.
fire detection	The means of detecting the occurrence of heat, smoke or other particles or products of combustion.
fire protection	The active means of detecting and suppressing fires.
fire suppression	The means of extinguishing an active fire.
flexibility	A design's ability to anticipate future changes in space, communications, power density, or heat rejection and to respond to these changes without affecting the mission of the critical IT functions.
frame	A special purpose equipment mounting structure (e.g., IDC blocks, fiber termination hardware not meant to be mounted in standard 19 inch or 23 inch racks).
functional performance test	The full range of checks and tests carried out to determine whether all components, subsystems, systems, and interfaces between systems function in accordance with the design documents.
ground	A conducting connection, whether intentional or accidental, between an electrical circuit or equipment and the earth or to some conducting body that serves in place of earth.
ground fault circuit interrupter	A device intended for the protection of personnel that functions to de-energize a circuit or portion thereof within an established period of time when a current to ground exceeds the values established for a Class A device.
grounding	The act of creating a ground.
grounding conductor	A conductor used to connect the grounding electrode to the building's main grounding busbar.
grounding electrode	A conducting object through which a direct connection to earth is established.
grounding electrode conductor	The conductor used to connect the grounding electrode to the equipment grounding conductor or to the grounded conductor of the circuit at the service equipment or at the source of a separately derived system.
grounding electrode system	One or more grounding electrodes that are connected together.
grounding equalizer	The conductor that interconnects elements of the telecommunications grounding infrastructure.

hanging load	The weight that can be suspended from the underside of the floor or structure above.
hardening	Protection from physical forces, security breaches, and natural disasters.
heat (fire protection)	The existence of temperatures significantly above normal ambient temperatures.
high-order mode transient losses	Losses in optical signal level power caused by the attenuation of weakly guided high-order modes of multimode optical fiber.
high resistance/impedance grounding system	A type of impedance grounded neutral system in which a grounding impedance, usually a resistor, limits the ground-fault current.
higher Class	Within this standard, a higher Class data center is a data center that meets the requirements of either Class 3 or Class 4.
horizontal cabling	(1) The cabling between and including the telecommunications outlet/connector and the horizontal cross-connect. (2) The cabling between and including the building automation system outlet or the first mechanical termination of the horizontal connection point and the horizontal cross-connect. (3) Within a data center, horizontal cabling is the cabling from the horizontal cross-connect (in the main distribution area or horizontal distribution area) to the outlet in the equipment distribution area or zone distribution area.
horizontal cross-connect	A cross-connect of horizontal cabling to other cabling (e.g., horizontal, backbone, equipment).
horizontal distribution area	A space in a computer room where a horizontal cross-connect is located and may include LAN switches, SAN switches, and keyboard/video/mouse (KVM) switches for the end equipment located in the equipment distribution areas.
hot spot	A temperature reading taken at the air intake point of equipment mounted in a cabinet or rack in excess of the design standard or equipment requirement.
human events	Man-made incidents, including economic, general strike, terrorism (e.g., ecological, cyber, nuclear, biological, chemical), sabotage, hostage situation, civil unrest, enemy attack, arson, mass hysteria, accidental and special events.
hybrid cable	A manufactured assembly of two or more cables of the same or differing types of media, categories designation, covered by one overall sheath. See also <i>bundled cable</i> .
identifier	An unique item of information that links a specific element of the telecommunications infrastructure with its corresponding record.
impact of downtime	One of three characteristics used to determine the performance requirements and associated redundancy of the critical systems within a data center. The impact of downtime characteristic integrates the multiple effects that a disruption in computer processing services has on an organization's ability to achieve its objectives. See also <i>operational level</i> and <i>operational availability</i> .
incipient	The early or beginning stage of a fire where combustion particulates may be emitted from materials developing inherently high heat but no smoke is visible and are low in density and below the level of detection capabilities of conventional smoke detectors.
inductive/reactance-grounded power system	A method of grounding in which the system is grounded through impedance, the principle element of which is inductive reactance.
information technology equipment	Electronic equipment used for the creation, processing, storage, organization, manipulation and retrieval of electronic data.
information technology equipment power	The power consumed by ITE to manage, monitor, control, process, store, or route data within the data center, excluding all infrastructure equipment.
infrastructure (telecommunications)	A collection of those telecommunications components, excluding equipment, that together provides the basic support for the distribution of all information within a building or campus.

input source transfer	The function of and the location in the electrical system where the transfer occurs between two sources.
insertion loss	The signal loss resulting from the insertion of a component or link between a transmitter and receiver. Insertion loss is often referred to as <i>attenuation</i> .
inside plant	Communication systems inside a building (wire, optical fiber, coaxial cable, equipment racks, and information outlets). Telecommunications companies refer to this as inside wire or intrafacility cabling.
interconnection	(1) A connection scheme that employs connecting hardware for the direct connection of a cable to another cable without a patch cord or jumper. (2) A type of connection in which single port equipment connections (e.g., 4-pair and optical fiber connectors) attach to horizontal or backbone cabling by means of patch cords or jumpers.
intermediate cross-connect	A cross-connect between first level and second level backbone cabling. Also referred to as the horizontal cross-connect (HC).
intersystem bonding conductor	A conductor used to connect grounding systems for diverse (e.g., electrical, telecommunications) or multiple electrical services to a common building grounding electrode system (e.g., building ground [electrode] ring).
isolated bonding network	Typically expressed as <i>IBN</i> , an isolated bonding network is a bonding and grounding subsystem in which all associated equipment cabinets, frames, racks, cable trays, pathways and supplementary bonding grids designated to be within that IBN are bonded together at a single point of connection (SPC). The SPC is also bonded to either the common bonding network (CBN) or another IBN. All IBNs have a connection to ground through the SPC.
isolation	A design strategy that mitigates the risk of concurrent damage to some components in a facility using physical, logical, or system separation.
jumper	(1) An assembly of twisted pairs without connectors used to join telecommunications circuits/links at the cross-connect. (2) A length of optical fiber cable with a connector plug on each end. (3) A length of twisted-pair or coaxial cable with connectors attached to each end, also called a <i>patch cord</i> .
label	A piece of paper or other material that is fastened to something and gives predefined information about it. Describes its identity, path, location, or other important information about the product or material.
ladder rack	A cable tray with side stringers and cross members, resembling a ladder, which may support cable either horizontally or vertically.
layering	In security, the use of many layers of barriers, other countermeasures, or a mixture of both used to provide the maximum level of deterrence and delay to intruders.
link	A transmission path between two points, not including equipment and cords.
linkage	A connection between a record and an identifier or between records in a database.
Listed	Equipment, materials, or services included in a list published by an organization that is acceptable to the authority having jurisdiction (AHJ), maintaining periodic inspection of production of listed equipment or materials or periodic evaluation of services and whose listing states either the equipment, material, or services meets appropriate standards or has been tested and found suitable for use in a specified manner
load bank	A device to simulate actual equipment consisting of groups of resistive and reactive elements, fans, and controls. The load bank is an electrical load that is connected to power distribution unit (PDU) systems, uninterruptible power supply (UPS) systems or generators in load test situations.

local distribution point	A connection point within the zone distribution cabling subsystem between a zone distributor and an equipment outlet as described in CENELEC EN 50173-5 and ISO/IEC 24764. A LDP is equivalent to the consolidation point (CP) in a zone distribution area (ZDA) as described ANSI/TIA-942-A.
luminaire	An electric light and its components; an electrical lighting fixture.
M13 multiplexer	Consolidates T-1 and E-1 signals into a T-3 or E-3 circuit. A cost-effective device for combining independent T-1s, E-1s, or a combination of the two over the same T-3 or E-3 circuit.
main cross-connect	A cross-connect for first level backbone cables, entrance cables, and equipment cords.
main distribution area	The space in a computer room where the main cross-connect is located.
main distributor	A distributor used to make connections between the main distribution cabling subsystem, network access cabling subsystem, cabling subsystems and active equipment. Equivalent to the main cross-connect.
main electrical grounding busbar	The busbar within the building at which electrical service grounding electrode conductor(s) and other grounding and bonding conductors are interconnected to establish the main equipotential location for the building.
maintenance mode	A system state resulting from an anticipated system outage or routine maintenance activity and typically a manual system response to that activity.
management information base	Within the simple network management protocol (SNMP), defines objects and attributes to be managed.
manual transfer switch	See <i>transfer switch, non-automatic</i> .
mechanical room	An enclosed space, which serves the needs of mechanical building systems.
media (telecommunications)	Wire, cable, or conductors used for telecommunications.
medium voltage	Any electrical voltage above the normal utilized value and below transmission-level system voltages. The utilization voltage varies from country to country. In the United States, medium voltage is considered to be between 1001 V and 35,000 V, whereas in the European Union and other parts of the world, the utilization voltage level can be significantly higher than in the United States.
meshed bonding network	A non-insolated bonding network to which all associated equipment cabinets, frames racks, cable trays, and pathways are connected by using a bonding grid. This grid is connected at multiple points to the common bonding network.
mission critical	Any operation, activity, process, equipment, or facility that is essential to continuous operation for reasons of business continuity, personnel safety, security, or emergency management.
modular	As applied to a data center, a factory-built or pre-fabricated data center space, infrastructure or combination of data center space and infrastructure that is constructed away from the actual data center site and is delivered as a complete solution. A modular data center may utilize or require some final site assembly or fabrication.
modular jack	The receptacle (“female”) element of a telecommunications connector that may be keyed or unkeyed, typically has six or eight contact positions, of which not all the positions need to be equipped with contacts. NOTE: The element inserted into a modular jack is named a <i>modular plug</i> .
module	The incremental development size of a storage or computer node, electrical or mechanical system, or data center area.
multimode optical fiber	An optical fiber that carries many paths (modes) of light.

natural barrier	Any object of nature that impedes or prevents access, including mountains, bodies of water, deserts, and swamps.
natural events	Natural disasters, including drought, fire, avalanche, snow/ice/hail, tsunamis, windstorm/tropical storm, hurricane/typhoon/cyclone, biological, extreme heat/cold, flood/wind-driven water, earthquake/land shift, volcanic eruption, tornado, landslide/mudslide, dust/sand storm, and lightning storm.
near-end crosstalk	(1) The unwanted signal coupling between pairs. It is measured at the end of a cable nearest the point of transmission. (Contrast with <i>far-end crosstalk</i> , which is measured at the end farthest from point of transmission). (2) The signal transfer between circuits at the same (near) end of the cable.
network operation center	<i>See command center.</i>
normal mode	The steady-state system configuration while under load.
open transition	A change of state or transfer where the electrical circuit connection is not maintained during the transfer. This is also known as <i>break before make</i> .
operational availability	One of three characteristics used to determine the performance requirements and associated redundancy of the critical systems within a data center. The operational availability integrates the multiple effects of an organization's expected uptime of the computer processing systems during normal operations. See also <i>operational level</i> and <i>impact of downtime</i> .
operational level	One of three characteristics used to determine the performance requirements and associated redundancy of the critical systems within a data center. The operational level integrates the multiple effects of an organization's ability, or inability, to suspend all computer processing operations for planned maintenance. See also <i>impact of downtime</i> and <i>operational availability</i> .
optical fiber	Any filament made of dielectric materials that guides light.
optical fiber cable	An assembly consisting of one or more optical fibers.
outside plant	Communications system outside of the buildings (typically underground conduit and vaults, exterior/underground, aerial, and buried rated wire and cable).
panelboard (electrical)	A single panel, or groups of panel units, designed for assembly in the form of a single panel, including buses and automatic overcurrent devices such as fuses or molded-case circuit breakers, accessible only from the front.
passive damper	An unpowered device that is utilized in structures to mitigate the effects of vibration due to seismic or wind loading.
patch cord	<i>see cord.</i>
patch panel	A connecting hardware system that facilitates cable termination and cabling administration using patch cords.
pathway	A facility for the placement of telecommunications cable.
performance test	A series of tests for specified equipment or systems, which determines that the systems are installed correctly, started and are prepared for the functional performance tests. Often these tests are in a checklist format.
performance verification	The process of determining the ability of the system to function according to the design intent.
permanent link	(1) The permanently installed portion of horizontal cabling, excluding cords (e.g., test, equipment, patch). (2) A test configuration for a link excluding test cords and patch cords.
plenum	A compartment or chamber that forms part of the air distribution system.

power distribution unit	Typically expressed as <i>PDU</i> , this is a floor- or rack-mounted enclosure for distributing branch circuit electrical power via cables, either overhead or under an access floor, to multiple racks or enclosures of information technology equipment (ITE). A PDU includes one or more distribution panelboards and can include a transformer, monitoring, and controls. PDUs may also be called a <i>computer power center</i> or a <i>power distribution center</i> .
power strip	A device mounted onto or within an information technology equipment (ITE) rack or enclosure, supplied by a single branch circuit, and containing power receptacles into which multiple IT devices can be plugged. A power strip can include metering, controls, circuit protection, filtering, and surge suppression. A power strip is identified within IEEE 1100 as a <i>power outlet unit</i> or <i>POU</i> . A power strip may also be called a <i>rack-mount PDU</i> , <i>rack power distribution unit</i> , <i>ITE-PDU</i> , <i>cabinet distribution unit</i> , or <i>plug strip</i> .
power sum alien far-end crosstalk	The power sum of the unwanted signal coupling from multiple disturbing pairs of one or more 4-pair channels, permanent links, or components to a disturbed pair of another 4-pair channel, permanent link, or component measured at the far end.
power sum alien near-end crosstalk	The power sum of the unwanted signal coupling from multiple disturbing pairs of one or more 4-pair channels, permanent links, or components to a disturbed pair of another 4-pair channel, permanent link, or component measured at the near end.
power sum attenuation to alien crosstalk ratio at the far end	The difference in dB between the power sum alien far-end crosstalk (PSAFEXT) from multiple disturbing pairs of one or more 4-pair channels, permanent links, or components and the insertion loss of a disturbed pair in another 4-pair channel, permanent link, or component.
power sum attenuation to crosstalk ratio, far-end	A computation of the unwanted signal coupling from multiple transmitters at the near end into a pair measured at the far end and normalized to the received signal level.
power sum near-end crosstalk	A computation of the unwanted signal coupling from multiple transmitters at the near end into a pair measured at the near end.
power usage effectiveness	Typically expressed as <i>PUE</i> , power usage effectiveness is an efficiency metric for an entire data center calculated as the total facility power usage divided by the information technology equipment power usage. PUE is the reciprocal of data center infrastructure efficiency (DCIE).
primary side	The high-voltage side of the electrical power service transformer (above 600V), the electrical power service line side of the UPS, and the electrical power service line side of the PDU transformer or the 480V side of the static switch.
private branch exchange	A private telecommunications switching system allowing private local voice (and other voice-related services) switching over a network.
propagation delay	The time required for a signal to travel from one end of the transmission path to the other end.
protected circuit	A communication circuit in which a second path automatically activates when the primary path fails.
protection, fire	The active means of detecting and suppressing fires occurring within the data processing facility.
psychological barrier	A device, obstacle or lack of obstacle that by its presence alone discourages unauthorized access or penetration.
pull box	A housing located in a closed raceway used to facilitate the placing of wire or cables.
quality control	One of the four major strategies for increasing reliability by ensuring that high quality is designed and implemented in the facility, thus reducing the risk of downtime because of new installation failures or premature wear.

raceway	An enclosed channel of metal or nonmetallic materials designed expressly for holding wires or cables. Raceways include, but are not limited to: rigid metal conduit, rigid nonmetallic conduit, rigid nonmetallic conduit, intermediate metal conduit, liquid tight flexible conduit, flexible metallic tubing, flexible metal conduit, electrical nonmetallic tubing, electrical metallic tubing, underfloor raceways, cellular, cellular concrete floor raceways, cellular metal floor raceways, surface raceways, wireways, and busways. NOTE: Cable tray is not considered a type of raceway.
rack	An open structure for mounting electrical and electronic equipment.
rack unit	The modular unit on which panel heights are based. One rack unit is 45 mm (1.75 in) and is expressed in units of <i>U</i> or <i>RU</i>
radio frequency interference	Electromagnetic interference within the frequency band for radio transmission.
raised floor	See <i>access floor</i>.
record	A collection of detailed information related to a specific element of the infrastructure.
record drawing	A plan, on paper or electronically, that graphically documents and illustrates the installed infrastructure in a building or portion thereof. Also known as an <i>as-built drawing</i>.
redundancy	Providing secondary components that either become instantly operational or are continuously operational so that the failure of a primary component will not result in mission failure. See also <i>component redundancy</i>.
reliability	The probability that a component or system will perform as intended over a given time period.
remote power panel	A power distribution cabinet downstream from a PDU or UPS, typically containing circuits and breakers, without a transformer, located near the load.
report	Presentation of a collection of information from various records.
resistively grounded power system	A method of grounding in which the system is grounded through impedance, the principle element of which is resistance.
return loss	A ratio, expressed in dB, of the power of the outgoing signal to the power of the reflected signal. When the termination (load) impedance does not match (equal) the value of the characteristic impedance of the transmission line, some of the signal energy is reflected back toward the source and is not delivered to the load; this signal loss contributes to the insertion loss of the transmission path and is called return loss.
return on investment	The ratio of money gained or lost on an investment relative to the amount of money invested.
ring topology	A physical or logical network topology in which nodes are connected in a point-to-point serial fashion in an unbroken circular configuration. Each node receives and retransmits the signal to the next node.
riser	(1) Vertical sections of cable (e.g., changing from underground or direct-buried plant to aerial plant). (2) The space used for cable access between floors.
riser cable	Communications cable that is used to implement backbones located on the same or different floors.
risk	The likelihood that a threat agent will exploit a vulnerability, creating physical or technological damage.
risk management	The process of identifying risks and developing the strategy and tactics needed to eliminate, mitigate, or manage them.

scan	Within local area networks, a nonintrusive analysis technique that identifies the open ports found on each live network device and collects the associated port banners found as each port is scanned. Each port banner is compared against a table of rules to identify the network device, its operating system, and all potential vulnerabilities.
screen	A thin metallic wrapping (e.g., aluminum foil) used to isolate cable pairs from interference.
screened twisted-pair cable	A balanced twisted-pair cable with one or more pairs of individual unscreened balanced twisted-pairs having an overall foil screen shield and may contain a drain wire. The entire assembly is covered with an insulating sheath (cable jacket). It may also be called <i>foil twisted-pair cable</i> .
secondary side	The low-voltage side of the electrical power service transformer, the load side of the UPS, the load side of the PDU transformer, or the output side of the static switch.
seismic snubber	Mechanical devices, when anchored to the building structure and placed around vibration-isolated equipment, are intended to limit motion by containing the supported equipment. Snubbers are designed for use in locations subject to earthquakes, high winds, or other external forces that could displace resiliently supported equipment.
separately derived system	A premises wiring system in which power is derived from a source of electric energy or equipment other than a service. Such systems have no direct electrical connection, including a solidly connected grounded circuit conductor, to supply conductors originating in another system.
service gallery	Space adjacent to a computer room where electrical and mechanical equipment that supports the computer room may be located.
service provider	The operator of any service that furnishes telecommunications content (transmissions) delivered over access provider facilities.
sheath	See <i>cable sheath</i> .
shield	A metallic sheath (usually copper or aluminum) applied over the insulation of a conductor or conductors for the purpose of providing means for reducing electrostatic coupling between the conductors.
shielded twisted-pair cable	Cable made up of balanced metallic conductor pairs, each pair with an individual shield. The entire structure is then covered with an overall shield or braid and an insulating sheath (cable jacket).
simplicity	The application of irreducible functionality to achieve the intended goal with the corresponding understanding that complexity introduces additional risk.
single-mode optical fiber	An optical fiber that carries only one path (mode) of light.
smoke	Visible products of combustion prior to and concurrent with a fire.
solidly grounded	Connected to ground without inserting any resistor or impedance device.
space (telecommunications)	An area whose primary function is to house the installation and termination of telecommunications equipment and cable (e.g., MDA, IDA, HDA, TR, entrance room).
splice	A joining of conductors, which is meant to be permanent.
star topology (telecommunications cabling)	A topology in which telecommunications cables are distributed from a central point.
static switch	See <i>transfer switch, static</i> .
storage area network	A high-speed network of shared storage devices. A SAN permits storage devices attached to the SAN to be used by servers attached to the SAN.

structural barrier	Defined as something that physically deters or prevents unauthorized access, movement, destruction, or removal of data center assets.
supervisory control and data acquisition system	A control system composed of programmable logic controllers (PLCs), data input to the PLCs, custom software, and electrically operated circuit breakers in the distribution gear. All these combine to form a unique system that allows automatic operation and monitoring of the electrical system through control panel workstations.
supplementary bonding grid	A set of conductors or conductive elements formed into a grid or provided as a conductive plate and becomes part of the bonding network to which it is intentionally attached.
suppression, fire	The means of extinguishing an active fire.
surge protection device	A protective device for limiting transient voltages by diverting or limiting surge current. It has a nonlinear voltage-current characteristic that reduces voltages exceeding the normal safe system levels by a rapid increase in conducted current. NOTE: A surge protection device may also be known as a <i>voltage limiter</i>, <i>overvoltage protector</i>, <i>(surge) arrestor</i>, or <i>transient voltage surge suppressor (TVSS)</i>.
switch (device)	(1) A device designed to close, open, or both one or more electrical circuits. (2) A mechanical device capable of opening and closing rated electrical current. (3) A device for making, breaking, or changing the connections in an electric circuit. (4) An electronic device connected between two data lines that can change state between open and closed based upon a digital variable. NOTE: A switch may be operated by manual, mechanical, hydraulic, thermal, barometric, or gravitational means or by electromechanical means not falling with the definition of <i>relay</i>.
switch (equipment)	A voice communications device that uses switching technology to establish and terminate calls.
switch (network)	A network access device that provides a centralized point for LAN communications, media connections, and management activities where each switch port represents a separate communications channel.
switchboard	A single-panel frame or assembly of panels, typically accessed from the front, containing electrical disconnects, fuses, and circuit breakers used to isolate electrical equipment. Switchboards are typically rated 400 A to 5,000 A and are characterized by fixed, group-mounted, molded case, or insulated case circuit breakers, but they may include draw-out circuit breakers and usually require work on de-energized equipment only.
switchgear	An electrical enclosure, typically having both front and rear access, containing overcurrent protective devices, such as fuses and circuit breakers, used to isolate electrical equipment. Switchgear is typically rated 800 A to 5,000 A and is characterized by segregated, insulated-case, or low-voltage power circuit breakers, usually draw-out, and frequently contains monitoring and controls as well as features to permit addition or removal of switching devices on an energized bus.
switching	(1) The action of opening or closing one or more electrical circuits. (2) The action of changing state between open and closed in data circuits. (3) A networking protocol in which a station sends a message to a hub switch, which then routes the message to the specified destination station.
system redundancy	A strategy for increasing reliability by providing redundancy at the system level.
targeted availability	A positive expression of allowable maximum annual downtime
technological events	Technological incidents, including hazardous material release, explosion/fire, transportation accident, building/structural collapse, power/utility failure, extreme air pollution, radiological accident, dam/levee failure, fuel/resource shortage, strike, business interruption, financial collapse, and communication failure.

telecommunications	Any transmission, emission, and reception of information (e.g., signs, signals, writings, images, sounds) by cable, radio, optical, or other electromagnetic systems.
telecommunications bonding backbone	A conductor that interconnects the telecommunications main grounding busbar (TMGB) to the telecommunications grounding busbar (TGB).
telecommunications entrance point	See <i>entrance point (telecommunications)</i> .
telecommunications entrance room or space	See <i>entrance room or space (telecommunications)</i> .
telecommunications equipment room	See <i>equipment room (telecommunications)</i> .
telecommunications infrastructure	See <i>infrastructure (telecommunications)</i> .
telecommunications main grounding busbar	A busbar placed in a convenient and accessible location and bonded by means of the bonding conductor for telecommunications to the building service equipment (power) ground.
telecommunications media	See <i>media (telecommunications)</i> .
telecommunications room	A telecommunications space that differs from equipment rooms and entrance facilities in that this space is generally considered a floor-serving or tenant-serving (as opposed to building- or campus-serving) space that provides a connection point between backbone and horizontal cabling.
telecommunications space	See <i>space (telecommunications)</i> .
termination	The physical connection of a conductor to connecting hardware.
test procedures	The detailed, sequential steps to set the procedures and conditions necessary to test the system functionality.
threats	The agents by which damage, injury, loss, or death can occur. Threats are commonly classified as originating from temperature extremes, liquids, gases, projectiles, organisms, movement, or energy anomalies. See also <i>vulnerability</i> .
topology	The physical or logical arrangement of a system.
total facility power	The power dedicated solely to the data center, including all infrastructure equipment that supports the information technology equipment (ITE) such as power delivery components, cooling and environmental control system components, computer network and storage nodes, and miscellaneous other components necessary for the operation of the data center.
transfer switch, automatic	Self-acting equipment that transfers a load from one power source to an alternate power source through the use of electrically operated mechanical moving components, (e.g., switch, breaker). NOTE: Automatic transfer switches with open transition transfer times exceeding 20 milliseconds will result in a reboot or restart cycle of any loads with electronics or controls utilizing switch-mode power supplies. Automatic transfer switches with open transition transfer times of 16 milliseconds or less will not result in a reboot or restart cycle of any loads with electronics or controls utilizing switch-mode power supplies.
transfer switch, non-automatic	Equipment that enables an operator to transfer a load from one power source to an alternate power source through the use of manually operated mechanical moving components (e.g., switch or breaker). NOTE: The transfer time consists of an open transition greater than 20 milliseconds, which results in a reboot or restart cycle of any loads with electronics or controls (also commonly referred to as manual transfer switch).

transfer switch, static	Self-acting equipment that transfers a load from one power source to an alternate power source through the use of semiconductor devices (e.g., silicon controlled rectifiers). NOTE: Because there are no mechanical moving components the transfer time is typically less than 6 milliseconds, which will not result in a reboot or restart cycle of any loads with electronics or controls that utilize switch-mode power supplies.
tree topology	A LAN topology that has only one route between any two nodes on the network. The pattern of connections resembles a tree or the letter “T”.
trunk cables	Cables bundled together to form a single unit.
trunk cabling assemblies	A type of bundled cable consisting of two or more preconnectorized cabling links of the same or different types cabling media, which may either be covered by one overall sheath or be continuously bound together to form a single unit.
trunking	(1) A combination of equipment, software and protocols that allows many clients to share relatively few telecommunications channels as opposed to each channel being dedicated to an individual client. In radio systems, the channels are frequencies and repeaters. In wireline systems, the channels are copper wire pairs or fiber optic strands. Trunking greatly expands the efficiency of resource usage, making limited resources (channels) available to many more clients. (2) In networking protocols, combining (multiplexing) frames from multiple VLANs across a single physical link (trunk) by using an encapsulation protocol such as IEEE 802.1Q. The protocol modifies the frame to identify the originating VLAN before the frame is placed on the trunk. The reverse process occurs at the receiving end of the trunk.
uninterruptible power supply	A system that provides a continuous supply of power to a load, utilizing stored energy when the normal source of energy is not available or is of unacceptable quality. A UPS will provide power until the stored energy of the system has been depleted or an alternative or the normal source of power of acceptable quality becomes available.
uninterruptible power supply, rotary	A UPS consisting of a prime mover (such as an electric motor), a rotating power source (such as an alternator), a stored energy source (such as a battery), associated controls and protective devices, and a means of replenishing the stored energy (such as a rectifier/charger).
uninterruptible power supply, static	A UPS consisting of nonmoving (solid state) components, usually consisting of a rectifier component, an inverter component, a stored energy component, associated controls and protective devices.
unshielded twisted-pair	A balanced transmission medium consisting of a pair of electrical conductors twisted to provide a level of immunity to outside electrical interference without the use of metallic shielding. Typical construction has four such pairs of conductors contained with a common outer sheath.
uplink	Referring to data processing, a connection between layers (switches) in a hierarchical network. Uplinks are usually optical fiber links configured on Gigabit Ethernet (GbE) ports. (Fast Ethernet uplinks can also be configured using optical fiber or balanced twisted-pair cabling). An uplink can be referred to as a <i>trunk</i> .
uptime	The period of time, usually expressed as a percentage of a year, in which the information technology equipment (ITE) is operational and able to fulfill its mission.
validation	The establishment of documented evidence that will provide a high degree of assurance the system will consistently perform according to the design intent.
verification	The implementation and review of the tests performed to determine if the systems and the interface between systems operates according to the design intent.

virtual local area network	A networking protocol that allows the overlay of logical topologies onto a separate physical topology. VLANs provide traffic separation and logical network partitioning. A VLAN forms a broadcast domain and, to communicate between VLANs, a routing function is required.
vulnerability	A physical, procedural, or technical weakness that creates an opportunity for injury, death, or loss of an asset. See also <i>threats</i> .
wire	An individual solid or stranded metallic conductor.
wire management	See <i>cable management</i> .
wireless	The use of radiated electromagnetic energy (e.g., radio frequency and microwave signals, light) traveling through free space to convey information.
X-O bond	The point in the electrical system where a separately derived ground is generated. This point generates a power carrying neutral conductor or 4 th wire for the electrical power system. The X-O bond point is typically used as the ground reference for the downstream power system.
XaaS	A generic representation of services provided by external vendors and data centers. Examples of usages include Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).
zero U space	A space for mounting accessories in cabinets that does not consume any rack mount spaces, typically between the side panel and the sides of equipment mounted in the rack unit mounting space.
zone distribution area	A space in a computer room where a zone outlet or a consolidation point is located.
zone distributor	Distributor used to make connections between the main distribution cabling subsystem, zone distribution cabling subsystem, network access cabling subsystem, and cabling subsystems specified in ISO/IEC 11801 or EN 50173-1 and active equipment (CENELEC EN 50173-5 and ISO/IEC 24764). Equivalent to the horizontal cross-connect (HC) in ANSI/TIA-942-A.
zone outlet	A connecting device in the zone distribution area terminating the horizontal cable enabling equipment cord connections to the equipment distribution area.

4.2 Acronyms and Abbreviations

Abbreviations and acronyms, other than in common usage, are defined below.

24/7	twenty-four hours a day, seven days a week	DCIE	data center infrastructure efficiency
A/E	architectural/engineering	DCIM	data center infrastructure management
AC	alternating current	DP	data processing; distribution panel
ACEG	alternating current equipment grounding conductor	DS-1	digital signal level 1
ACRF	attenuation to crosstalk ratio, far-end	DS-3	digital signal level 3
ADA	Americans with Disability Act	DSX	digital signal cross-connect
AFEXT	alien far-end crosstalk	DWDM	dense wave division multiplexer
AHJ	authority having jurisdiction	E-1	European trunk level 1
AHU	air handling unit	E-3	European trunk level 3
AISS	automated information storage system	EAC	electronic access control
ANEXT	alien near-end crosstalk	EAP	electronic asset program
APC	angle physical connector; angle polished connector	EDA	equipment distribution area
ASTS	automatic static transfer switch	EGC	equipment grounding conductor
ATM	asynchronous transfer mode	EGS	equipment grounding system
ATS	automatic transfer switch	EMD	equilibrium mode distribution
AWG	American wire gauge	EMI	electromagnetic interference
BAS	building automation system	EMS	energy management system
BCT	bonding conductor for telecommunications	EO	equipment outlet
BMS	building management system	EPMS	electrical power management system
BN	bonding network	EPO	emergency power off
BNC	Bayonet Neill-Concelman	ESCON	enterprise system connection
CATV	community antenna television	ESD	electrostatic discharge
CBN	common bonding network	ESS	electronic safety and security
CBRNE	chemical, biological, radiological, nuclear, or explosive	EU	European Union
CCTV	closed-circuit television	F/UTP	foil screened unshielded twisted-pair
CD	construction document	FDDI	fiber distributed data interface
CFD	computational fluid dynamics	FE	Fast Ethernet
CO	central office	FICON	fiber connection
CP	consolidation point; critical power	GbE	Gigabit Ethernet
CPE	customer premises equipment	GE	grounding equalizer
CPU	central processing unit	GEC	grounding electrode conductor
CPVC	chlorinated polyvinyl chloride	GES	grounding electrode system
CRAC	computer room air conditioner; computer room air conditioning	GFCI	ground fault circuit interrupter
CRAH	computer room air handler; computer room air handling	GUI	graphical user interface
CM	construction management	HC	horizontal cross-connect
DC	direct current	HCP	horizontal connection point
DCEG	direct current equipment grounding conductor	HDA	horizontal distribution area
		HEPA	high-efficiency particulate air
		HMI	human machine interface
		HVAC	heating, ventilating, and air conditioning
		IBN	isolated bonding network
		IC	intermediate cross-connect
		IDC	insulation displacement contact

IIM	intelligent infrastructure management	PSAFEXT	power sum alien far-end crosstalk
ISDN	integrated services digital network	PSANEXT	power sum alien near-end crosstalk
ISP	inside plant	PSNEXT	power sum near-end crosstalk
IT	information technology	PSU	power supply unit
ITE	information technology equipment	PUE	power usage effectiveness
KVM	keyboard/video/mouse	PVC	polyvinyl chloride
LAN	local area network	QoS	quality of service
LDP	local distribution point	RAID	redundant array of independent (or inexpensive) disks
LED	light-emitting diode	RC	room cooling
LPS	lightning protection system	RCI	rack cooling index
LSZH	low smoke zero halogen	RF	radio frequency
MC	main cross-connect	RFI	radio frequency interference
MD	main distributor	RFP	request for proposal
MDA	main distribution area	RH	relative humidity
MDF	main distribution frame	RJ48X	registered jack with individual 8-position modular jacks with loopback
MEGB	main electrical grounding busbar	ROI	return on investment
MERV	minimum efficiency reporting value	RPP	remote power panel
mesh-BN	mesh-bonding network	RU	rack unit
MIB	management information base	SAN	storage area network
MPLS	multiprotocol label switching	SBG	supplementary bonding grid
MTBF	mean time between failures	SC	supplemental cooling
MTTR	mean time to repair	SCADA	supervisory control and data acquisition
NC	noise criterion	SCSI	small computer system interface
NEBS	network equipment building system	ScTP	screened twisted-pair
NEC®	National Electrical Code®	SD	schematic design
NEXT	near-end crosstalk	SDH	synchronous digital hierarchy
Ni-Cd	nickel-cadmium	SNMP	simple network management protocol
NRTL	nationally recognized testing laboratory	SONET	synchronous optical network
O&M	operation and maintenance	SPC	single point of connection
OC	optical carrier	SPD	surge protection device
OLTS	optical loss test set	SPG	single point ground
OSP	outside plant	STM	synchronous transport module
OTDR	optical time domain reflectometer	STP	shielded twisted-pair
PBX	private branch exchange	STS	static transfer switch
PC	personal computer	T-1	trunk level 1
PD	propagation delay	T-3	trunk level 3
PDU	power distribution unit	TBB	telecommunications bonding backbone
PLC	programmable logic controller	TGB	telecommunications grounding busbar
PM	preventive maintenance	TLE	telecommunications load equipment
PoE	power over Ethernet	TMGB	telecommunications main grounding busbar
POU	power outlet unit	TR	telecommunications room
PPE	personnel protection equipment	TVSS	transient voltage surge suppression
PQM	power quality monitoring	UPS	uninterruptible power supply
PSAACRF	power sum attenuation to alien crosstalk ratio at the far end	UTP	unshielded twisted-pair
PSACRF	power sum attenuation to crosstalk ratio, far-end		

VBIED	vehicle borne improvised explosive device	VLAN	virtual local area network
VCSEL	vertical cavity surface emitting laser	VoIP	voice over Internet protocol
VFD	voltage and frequency dependent, variable frequency drive	VPN	virtual private network
VFI	voltage/frequency independent	VRLA	valve-regulated lead-acid
VI	voltage independent	VSS	video surveillance system
VLA	vented lead-acid	WAN	wide area network
		ZD	zone distributor
		ZDA	zone distribution area

4.3 Units of Measurement

The units of measurement used in this standard are metric. Approximate conversions from metric to United States customary units are provided in parentheses, e.g., 100 millimeters (4 inches).

Units of measurement used in this standard are defined below:

°C	degree Celsius	kPa	kilopascal
°F	degree Fahrenheit	kVA	kilovolt-ampere
μm	micrometer	kW	kilowatt
A	ampere	lb	pound
BTU	British thermal unit	lbf	pound-force
dB	decibel	lbf/ft ²	pound force per square foot
fc	foot-candle	lx	lux
ft	foot	m	meter
ft ²	square foot	m ²	square meter
ft/min	foot per minute	m ³ /min	cubic meter per minute
ft ³ /min	cubic foot per minute	m/s	meter per second
ft/s	foot per second	Mb/s	megabit per second
Gb/s	gigabit per second	MCM	thousand circular mils
GHz	gigahertz	MHz	megahertz
gpd	gallons (U.S.) per day	MHz•km	megahertz kilometer
gpm	gallons (U.S.) per minute	mm	millimeter
h	hour	mph	mile per hour
hr	hour	MW	megawatt
Hz	hertz	N	newton
in	inch	nm	nanometer
in Hg	inches of mercury (pressure)	Pa	pascal (pressure)
in WC	inches of water column	psi	pound per square inch (pressure)
in WG	inches water gauge	RU	rack unit
K	kelvin	V	volt
kb/s	kilobit per second	VA	volt-ampere
kg	kilogram	V _{AC}	volt alternating current
kg/m ²	kilogram per square meter	V _{DC}	volt direct current
kHz	kilohertz	W	watt
km	kilometer	W/ft ²	watt per square foot
km/h	kilometer per hour	W/m ²	watt per square meter
kN	kilonewton		

This page intentionally left blank

5 Site Selection

5.1 Introduction

This section outlines the considerations that should be reviewed and provides recommendations when selecting a location for a data center, whether the location is for a “green field” site that involves the construction of a new data center, reviewing the location of an existing building that will function as a data center, or the ranking of data centers when considering closure or consolidation.

NOTE: When evaluating the suitability of existing buildings and data centers, additional areas (e.g., building structure and architecture, mechanical and electrical systems) should be considered and can be found in other sections of this standard.

The guidance and examples provided are applicable in a wide range of jurisdictions and locations; however, when determining the suitability of a specific site, it is recommended that all applicable local and region guidelines and codes are also reviewed prior to final selection.

5.2 Site Evaluation

5.2.1 General Requirements

The suitability of a site shall be determined by a site survey and evaluation and a risk analysis.

5.2.2 General Recommendations

An existing site survey should only be referred to if the documents are not older than 6 months. An existing risk analysis for a specific site should only be referred to if it was conducted for a similar objective.

A risk assessment should include the following hazards to be evaluated:

- Natural hazards (e.g., geological, meteorological, and biological)
- Human-caused events (e.g., accidental and intentional)
- Technologically caused events (e.g., accidental and intentional)

NOTE: NFPA 1600, ISO 22301, and ISO 31000 contain additional information on risk analysis and business continuity planning.

5.2.3 Cost Evaluation Recommendations

The site selection process should include a detailed analysis of all the costs associated with any particular location.

Costs that should be considered when comparing available sites are listed below:

- One-time costs that may be significant such that any one may drive the site selection process are:
 - Real estate costs.
 - Local tax incentives.
 - Environmental assessment consulting costs.

This could include an environmental impact study if wetland or other environmentally sensitive areas are impacted or if the site has any contaminants present. Some sites may require a significant effort to develop the assessment and attend required meetings with the AHJ.
 - Cost to bring adequate utilities infrastructure (e.g., power, water, sewer, gas, telecommunications) to the site in order to support the critical load, both initial and future anticipated growth.
 - Cost to provide redundant utilities (e.g., power, water, gas, telecommunications) to the site as required.

Determine the additional costs associated with redundant site utilities and any impact that the implementation may have on the schedule. Costs for diverse underground service from an alternate access provider office may be quite high.
 - Demolition costs for any existing structures; site preparation costs.
- Cost and availability of permanent telecommunications service and temporary telecommunications services to support the migration of data from existing data center(s).

<List continues on next page>

- Costs associated with the temporary circuits for movement of data, including:
 - Consider temporary telecommunications circuits that may be needed to support the migration of data from the existing data center(s) to the new data center.
 - Cost of relocation of systems into the new data center:
Develop a high-level move strategy so that appropriate funds can be allocated for the move of systems and networks into the new data center. Identify any needs for consultants, temporary labor, media, network, server, and storage hardware to support the move and their associated costs.
 - Impact of data center constructability:
Determine if there are any conditions at a particular site that will affect the constructability of the new data center. A particular site may require a longer approval, permitting, or construction schedule. An extended schedule may affect feasibility because of decommissioning requirements of the existing data center.
- Recurring costs that will have long-term effects on the feasibility of the proposed site:
 - Usage costs for utility services (power, water, sewer, gas)
 - Cost of telecommunications services
 - Prevailing wage for skilled labor in local area
 - Lease costs
 - Taxes
- Intangible costs:
 - Proximity to other corporate facilities (travel time)
 - Proximity of skilled staff

5.2.4 Existing Facilities Requirements

If the data center is moving into an existing building, determine if the building is up to current code and industry standards. It may actually be less desirable to move into a building with an existing electrical and mechanical plant as it may be unsuitable for use in the data center. The existing systems may need to be removed and replaced at considerable expense.

5.3 Natural Hazards

5.3.1 Introduction

While many things can be determined to be a “natural hazard,” this section covers specifically those natural events that are typically major adverse events and may be known as “natural disasters.”

5.3.2 General Requirements

The risk from natural hazards identified in this section shall always be evaluated and considered during the site selection process.

5.3.3 Seismic Activity

5.3.3.1 Introduction

Seismic activity (earthquakes) is typically associated with the presence of a geological fault or volcano. Earthquakes can range from a low-level vibration lasting less than a second to a catastrophic event lasting over 20 seconds, severely damaging or destroying structures in the event area.

5.3.3.2 Recommendations

Seismically active areas should be avoided whenever possible. If this is not possible, appropriate seismic equipment supports and structures shall be provided to meet or exceed the requirements of the local AHJ.

In a seismically active area, the equipment within the data center, including the ITE cabinets and racks, should be designed for the level of seismic activity that the data center is designed to survive and have corresponding structural anchorage. Additionally, the building will have higher structural requirements. If one is not already required by the AHJ, consider working with a professional structural engineer to meet the appropriate seismic criteria of the data center facility.

Refer to seismic charts and other seismic activity information for the specific proposed data center site. An example of a global seismic activity map is shown in Figure 5-1.

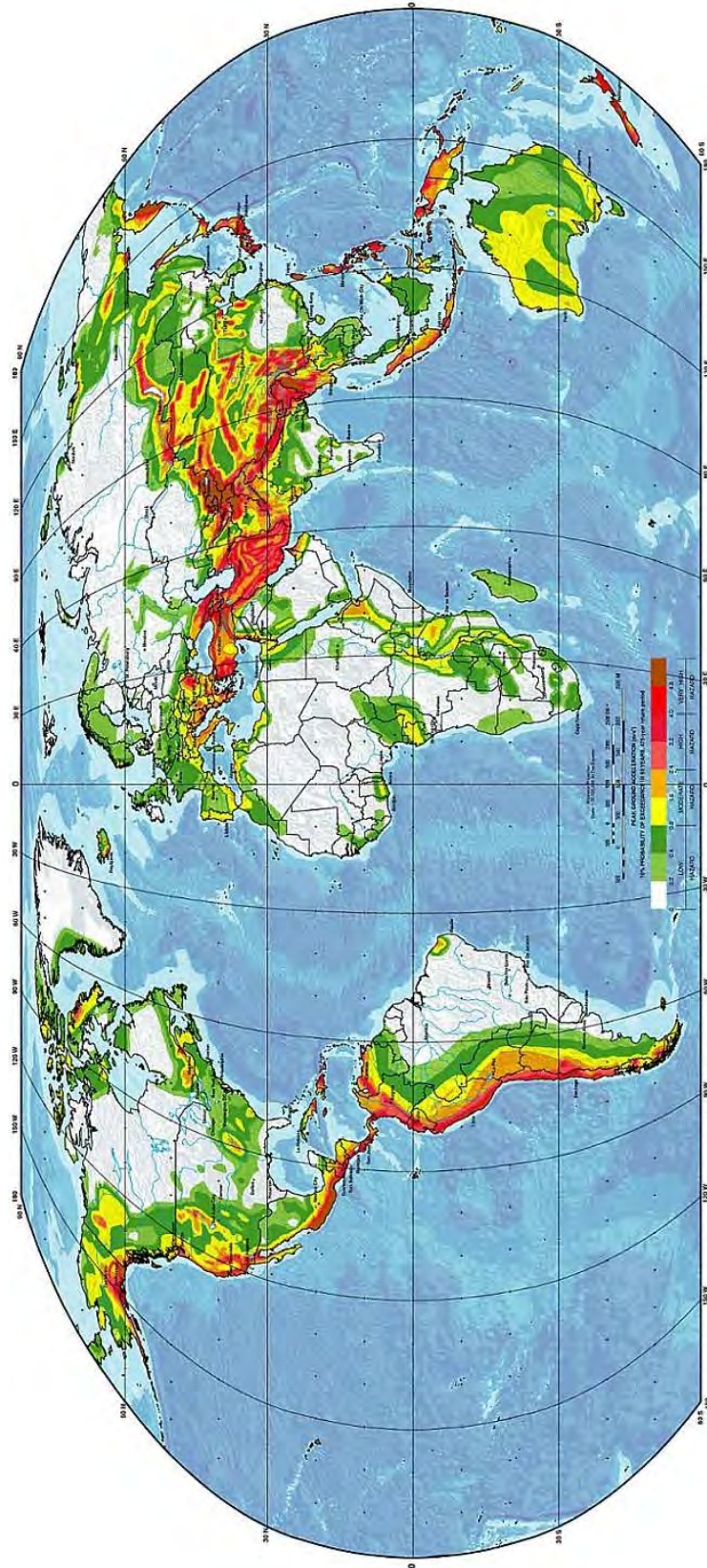


Figure 5-1
Global Seismic Hazard Map

5.3.4 Volcanic Activity

5.3.4.1 Introduction

Volcanoes are typically located on or near a geological fault. However, volcanoes pose additional risk from the event of an eruption and subsequent lava flow, ash fall, lahars, or flooding.

5.3.4.2 Recommendations

Data centers should be located outside the immediate risk (buffer) area of an active volcano. Hazard zones for each volcano should be obtained and evaluated. (See Figure 5-2 for an example.)

5.3.5 Wildfire

5.3.5.1 Introduction

Wildfires can easily spread to 6,000 hectares (15,000 acres) or larger. While a site may not be in immediate danger, large wildfires that occur 80 km (50 mi) or farther away from the site can affect an access provider's transmission infrastructure being used by the data center.

Wildfires typically occur away from urban environments. However, depending on the topography of the area and the amount of other development in the area, some sites are susceptible to operational interruption or structural damage from wildfires.

5.3.5.2 Recommendations

Data centers should not be placed on the edge of urban development or near protected natural areas. Data center sites within areas that have historical wildfire events should review all access providers' records for service disruptions because of wildfires.

If a data center is to be placed within an area with moderate to high wildfire risk, redundant access routes should be made available to provide both data center operators and fire suppression crews access to the site. Security and disaster recovery plans should detail procedures for evacuation and continued data center operation in event of required wildfire evacuation.

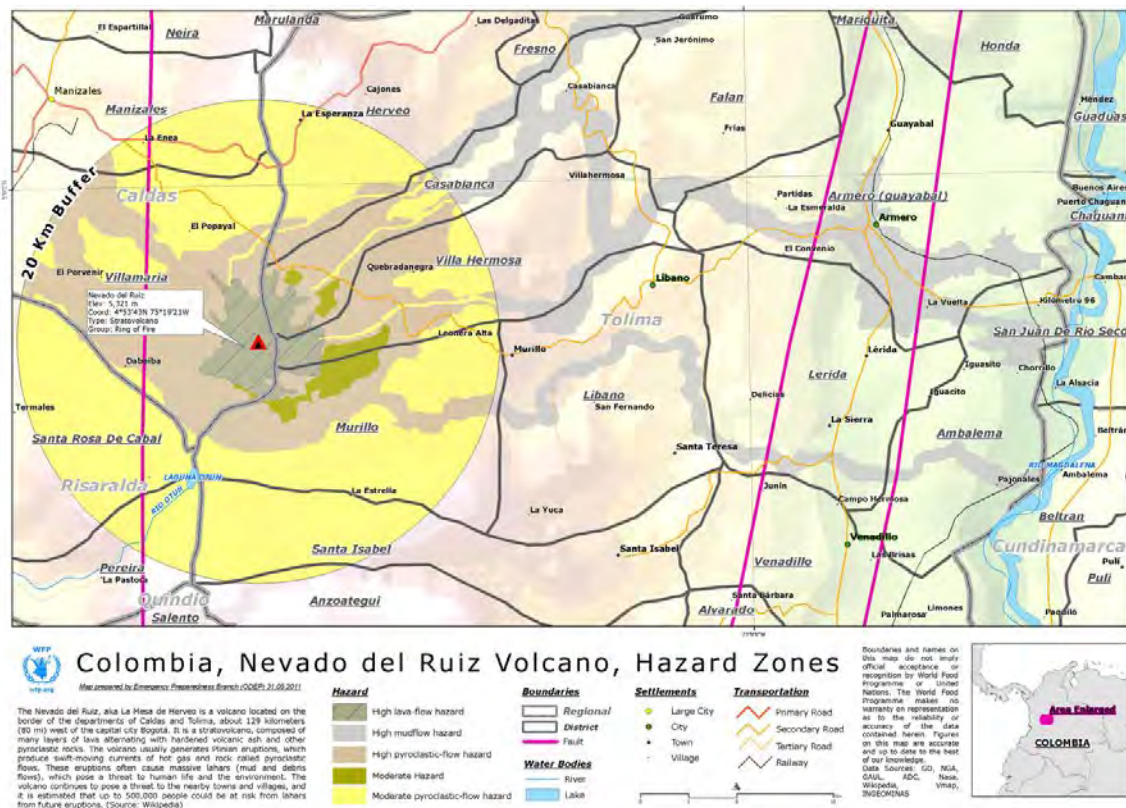


Figure 5-2
Example Volcano Hazard Map

5.3.6 Flood Plains

5.3.6.1 Introduction

Flooding may occur in a number of areas and may occur in areas not known for significant annual rain or snowfall.

5.3.6.2 Recommendations

The site should be free of flood risk from river flood plain proximity, tidal basin proximity, dam failure, tsunami, or levee failure. The site should not be within the flood hazard and tsunami inundation area as defined in the *IBC*, be within 91 m (300 ft) of a 500-year flood hazard area, or be less than 3 m (10 ft) above the highest known flood level. The site should also have multiple access roads with elevations above the flood recommendations along their entire route.

NOTE: Some locations may warrant a site specific flood study.

An example of available flood information is Figure 5-3, which shows global flood risk. Information is also available on a region or country basis.

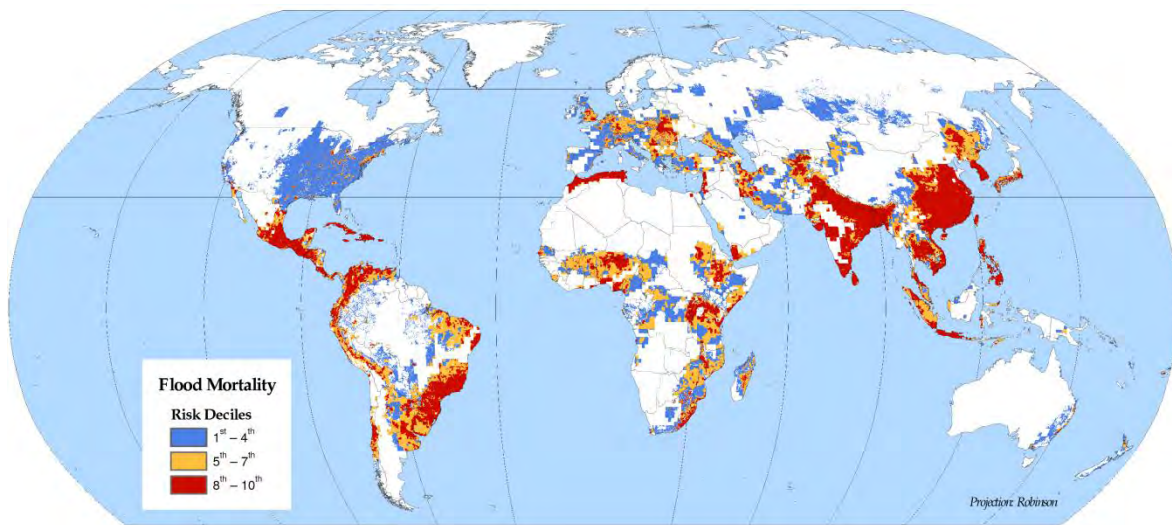


Figure 5-3
Global Flooding Hazard

5.3.7 Wind

5.3.7.1 Introduction

While wind is prevalent in every area of the Earth, extreme winds because of storms (e.g., tornado, hurricane, cyclone, derechos) can affect a data center's operation.

5.3.7.2 Recommendations

The most desirable location should be an area with winds less than or equal to 54 m/s (120 mph) per ASCE 7. When business drivers dictate that a data center be located in an area with greater wind velocity, specific detail in the "hardening" of the facility should be incorporated into the design.

Class 2 and lower data centers should be designed to meet Risk Category I (USA) or designed to withstand at a minimum wind speeds of 16 km/h (10 mph) above the highest 100 year mean recurrence interval wind speed. Class 3 data centers should be designed to meet Risk Category II (USA) or designed to withstand at a minimum wind speeds of 32 km/h (20 mph) above the highest 100 year mean recurrence interval wind speed, and Class 4 data centers should be designed to meet Risk Category III-IV (USA) or designed to withstand at a minimum wind speeds of 48 km/h (30 mph) above the highest 100 year mean recurrence interval wind speed.

Refer to wind charts and other wind activity information for the specific proposed data center site. While wind/windstorm risk maps are typically specific to region or country, Figure 5-4 is an example of a global tornado risk map.

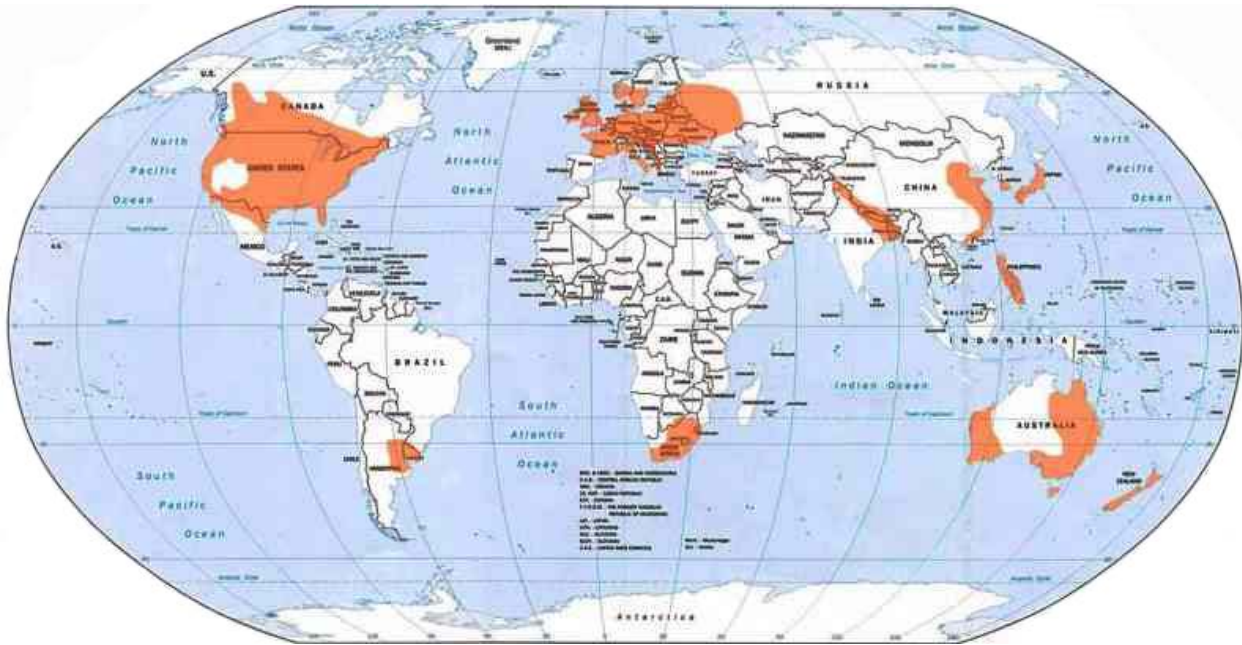


Figure 5-4
Global Tornado Risk Areas

5.4 Natural Environment

5.4.1 Introduction

The natural environment has its own set of risks that while they may not cause the potential destruction of that of an earthquake or hurricane, still have the potential to cause adverse effects to a data center's construction or operation.

5.4.2 Ground Stability

5.4.2.1 Landslides

5.4.2.1.1 Introduction

Landslides occur when the stability of the slope changes from a stable to an unstable condition. A change in the stability of a slope can be caused by a number of factors. Landslides do not need a dramatic difference of elevations as a landslide can occur over a seemingly flat area because of the ground structure underneath.

5.4.2.1.2 Recommendations

For new building locations, the suitability of the site should be verified by current documents, recent geological records, or by appropriate analytical measures.

5.4.2.2 Soil Stability

5.4.2.2.1 Introduction

While the most dramatic effect of insufficient ground stability is the formation of sinkholes, even minimal instability can cause a building to not uniformly "settle", leading to structure issues and damage.

5.4.2.2.2 Requirements

The sub terrain shall be suitable to support the loads of the facility. The suitability of the site shall be verified by current documents or by appropriate analytical measures.

5.4.2.2.3 Recommendations

The following criteria should be used in determining a site's suitability:

- Avoid the potential for quick, unstable, or expansive soils.
- Ensure that there is no known subsurface contamination from either on-site hazardous waste storage or other adjacent site.
- Ensure that there is no potential of underlying solution-formed cavities common in limestone formations or the source of potential sinkhole problems.

Consider working with a professional geotechnical engineer to meet the appropriate criteria of the data center and to provide a formal written geotechnical report.

5.4.3 Groundwater

5.4.3.1 Introduction

Groundwater is water located beneath the earth's surface in soil pore spaces and in the fractures of rock formations. The depth at which soil pore spaces or fractures and voids in rock become completely saturated with water is called the water table. Groundwater is recharged from, and eventually flows to, the surface naturally; natural discharge often occurs at springs and seeps and can form oases or wetlands.

5.4.3.2 Recommendations

The site should have a water table that is as low as possible; it should be below the utility ducts and below the lowest level of the building at a minimum.

If the data center is a “slab on grade”, then placing it at the top of a hill or in a relatively flat topographical area should minimize ground water issues.

If the building has one or more subgrade floors or is located at the bottom of a hill, additional efforts may be required to protect the data center from seepage or the effects of seasonal variances in the water table. If the data center is located at the bottom of a hill, there should be great concern for ground water issues.

Refer to ground water charts and other ground water activity information, such as shown in Figure 5-5, for the specific data center site.

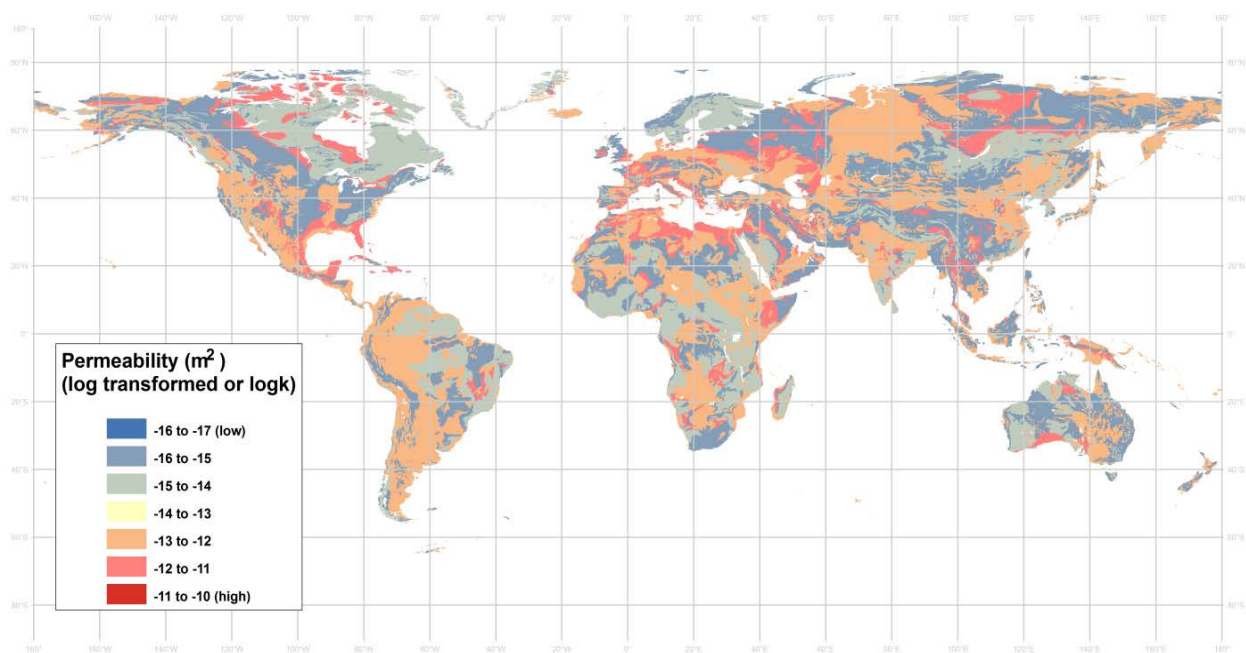


Figure 5-5
Example Ground Permeability Chart

5.4.4 Lightning

5.4.4.1 Recommendations

Sites with a flash rate of 10 or less are preferred.

The type and duration of service provider failures should be researched for potential site locations with a flash rate greater than 1 and integrated into the overall site selection and design criteria.

5.4.4.2 Additional Information

Areas with a flash rate of 0.6 or less are typically seen as “lightning free”. However, lightning may occur at almost any point on the globe, and a single lightning flash has the potential to cause a downtime event.

Examples of lightning flash data can be found in Figure 5-6.

5.4.5 Air Quality

5.4.5.1 Intake Recommendations

Air quality issues should be considered for the data center fresh air intake and for external mechanical components like cooling towers and heat exchangers (e.g., ashes, sand) as well as anything that may be emitted from the site. Fresh air intake requirements are usually regulated by the local AHJ. Provide appropriate air intake filtration systems as required.

When data centers must be located in densely populated areas or metropolitan areas, consider the effects of noise and emissions from the data center exhausts on neighbors and surroundings. Although usually regulated, it is common to have restaurants, dry cleaners, and other similar businesses requiring venting of chemicals and contaminants into the immediate environment. Special air intake filtration systems may be required for the data center in addition to any regulations.

5.4.5.2 Emission Recommendations

An area with clean air quality is preferred so that emission of gases and particles does not cause a new air quality problem or worsen an existing problem.

In areas with existing air quality problems, regulations may be very stringent regarding emissions produced from fossil fuel consumption.

Ensure that generator run time permitting documents are issued in a timely manner to the jurisdiction overseeing air quality control and other local environmental authorities. In most cases, annual operation hours will be restricted and compliance must be verified.

If the owner wants to consider cogeneration of electricity, there may be stricter air quality requirements and special permits required.

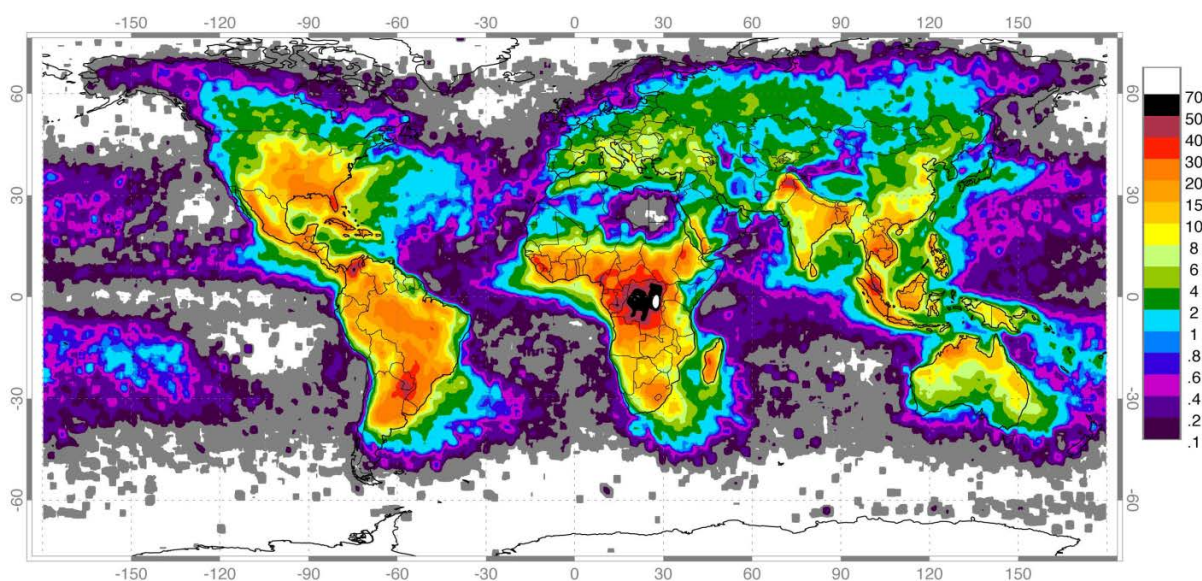


Figure 5-6
Example Map of Lightning Flash Data

5.4.6 Noise

5.4.6.1 Introduction

Wind will carry sound long distances. Even the slightest breeze can carry the sound of a facility well beyond the property line.

5.4.6.2 Recommendations

It is recommended to verify acceptable noise levels at the property line and determine the noise levels produced by equipment.

Critical silencers on generator exhausts and sound attenuated enclosures on outdoor equipment, such as generators and cooling towers, should be always considered.

Outdoor equipment located on the ground and on rooftops may require screening for architectural aesthetics or building codes. Consider incorporating sound barriers within the architectural screening.

5.4.7 Other Topography and Natural Environment Recommendations

Avoid sites with larger than a 15% ground slope if possible; otherwise, this may limit the developable area. Sites with steep slopes may be difficult to access in adverse weather conditions.

The site topographical features should not restrict the line of sight to geosynchronous satellites and location of ground dish arrays if required. Line-of-sight issues may also affect the location of wireless access equipment such as microwave, infrared, and directional antennas.

Sites with wetlands and protected habitat should be avoided because construction in these areas can be delayed, have higher costs, and may create unwanted public awareness of the facility.

A maximum elevation of 3050 m (10,000 ft) is recommended as the effectiveness of air cooling systems degrades significantly at higher elevations where air density is lower. Generator radiator cooling systems are severely limited at higher altitude (above 450 m/1500 ft), affecting both operating times for prime, standby, or continuous duty engines in addition to the derating of the kW output to maintain a generator system's prime, standby, or continuous rating.

5.5 Man-Made Hazards

5.5.1 Introduction

Man-made hazards from accidents and incidents typically have a greater impact on a data center's operational availability than natural events.

5.5.2 Recommended Separation Distances

The following distances shown in Table 5-1 should be observed when selecting a data center.

NOTE: Each element on the list has its own risk factors and rating dependent on the specific site.

5.5.3 Other Recommendations

Locations that are adjacent to or accessed via routes that could be subject to protest or blockade because of their antisocial nature should be avoided.

When placing a data center in close proximity to a railroad, measurement of vibration and EMI at the site should be conducted over the period of several days to aid in the assessment and mitigation requirements, if any, required at the site.

Risk of terrorist attack can be a significant reason for avoiding a location close to an underground train station. Additionally, underground train traffic can create vibration and provide EMI within a building located directly above the train tunnel.

Table 5-1 Recommended Distances from Man-Made Elements

<i>Man-Made Element</i>	<i>Minimum Distance</i>
Airports	8 km (5 mi)
Auto body or other paint shops	1.6 km (1 mi)
Canals	3.2 km (2 mi)
Chemical plants and storage (e.g., fuel, fertilizer)	8 km (5 mi)
Conventional power plants (e.g., coal, natural gas)	8 km (5 mi)
Embassies and political group properties	5 km (3 mi)
Foundries and heavy industry operations	8 km (5 mi)
Gas stations and distributors	1.6 km (1 mi)
Grain elevators	8 km (5 mi)
Harbors and ports	3.2 km (2 mi)
High-voltage power transmission lines	1.6 km (1 mi)
Lakes, dams, and reservoirs	3.2 km (2 mi)
Landfills and waste storage facilities	3.2 km (2 mi)
Landing and takeoff flight paths for any airport	1.6 km (1 mi)
Military installations and munitions storage	13 km (8 mi)
Municipal water and sewage treatment plants	3.2 km (2 mi)
Nuclear power plants	80 km (50 mi)
Overflow areas for reservoirs and man-made lakes	1.6 km (1 mi)
Quarries	3.2 km (2 mi)
Radio/television transmitters/stations	5 km (3 mi)
Railroads	1.6 km (1 mi)
Research laboratories	5 km (3 mi)
Self-storage facilities	1.6 km (1 mi)
Stockyards and livestock feedlots	3.2 km (2 mi)
Transportation corridors where hazardous material could be transported	1.6 km (1 mi)
Water storage towers	1.6 km (1 mi)
Weather or other radar installations	5 km (3 mi)

5.6 Site Access and Location

5.6.1 Public Road Access Recommendations

The site should allow the placement of the building so that it is not close enough to the road that an adjacent road traffic accident could result in vehicular contact with the building fabric or any external component of the data center's mechanical or electrical systems and the potential for resulting structural damage or the potential for fire.

The site should allow the placement of the building so that it is not close enough to the road that an adjacent road traffic accident could result in the spillage of a toxic or flammable load coming into contact with the building fabric and resulting in structural damage or the potential for fire.

The site should be within reasonable distance—3.2 km (2 mi) to 16 km (10 mi)—to a freeway or other major arterial road. However, it is generally not desirable for the data center to be within 1.6 km (1 mi) of a freeway, railroad, or other major thoroughfare to minimize exposure to contaminants in the event of an accident.

The site should have two or more access roads from the nearest major arterial road with each road having a minimum of 4.3 m (14 ft) height clearance for vehicles throughout. Utilizing a single access road with bridges or tunnels should be avoided.

The sub-structure and surface of the access roads should be designed in a way so that in any weather condition deliveries (e.g., heavy components of the technical building systems, including mobile cranes required for unloading) can be made.

If the data center is on a campus, then the campus should have redundant access roads with either a security checkpoint at the access point to the data center facility or at each access point to the campus.

5.6.2 Adjacent Property

5.6.2.1 Recommendations

The data center should be built far from any other buildings and facilities that may pose a fire threat or that could cause damage to the data center should the other buildings or structures collapse.

A facility located adjacent to a large campus or manufacturing plant may suffer from traffic issues at certain times of the day (e.g., at the start and end of the working day; if adjacent to a 24-hour facility, this could be three times a day or more, depending on shift patterns).

5.6.2.2 Additional Information

The following is a partial list of adjacent properties that have an increased potential to affect data center operations:

- Embassy/consulate
- Military
- Police
- Fire station
- Hospital
- Chemical plant
- Political target
- Research lab
- Publishing house/foreign press

Adjacent vacant lots may cause future issues because of:

- Possible future development and disruption during construction
- Unknown tenant(s)

5.6.3 Proximity to Existing or Redundant Data Center

For disaster backup sites, consider the issue of distance from the primary data center. Distance will be determined by the use of the primary site and whether the backup site must have synchronous or asynchronous replication with the primary data center.

5.6.4 Security and Emergency Services

5.6.4.1 Requirements

Avoid high crime areas. Refer to Section 12 for additional threats and concerns to be considered.

5.6.4.2 Recommendations

Having emergency services reasonably accessible can be a valuable lifesaving resource for site occupants. Ideally, a staffed (or at least volunteer) fire station and police station should be within 8 km (5 mi) of the candidate site and a hospital emergency room within 16 km (10 mi).

Consideration should be made for level and type of perimeter security required for the site, depending on an initial risk and threat analysis. This would include building type, site location, fenestration, and neighborhood. These factors will vary based on the users need.

5.6.5 Proximity to Skilled Labor

If the site is in a rural location, skilled personnel to staff the data center may not be available locally, and skilled people may not be willing to relocate from urban locations. A location close to technical colleges and universities is desirable. The site should be close to the location of vendor technicians that perform maintenance and repair of ITE and facility equipment.

5.7 Utility Services

5.7.1 Power and Electrical Service

5.7.1.1 Introduction

Figure 5-7 shows an overview of electrical transmission and distribution.

5.7.1.2 Capacity Available to Site

5.7.1.2.1 Requirements

Adequate electrical utility capacity to the site shall be provided to meet both current and projected needs of the entire site and depends on the data center Availability Class requirements (as described in Appendix B).

5.7.1.2.2 Recommendations

Consider using multiple electrical utility circuits, each with enough capacity, to handle the entire site requirements. Circuit capacity to the site should be planned and implemented very carefully. If the data center is designed for minimal initial capacity with large future capacity requirements, careful consideration should be given to the amount of initial power requested to be delivered to the site by the utility company.

Work with a professional electrical engineer and the electrical utility or utilities serving the site. A cost benefit analysis and progressive circuit capacity design/implementation may benefit the site.

5.7.1.3 Unit Substations

5.7.1.3.1 Introduction

Unit substations are usually medium voltage switchgear that is used to parallel electrical utility circuits or to transfer between redundant electrical utility circuits feeding the data center site. Unit substations are generally located outdoors on pads within fenced areas, but in some cases, may be found inside of the data center building (e.g., data centers located in metropolitan settings).

Depending on the size, Availability Class, and location of the data center, a unit substation may be required on the site. Very large data centers typically have substations on the premises. In most cases, the unit substations are owned and maintained by the electric utility. The largest data centers may prefer to have control over the unit substations for security and availability reasons.

Unit substations generally connect to utility transformers sized to meet the building voltage and amperage requirements.

5.7.1.3.2 Recommendations

Data centers should be located in an area with easy sustainable circuit access to utility substations with preference toward an area with utility circuits provided by two or more utility substations.

When selecting a site, consider space for an electrical unit substation and its associated transformers and electrical utility circuit paths. It is preferable that these are located on the data center site in a secure and aesthetically pleasing manner.

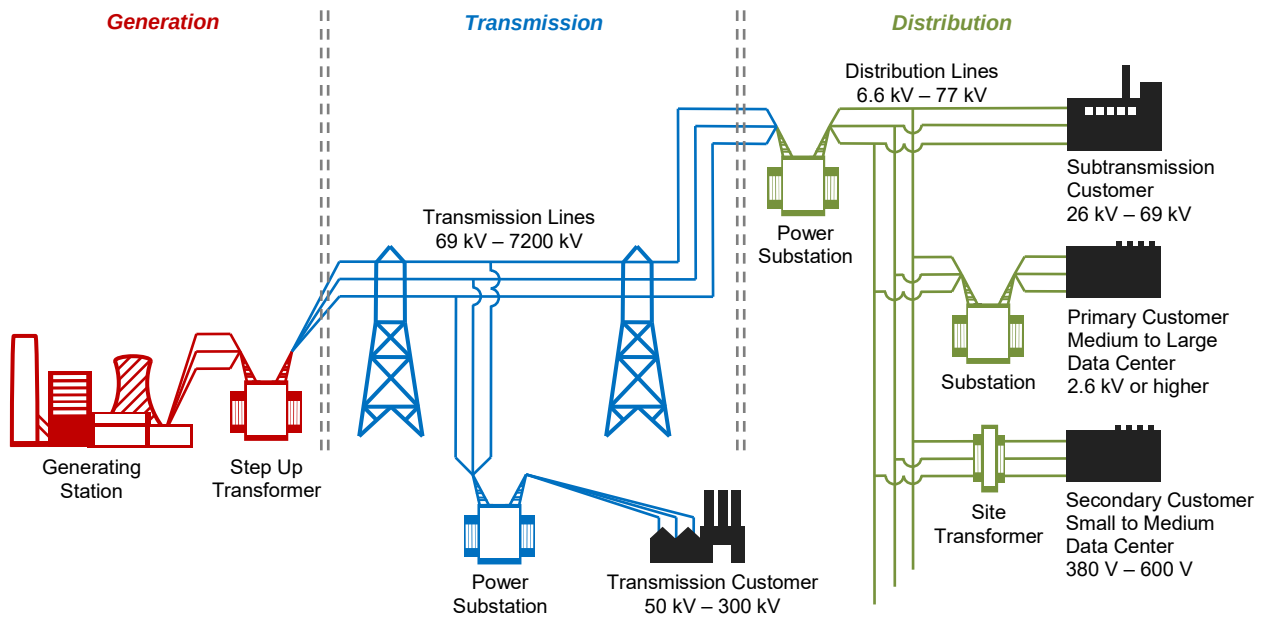


Figure 5-7
AC Electricity Distribution from Generation Stations to Data Centers

5.7.1.4 Utility Transformers

5.7.1.4.1 Introduction

For small data centers, the utility transformer might be pole-mounted or pad-mounted outside of the facility. For most data centers, depending on the data center's size, class, and location, the unit transformer will be on site. Utility transformers are generally located outdoors, but in some cases, may be found inside the data center building (e.g., data centers located in metropolitan settings).

The utility transformer is usually the last utility-provided device prior to the electric meter, which marks the demarcation between the electric utility and the electricity consumer. In many cases, this transformer is owned by the power consumer, in which case, it is located on the load side of the electric meter.

Utility transformers usually transform the utility's medium distribution voltage to a lower voltage for utilization by the data center. For example, for a large data center, the unit substation might transform voltage in excess of 13 kV to a voltage up to 1 kV. An on-site utility transformer might then transform the voltage to a lower voltage utilized by the building or facility. Consumption voltages vary around the world and will typically be defined by the regulatory authority in the country or region where the data center is located.

5.7.1.4.2 Recommendations

When selecting a site, consider space for one or more electrical utility transformers and their associated electrical utility circuit paths. It is preferable that these are located on the data center site in a secure and aesthetically pleasing manner.

5.7.1.5 Proven Utility Reliability (Percentage Availability)

5.7.1.5.1 Introduction

For critical data centers, there may be benefit in providing a second, independent utility service to the data center site.

5.7.1.5.2 Requirements

A second power utility connection is not required for any Class of data center.

5.7.1.5.3 Recommendations

The benefit of installing a second utility feed should be analyzed based on the mean time between failure (MTBF) rate, mean time to repair (MTTR), and the power quality of the service to the data center.

A second diverse power utility feed is only recommended when all of the following are true:

- 1) The operational requirements of the data center results in an Operational Level 4
- 2) The availability requirements of the data center results in an Availability Ranking Level 4
- 3) The impact of downtime of the data center results in a Catastrophic classification
- 4) The reliability of the utility, based on the specific MTBF rates of the utility and the required mission time of the data center, is greater than 50%.

For the electrical feed, determine if there are other customers, such as manufacturing plants, that can create electrical noise. An electrical feed that also serves a hospital is generally desirable because such feed is less prone to shutdown by a utility.

5.7.1.5.4 Additional Information

Table 5-2 shows reliabilities of a utility, given examples of MTBF, and the mission times expressed in years. In the table shown, the only scenario that achieves greater than 50% reliability is where the mission time is 5 years with a utility MTBF of 10 years. Within this scenario, the second utility with an example reliability of 50% will result in between 1/10% and 1% of an increase in the overall power systems, assuming the power systems meet a Class 4 topology. The increase in capital expenditures (CapEx) and operational expenditures (OpEx) costs for the second utility must be weighed against the value of increasing the overall reliability by 1/10% to 1%.

Table 5-2 Utility Reliability Examples

		Mean Time Between Failure (MTBF) - Years				
		0.5	1	2	5	10
Mission Time (Yrs)	5	0.004539992976%	0.673794699909%	8.208499862390%	36.787944117144%	60.653065971263%
	10	0.000000206115%	0.004539992976%	0.673794699909%	13.533528326610%	36.787944117144%
	15	0.000000000009%	0.000030590232%	0.055308437015%	4.978706836786%	22.313016014843%
	20	0.000000000000%	0.000000206115%	0.004539992976%	1.831563888873%	13.533528326610%
	25	0.000000000000%	0.000000000139%	0.000372665310%	0.673794699909%	8.208499862390%

The power utility services in the United States average 1.86 outages annually (MTBF equals $1/1.86 = 0.5376$ yrs). For a $2(N+1)$ electrical topology where the number of generators required to meet the load is $N=2$, the resulting overall increase in the power systems reliability with a second utility would be approximately 1/100000000% compared to a $2(N+1)$ backup power generation topology combined with a single power utility connection. This insignificant increase in reliability would not normally be considered worth the significant increase in CapEx and OpEx of the second utility connection.

5.7.1.6 Utility Service

5.7.1.6.1 General Recommendations

Electrical service entrance feeds should have a minimum separation of 1.2 m (4 ft) from other utilities along the entire route. If redundant feeds are provided to the data center, it is recommended that the electrical service entrances to the facility have a minimum separation of 20 m (66 ft) from the other electrical service entrances along the entire route.

The following is a list of preferences (in successive order) of utility line sources:

- 1) At least two diversely routed electrical service feeds from different utility substations with each substation on separate power grids.
- 2) At least two diversely routed electrical service feeds from different utility substations with both substations on the same power grid.
- 3) At least two diversely routed electrical service feeds from one utility substation.
- 4) One electrical service feed from one utility substation.

5.7.1.6.2 Overhead Utility Service Recommendations

Overhead utility service to the facility is not recommended, especially if there is only one service entrance feed. Instead, provide underground utility service to the facility whenever possible. This will reduce the potential for system failure caused by overhead utility line damage. Vehicle accidents, wind, snow, and other weather conditions are known factors for utility line damage.

5.7.1.6.3 Underground Utility Service Recommendations

It is recommended that all electrical service entrances and feeds to the facility be underground.

5.7.1.7 On-Site Generation

5.7.1.7.1 Introductions

Backup generators are used to backup data center equipment in case of utility power failure. Emergency generators (as opposed to backup generators) are used to power data center life safety systems (e.g., emergency lighting, fire pumps) if utility power fails.

Backup generators can be as small as a compact car and as large as a full-sized truck. Some generator solutions utilize a space as large as a shipping container or larger. These may be either indoors or outdoors, and it is common to find building rooftop-mounted generators.

5.7.1.7.2 Requirements

For buildings to be occupied for extended power outages, areas of the building outside the data center must provide basic life safety and building occupancy requirements, including but not limited to, lighting, fire alarm, operable restrooms, elevators, security, and ventilation.

5.7.1.7.3 Recommendations

When selecting a site, consider space for one or more backup and one or more emergency generators and their associated electrical utility and life safety circuit paths. It is preferable that these are located on the data center site in a secure and aesthetically pleasing manner.

Space considerations for generators should also include the necessary fuel pumps, piping, and on-site storage required. For some data center applications, the space required can be quite extensive as operational requirements may dictate performance for a minimum of 48 hours without outside services or deliveries.

5.7.2 Communications

5.7.2.1 Capacity Available to Site Recommendations

Adequate copper conductor and optical fiber capacity to the site should be provided to meet the current and projected needs of the entire site, and depending on the data center Class requirements, provide one or multiple connectivity paths, each with enough capacity, to handle the entire site requirements.

Connectivity capacity to the site should be planned and implemented very carefully. If the data center is designed for minimal initial capacity with large future capacity requirements, careful consideration should be given to the amount of capacity requested to be delivered to the site by the access providers.

Work with a professional IT consultant and the access providers serving the site. A cost benefit analysis and progressive connectivity capacity design/implementation may benefit the site.

5.7.2.2 Proven Access Provider Reliability (Percentage Availability) Recommendations

The reliability of the primary access provider should be determined to ensure that the required availability requirements can be achieved.

Reliability of the communication services can be improved by either adding redundant circuits from the primary access provider or adding services from alternate access providers. The reliability of the overall communications services can be further increased if the redundant circuits are serviced from separate access provider offices following diverse routes.

5.7.2.3 General Service Recommendations

If redundant telecommunications service cabling is desired or required, telecommunications service cabling pathways should maintain a minimum separation of 20 m (66 ft) along the entire route.

The following is a list of preferences (in successive order) of communication service sources:

- 1) At least two diversely routed telecommunications service feeds from different access provider central offices with each access provider central office connected to multiple higher level access provider and multiple long-distance carrier offices.
- 2) At least two diversely routed telecommunications service feeds from different access provider central offices with both access provider central offices connected to the same higher level access provider and long-distance carrier offices.
- 3) At least two diversely routed telecommunications service feeds from one access provider central office.
- 4) One telecommunications service feed from one access provider central office.

5.7.2.4 Underground Service to Facility

5.7.2.4.1 Requirements

Determine if the site can accommodate customer-owned maintenance holes and if elevation of maintenance holes (utility or customer owned) can cause problems with water infiltration into data center.

5.7.2.4.2 Recommendations

It is recommended that all telecommunications service cabling to the facility be underground with a minimum separation of 1.2 m (4 ft) from other utilities along the entire route.

Provide underground utility service to the facility whenever possible.

5.7.2.5 Overhead Service to Facility

5.7.2.5.1 Introduction

Overhead utility service to the facility is not desirable, especially if there is only one service entrance.

5.7.2.5.2 Requirements

If overhead utility lines to the site cannot be avoided, provide multiple source paths. Ensure that the entrance cables are well protected from physical damage at the drop pole.

5.7.2.5.3 Recommendations

If cables drop from service poles to underground, the drop pole should provide 100 mm (4 in) rigid conduits from below grade up to the elevation where the cables are suspended to protect the entrance cables from physical damage.

5.7.2.6 Proximity to Service Providers or Other Data Centers

Data centers should be located in an area with easy sustainable connectivity to the access provider central offices. Locating a data center in an area with connectivity provided by two or more access provider central offices is recommended for Class 2 and higher data centers.

Redundant data centers for disaster recovery (DR) purposes should be located with sufficient physical separation to reduce single modes of failure (natural or manmade) to within acceptable limits for the critical data. The two locations should be on separate distribution systems to minimize the occurrence of one outage affecting both locations.

5.7.3 Water Service

5.7.3.1 Introduction

The data center may need to have access to reliable significant quantities (750-1100 liter/min [200-300 U.S. gallon/min]) of quality water, depending on cooling system design. However, not all areas are able to provide this quantity of quality water continuously independent of long-term weather conditions.

Data centers may require large volumes of water for other uses. Some uses of water that may be required are as follows:

- Domestic water (e.g., drinking water, restrooms, kitchens)
- Irrigation (e.g., lawn watering)
- Fire suppression (e.g., sprinkler systems)
- HVAC (e.g., cooling towers, air humidification)

5.7.3.2 Municipal Water Supply

5.7.3.2.1 Capacity Available to Site Requirements

Provide adequate municipal water delivery to the site to meet the requirements of the data center. For Class F3 or F4 data centers, the ability of the water supply pumping station(s) to deliver water when there is a major power outage must be documented or mitigated.

5.7.3.2.2 Water Quality Recommendations

Although water delivered to sites by most municipalities is generally considered to be potable (drinkable), the water should be tested for contaminants and particulates. Water filtration systems may be required for some or all of the various water uses listed above. It is common to find a water filtration system specific to the domestic water system in a building.

5.7.3.3 Non-potable Water Systems (Greywater)

5.7.3.3.1 Introduction

Non-potable (waste water that doesn't contain serious or hazardous contaminants) systems can be municipally provided or project generated and can be used to minimize a project's impact on the surrounding community and potentially reduce operating costs.

5.7.3.3.2 Requirements

Non-potable water systems shall be used according to the local AHJ.

5.7.3.3.3 Recommendations

Greywater systems should not store grey water for longer than one day to minimize the risk of microbial growth. Greywater storage tanks should be designed to drain completely upon use and have minimal to no anaerobic corners or pockets.

5.7.3.4 Private Well Supply (Well Water)

5.7.3.4.1 Capacity Available to Site

5.7.3.4.1.1 Requirements

If well water is to be utilized, make sure that there is adequate well water delivery on the site to meet the requirements of the data center. It is first necessary to determine the volume and quality of water that will be consumed for all purposes (data center cooling, building plumbing and occupant use, lawn irrigation, etc.) and how much can be recycled.

5.7.3.4.1.2 Recommendations

A hydrogeological risk assessment may be required. The assessment should be conducted by a licensed hydrology engineering firm. An environmental impact study might be required. A hydrogeological report can include information on:

- Groundwater
- Infiltration
- Soil moisture
- Surface water flow
- Precipitation and evaporation
- Uncertainty analysis
- Water quality
- Remote sensing
- Integrating measurement and modeling
- Prediction

5.7.3.4.2 Quality Recommendations

The available on-site water (well water) should be tested for contaminants and particulates. Water filtration systems may be required for some or all of the various water uses listed above. It is common to find a water filtration system specific to the domestic water system in a building.

5.7.3.4.3 Dual Water Supply (Municipal Water Supply and Well Water Supply)

Occasionally, a data center site will require both a municipal water feed to the site as well as using an on-site well. A domestic water system and fire suppression system may be connected to the municipal water source while having the HVAC and irrigation systems connected to the on-site well. An on-site well can also be used as a backup water source for HVAC water systems connected to a municipal water source.

5.7.3.5 Backup Water Supply

5.7.3.5.1 Introduction

Backup systems could be multiple water sources or onsite water storage.

5.7.3.5.2 Requirements

A backup water supply of at least 8 hours at any time shall be provided for data centers with Class F3 or F4 that use evaporative cooling towers for heat rejection.

5.7.3.5.3 Recommendations

Review need and availability of a backup water supply for the facility for domestic uses as well as water cooled cooling systems.

Backup water supply should be provided that meets the minimums listed in Table 5-3.

Table 5-3 Recommended On-Site Supply of Services for Data Center Facility Classes

<i>Class F0</i>	<i>Class F1</i>	<i>Class F2</i>	<i>Class F3</i>	<i>Class F4</i>
No requirement	8 hours minimum	24 hours minimum	72 hours minimum	96 hours minimum

5.7.4 Sanitary Sewer

5.7.4.1 Municipal Sanitary Waste Sewer System

5.7.4.1.1 Capacity Available to Site Requirements

Provide adequate sanitary waste capacity from the site to the municipal sanitary waste sewer system. A private sanitary waste system will be required in regions where no municipal sanitary waste sewer system is available.

Sanitary systems or storm drainage systems (depending on local requirements) need to be sized for the amount of expected water usage by cooling systems, including cooling tower blow down or filtration systems, which could be greater than 750 liters/min (200 gpm).

5.7.4.1.2 Remediation Requirements

Coordinate with the local AHJ, and provide all remediation as may be required by code and standards. Holding tanks, traps, and the like may be required and need to be planned into the site design.

5.7.4.1.3 Recommendations

A private sanitary waste system is recommended for critical facilities that require on-site operations personnel 24/7 to maintain uninterrupted services. This will help mitigate having to vacate the facility in the event the municipal sanitary waste sewer system fails.

5.7.4.2 Private Sanitary Waste System

5.7.4.2.1 Capacity Available to Site Requirements

Provide adequate sanitary waste capacity from the building to the on-site sanitary waste system (septic system).

5.7.4.2.2 Remediation Requirements

Coordinate with the local AHJ, and provide all remediation as may be required by code and standards. Holding tanks, traps, and similar facilities may be required and need to be planned into the site design.

5.7.5 Natural Gas and Other Fuels

5.7.5.1 Introduction

Fuels (e.g., natural gas, propane, diesel) may be used to support primary or back-up systems of a data center. On-site fuel (e.g., propane, diesel) storage tanks are usually located outdoors on the ground and are sometimes buried below grade.

5.7.5.2 Requirements

If natural gas is selected to support the heating systems, cooling systems, or backup electricity generation that the site requires, provide properly sized natural gas feed from the local utilities.

Make sure that the utility company assures full capacity natural gas delivery to the site for the duration of any prolonged power outage or disaster situation.

5.7.5.3 Recommendations

Redundant gas feeds from redundant gas sources is the most desirable, although rarely available, method for natural gas delivery to a site. Natural gas in combination with diesel fuel may also be considered if dual-fuel generators are incorporated into the design. Dual-fuel generators start on diesel but can run on either diesel or natural gas. For sites with natural gas generators sized 25 kW or less, on-site storage of natural gas should be considered. The number of hours or days of reserve should be based upon a risk analysis or meet the recommendations listed in Table 5-3.

The data center site should be carefully planned to support on-site fuel storage when it is required. On-site fuel storage should be located on the data center site in a secure and aesthetically pleasing manner. Fuel should be stored as far away from the data center as practical. Blast containment (proximity to building or actual structure) should always be planned into the site.

Special containment or controls are usually required in case of fuel leaks.

Controls for fuel transfer should be in a secure location, above worst-case flood levels, and protected from other natural disasters.

5.7.5.4 Alternative Fuel Source Recommendations

Other fuel or energy sources (e.g., wind, solar) may be used to support the site. Consider their continuous availability to determine if they can be primary or secondary energy sources. If other energy sources are used, their requisite equipment and system infrastructure (wind generator, photovoltaic panels) will require additional space and may affect building and structural requirements.

Careful consideration should be given to the visual intrusion on neighbors and any effects on the surrounding environment. Zoning, codes, and other governmental/municipal restrictions may not allow for alternate fuel/energy sources.

5.8 Regulations (Local, Regional, Country)

5.8.1 Air Quality Requirements

Determine if local air quality regulations exist such as generator emission restrictions. These regulations may restrict the acceptable hours of operating backup generators.

Particular concerns that data centers may have for local authorities are the emissions of oxides of nitrogen (NO_x), carbon monoxide (CO) and particulate matter (PM-10).

NOTE: The United States government enacted a law through the 1990 Clean Air Act that mandated individual states are required to only meet the minimum requirements of the Act. However, individual states were, and continue to be, permitted to enforce stricter requirements.

5.8.2 Noise Requirements

Determine if there are any local, regional, or federal regulations that identify acceptable levels of noise from equipment operating within the data center facility or campus or that cannot be exceeded at or beyond the property line.

5.8.3 Towers and Tall Structures Requirements

Determine if there are any local regulations that will restrict the height or proximity to other facilities for communication towers, water tanks, cooling towers, and other tall structures.

Determine if there are any federal or local requirements to hide these structures from public view.

5.8.4 Fuel Tanks Requirements

Determine if there are any local regulations that will require double-walled tanks or restrict the size or proximity to other facilities for fuel tanks.

Determine if there are local regulations that will allow above ground fuel tanks only.

Evaluate security of the fuel tanks.

5.8.5 Generator Requirements

Emission levels need to meet state and local emission requirements. Generator hours may be limited by local codes because of air quality emission control or noise abatement.

5.8.6 Site Access and Required Parking

Determine if there are any road restrictions (permanent or seasonal) on the size of vehicular traffic or time of day restrictions for truck traffic.

Determine how the AHJ determines the required number of parking stalls for a new facility. Negotiations with the AHJ may be necessary to try to reduce the number of required stalls if the AHJ treats the data center as typical commercial office space.

Consideration should be given to disaster recovery scenarios, which may require additional parking for the respective personnel.

5.8.7 Setbacks and Sight Lines

Determine the required setbacks from the property line for the building, parking, or perimeter security. Verify with the AHJ that the target location does not have sight line restrictions that must be mitigated or that they can be done so economically.

5.8.8 Environmental Assessment

An environmental assessment could include an environmental impact study if wetlands are impacted or if the site has any contaminants present. An environmental impact study may be required by the AHJ. Ensure sufficient time prior to proceeding with the detailed design phase to allow completing the study, and attend AHJ meetings as required to obtain approval.

NOTE: The United States Environmental Protection Agency and the European Commission (i.e., Environmental Impact Assessment Directive 2011/92/EU) may provide further relevant information specific to the site or project.

6 Space Planning

6.1 Overall Facility Capacity

6.1.1 General

The capacity of a data center is based on the size of the computer room space (floor space or rack space available for IT and telecommunications equipment), and the capacity of the power and cooling systems per unit of computer room floor space. High-density data centers have a higher capacity of power and/or cooling per unit of computer room floor space.

A balance between space and capacity needs to be determined at the outset when designing a new data center and when modifying an existing data center space. The balance will depend on the type of IT and telecommunications systems the data center is to support and the number/combination of those systems that are to be placed within each cabinet or rack.

When planning for the overall facility:

- Design to accommodate a defined load (N) over a defined area.
- Consider current and future platforms for servers and storage when identifying the design load and area requirements.
- Consider the physical expansion of the building or additional buildings on the site.
- Estimate the change in IT program, and set upper and lower limits that the space and infrastructure plan may be expanded or contracted to meet the ITE and building program.
- Determine percentages for mainframe high-end processing, mid-range processing, small-form or blade servers, communications networks, and storage.
- Identify potential growth rates not only within business units, but also identify growth rates across platforms as these effect capacity and space plans.
- Define the portions or segments in which the data center will be developed between the initial build and final build if not developed to the full capacity at its inception. This will be the “module” size for the life of the facility.
- Define and connect the ITE program to the facility program with the operational expense and capital expense budgets, and the length of time to construct, test and implement following phases of work. Similarly, project the total cost of ownership (TCO) for builds based on the kW development integer chosen and the capital to be expended on the initial build, ultimate build, and the costs of the incremental work between these two points.

If it is perceived that meeting the performance balance will require delivery of both high levels of power and large amounts of cooling to the cabinet or rack, it may be more cost-effective to design and build a more moderate density data center by designing the data center into a space that can accommodate a larger computer room. The resulting space utilization with power and cooling density limitations should be clearly communicated and documented.

6.1.2 Module and Modular Design

Data center “module” sizes might not be in exact size harmony with each other or that they would be added in synch. There are logical break points in the entire system module sizes discussed in the Standard. As long as modules are added at or ahead of ITE need, there will be no risk to the operation’s Class rating falling. Modules may certainly be built out ahead in anticipation of following ITE or data center needs. For example, a data center owner may choose to construct the entire building shell of the data center, only to defer some of the data center space and infrastructure space to a time when it is needed in order to preserve capital. Some modules might actually lag development, which may pose a problem in maintaining the Class rating.

Should a modular infrastructure solution be utilized, link the electrical deployment critical power kW output size to the corresponding cooling capacity additions to the storage and compute cluster module’s growth increment. For example, if 200 cabinets at 6 kW each are anticipated, add 1,200 kW of UPS output power and cooling in addition to any space needed, excluding any safety or design factors. If the 200 cabinets and 1,200 kW of IT load is the typical deployment, then that is the module size.

The time to make facility or ITE deployment decisions must also be factored into space planning decisions and module sizes. The space and infrastructure total deployment time (viewed as the total time to decide an addition is necessary, solicit the bid to develop the space, and turn it over) must be less than the IT planning time offered to the space developers. For example, should the company be incapable of providing IT projections beyond the time it would take to develop the requisite space or infrastructure by a built-in-place approach or by the existing delivery methods and processes, options available would be to either build ahead of the IT need or to adopt a facility or infrastructure solution that can meet that need.

An example of the decision flow for determining module size can be found in Figure 6-1. Alternatively, use of a checklist, as shown in Table 6-1, can be used.

This standard offers no endorsement of any particular building approach as the ultimate choice whether to employ a built-on-place, modular or containerized data center space, or infrastructure solution resides solely in the hands of the space developer or end user. Ultimately, the data center space and infrastructure must fully meet the Class requirements of the operation. This will be affected by the operation's access to capital; the ability to secure an actionable ITE program to support the space and infrastructure builds; and the speed in which space, cooling, and power can be deployed ahead of IT need. There are fewer choices if less time is available.

Density, module size, capital, and schedule requirements for a build and the Class rating of the platform and applications will be powerful contributors to space and infrastructure programs and will determine ultimate facility plans.

6.2 Power Systems

6.2.1 Introduction

The primary considerations when developing the space plan for the power systems include the spacing of electrical feeders, conduit and busbar usage, if the UPS system is centralized or distributed, the additional needs of redundant power systems, replacement space, and required equipment service areas.

6.2.1.1 Requirements

Sufficient clearances shall be provided for safety, access and maintenance for all electrical equipment as specified by the manufacturer, applicable codes and standards, and the applicable AHJ.

Sufficient access shall be provided to the electrical equipment spaces to remove components or systems for maintenance or replacement as specified by the manufacturer, applicable codes and standards, and the applicable AHJ.

6.2.1.2 Recommendations

Minimize the distance or increase the voltage of electrical feeders between various distribution equipment; excessive distances require increased feeder sizes and additional costs.

Provide sufficient space for the conduit runs or busbars with minimal bends. Because the routing of the electrical feeders can be very complex in a data center, coordination with all other disciplines is required.

Provide dedicated space and physical separation for each system in configurations that have redundant power systems or redundant computer systems.

Subsystems of the electrical distribution systems (e.g., main switch gear, generator switchgear, centralized UPS and batteries, and stored energy systems if appropriate) should be installed in dedicated electrical rooms or located outside of the data center computer room space, separated by a fire-rated wall. See Table 7-1 regarding fire-rated construction.

The electrical infrastructure for the data center should be isolated and separate from the base building electrical systems if the building is not exclusively dedicated to the data center function.

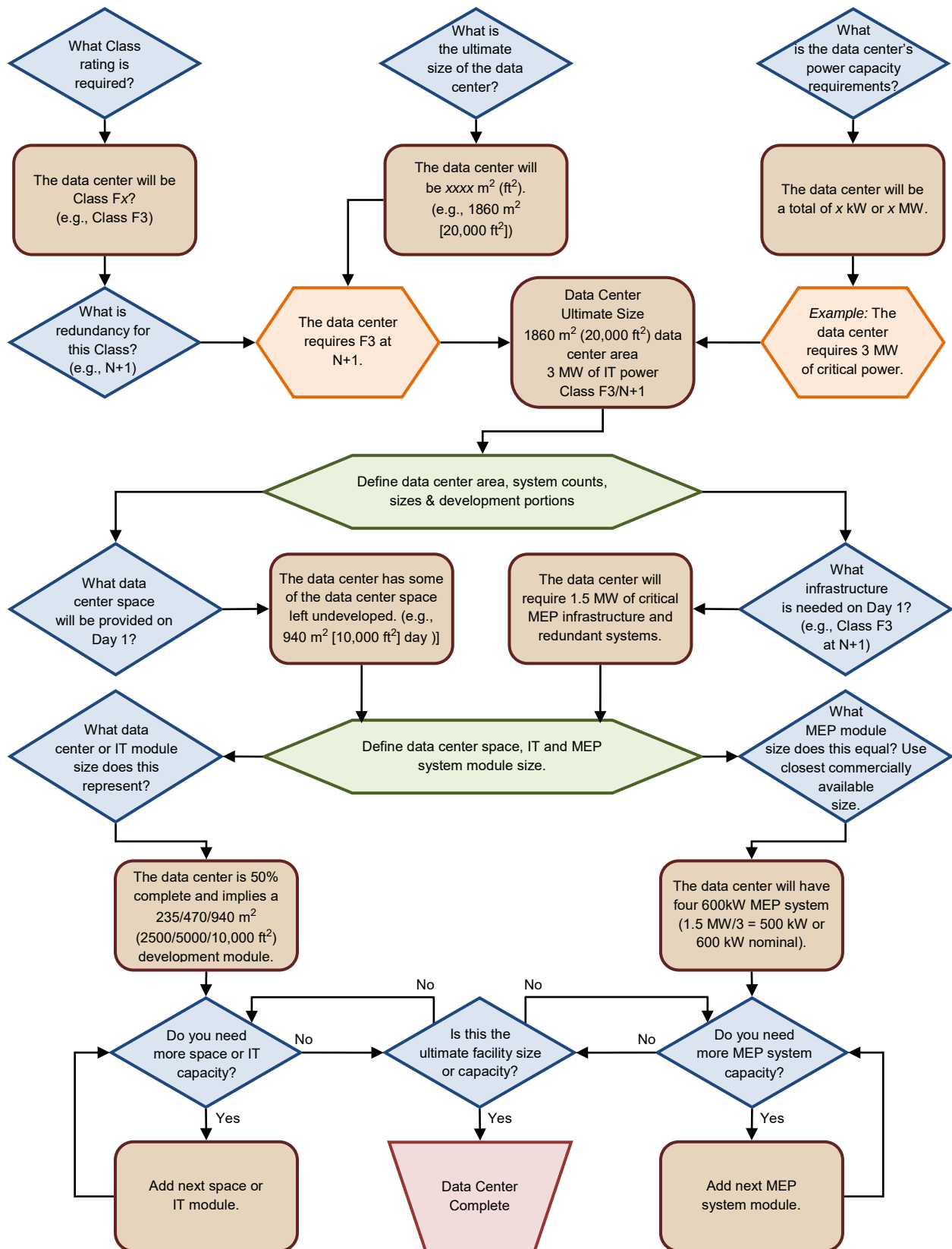


Figure 6-1
Example Module Size Decision Tree

Table 6-1 Example of a Module Size Design Checklist

<i>ID</i>	<i>Question or Item</i>	<i>Purpose or Notes</i>
1	<i>Class Rating Checklist</i>	
1.1	Does the data center have a Class rating?	Define Class rating for the project.
1.2	If "Yes", what is it?	
1.3	If "No", here are some questions concerning the data center and aspects of the business the data center support:	Ask question to determine system and service availability levels.
1.3a	Does the business operate worldwide, located within multiple time zones, or require after-hours access?	
1.3b	Does the data center fail over to another disaster recovery facility, or is it able to sustain an outage within the facility without undue harm to business operation?	
1.3c	Does the business have extended or 24/7 operational requirements?	
1.3d	Does the business require 24/7 processing or storage?	
1.3e	Does the business require a 24/7 network?	
1.3f	Can the data center have scheduled outages for maintenance purposes?	
1.3g	Does the data center support transaction verification or processing?	
1.3h	If part of the construction is deferred, can business operations sustain an outage during planned system or building additions?	
2	<i>Data Center Ultimate Size Checklist</i>	
2.1	What is the target area per rack or ITE position?	What is the area/rack for the data center plan?
2.2	How many rack positions does this data center need?	Define the number of ITE locations.
2.2a	As a minimum?	Minimum rack counts for the complete build out
2.2b	Ideally?	Ideal rack counts for the complete build out
2.2c	At an absolute maximum?	Maximum rack counts for the complete build out
2.3	How many rack positions are needed on day one?	Initial rack or ITE positions needed day one
2.4	Are there any factors that would increase or decrease the data center rack space, capacity or the speed of development?	Identify space planning considerations that will increase or decrease the per unit space assumptions from above
2.5	When does the data center need to be ready for service?	When will the data center be needed?
2.6	What is the growth rate for the data center?	How fast will the data center grow, requiring further development if work, systems, or space is deferred?
2.7	How long does this data center need to be in service?	What is the lifespan of the facility before complete renovation or abandonment?
3	<i>Data Center Power Density Checklist</i>	
3.1	What technology is currently being employed?	Technology used today will offer the current power density
3.2	What technology is projected to be employed?	Technology will indicate the power to be consumed in the future.
3.3	What is the proportion of the systems to be used processing, storage, network?	The mix and proportion of the technologies used will result in the target power density for the facility.

Table continues on next page

<i>ID</i>	<i>Question or Item</i>	<i>Purpose or Notes</i>
3.4	Are there considerations to current or future use of high-performance computing?	This will increase power density markedly and must be considered.
3.5	Are there any projects or programs likely to come into the data center in the next 3 years that is not here today?	What are the near- and mid-term projects and programs that might adversely affect the power density?
3.6	How much spare capacity is desired or planned?	How much spare capacity is needed for planning and system safety purposes?
3.7	How much growth in load density is planned?	How much do you see the technology mix changing and affecting the power density?
4 Data Center Phased Development Checklist		
4.1	How much data center space do is planned to be built initially?	What is the size of the first build?
4.2	Are there plans to leave undeveloped space for future use?	This allows for growth before a larger build must be undertaken?
4.3	Is there correlation between initial build size and data center size (e.g., does the planned development break into sensible portions)?	Power usage per area (e.g., W/m ² or W/ft ²) should be equivalent when comparing the data center area and the plant's total area.
4.4	What are the physical area build increments for the data center floor?	When considering the initial build requirement, the ultimate build size, what is the logical space development size (e.g., 1400 m ² [15,000 ft ²] modules in four phases for a 5600 m ² [60,000 ft ²] data center)
4.5	As the data center grows, is it planned or desired to add electric utility and cooling modules in increments equal to the capacity of the added data center IT modules?	Increasing electric and cooling in increments equal to the increase in IT will minimize operating costs, but it might be more disruptive when IT modules are installed. Operating with less than the designed Availability Class rating can be less disruptive when changes are made, but there will be operating cost penalties for stranded capacity until full capacity is utilized.
4.6	How many development phases are planned or desired?	
4.7	What is the electrical topology for the data center?	What topology have you chosen to meet your Class requirement?
4.8	What is the electrical build increment for the data center floor?	What electrical distribution system meets the Class requirement at the stated power density for a data center space module?
4.9	What is the electrical build increment for the central electrical plant?	What electrical plant-level system meets the Class requirement at the stated power density for a data center space module?
4.10	Can the electrical system be partitioned for future additions without a service interruption?	Has additional equipment or connection capability been accomdated for transparent, future work in concert with your Class rating?
4.11	What is the mechanical topology for the data center?	What mechanical distribution system meets the Class requirement at the stated power density for a data center space module?
4.12	What is the mechanical build increment for the data center floor?	What mechanical plant-level system meets the Class requirement at the stated power density for a data center space module?
4.13	Can the mechanical system be partitioned for future additions without a service interruption?	Do you need to account for additional equipment or connection to allow for transparent, future work in concert with your Class rating?

Table continues on next page

<i>ID</i>	<i>Question or Item</i>	<i>Purpose or Notes</i>
5	<i>Utility Module Size Checklist</i>	
5.1	Based on the space and load planning conclusions above, what is the logical module size for a given electrical system?	What is the electrical component size viewed in output kW and input kVA for your selected topology?
5.2	Are the electrical module sizes typical "trade" sizes?	What is the typical industry size for your key electrical components – UPS power module, generator, switchboard, critical power distribution, and substation transformer?
5.3	Based on the module size, what is the minimum number of electrical modules needed for the initial build?	Fully consider your Class rating when determining the number of modules for your initial build
5.4	Based on the module size, what is the minimum number of electrical modules needed for the ultimate build?	Fully consider your Class rating when determining the number of modules for your ultimate build
5.5	Based on the space and load planning conclusions above, what is the logical module size for a given mechanical system?	What is the mechanical component size viewed in kW and net tons for your selected topology?
5.6	Are the mechanical module sizes typical "trade" sizes?	What is the typical industry size for your key mechanical components – air handlers, pumps, chillers, coils, piping and the like?
5.7	Based on the module size, what is the minimum number of mechanical modules needed for the initial build?	Fully consider your Class rating when determining the number of modules for your initial build
5.8	Based on the module size, what is the minimum number of mechanical modules needed for the ultimate build?	Fully consider your Class rating when determining the number of modules for your ultimate build
6	<i>Space Planning Checklist</i>	
6.1	Knowing the data center development phases and physical sizes from before, what space is required for the associated electrical system?	What is the space size for a given module?
6.2	Does the electrical room require partitioning at this Class level?	
6.3	How many electrical module spaces are required?	
6.4	Do the electrical spaces need to be contiguous?	
6.5	Do the electrical spaces need to be adjacent to each other?	
6.6	Do the electrical spaces need to be adjacent to their data center module(s)?	
6.7	Are there any specific requirements for the electrical rooms to be on an outside wall, have direct access to the outdoors, or possess specific exiting requirements?	
6.8	Does the mechanical room require partitioning at this Class level?	
6.9	How many mechanical module spaces are required?	
6.10	Do the mechanical spaces need to be contiguous?	
6.11	Do the mechanical spaces need to be adjacent to each other?	
6.12	Do the mechanical spaces need to be adjacent to their data center module(s)?	
6.13	Are there any specific requirements for the mechanical rooms to be on an outside wall, have direct access to the outdoors, or possess specific exiting requirements?	

6.2.1.3 Additional Information

The space required for the power systems will be proportional to the required capacity and level of redundancy/reliability of the electrical systems. It is not proportional to the square footage of the computer room alone. For example, a power system for a 1,000 m² (10,000 ft²) computer room with a total critical capacity of 1 MW will require roughly the same physical space as a 500 m² (5,000 ft²) computer room with a total critical capacity of 1 MW at the same redundancy/reliability level.

The following is a partial list of electrical equipment, components, and systems that should be included in the space plan:

- Equipment typically installed in dedicated electrical rooms outside the main computer area:
 - Service entrance switchgear (medium or low voltage, metal enclosed, or metal clad)
 - Unit substation (medium voltage)
 - Tie breaker section for dual entrance configurations
 - Generators (indoor/outdoor)
 - Generator paralleling switchgear
 - Automatic transfer switches (ATS)
 - Load banks (permanently installed or portable load banks on trailers requiring connection to electrical systems)
 - Distribution boards (critical loads, noncritical loads, life safety loads)
 - Transformers
 - Centralized UPS - static system or rotary system
 - UPS battery room (static or rotary system with flooded cell batteries)
- Equipment typically installed in the computer room spaces:
 - Power distribution units (PDUs), with or without transformers and static transfer switches, depending on the UPS design and load requirements
Power distribution unit (PDU) equipment may be located outside the computer room in adjacent space. The benefit to locating the PDU equipment outside the computer room is that the electrical operations and maintenance activities are outside the critical computer room space.
 - Remote power panels (RPPs) – cabinet or rack mounted panels used to provide a concentration of breakers, typically close to the load
 - Power strips within each cabinet that provide power dedicated to the specific cabinet
 - Distributed UPS located in close proximity to the loads they support (i.e., rack or row level) with immobilized electrolyte batteries (e.g., VRLA)

Consider whether these systems are to be built-in-place, factory-build modules, or containerized solutions. While they typically reside outside of the data center space, these electrical systems may be included in more comprehensive solutions that include the mechanical and IT space in one built solution set.

When a factory-assembled, modular, or containerized electrical system is chosen for the power solution, the considerations of these system to the non-modular portions of the data center is typically different than if the electrical systems were built in place. Consider items such as installation during construction, additions to the electrical system during ongoing operations, and protection from weather for systems installed outdoors.

6.2.2 Electric Utility Service Feeds

6.2.2.1 Single Entrance Single Pathway

6.2.2.1.1 Recommendations

Independent electric utility service feeds and associated switchgear should be located in a dedicated space that is adjacent or in close proximity to the primary data center electrical distribution space.

6.2.2.2 Single Entrance/Dual Pathway

6.2.2.2.1 Recommendations

The electric utility service feeds and associated switchgear should be located in a dedicated space that is equally distanced between or in close proximity to the dual data center electrical distribution spaces.

6.2.2.3 Dual Entrance/Dual Pathway

6.2.2.3.1 Recommendations

Independent electric utility service feeds and associated switchgear should be located in dedicated spaces separate from each other. Utility entrance space A should be located adjacent to electrical distribution space A, and utility entrance space B should be located adjacent to electrical distribution space B. A catastrophic event affecting one should not affect the other.

6.2.3 Generator Power

6.2.3.1 Indoor/Outdoor Installations

6.2.3.1.1 Introduction

Locating the generators either indoors or outdoors is based on site and client specific requirements.

While there may not be a large difference in cost between locating the generators indoors or outdoors, factors to consider during the evaluation of generator location include:

- Indoor generators
 - Placement of indoor generators in an area of the building with the lowest cost per square meter to construct
 - Additional costs for items associated with an indoor implementation, such as automated louvers, noise reduction/mitigation, and exhaust management
 - Requirements for weight, vibration, lateral structure, and fire rating of surrounding surfaces of the space intended for a generator
 - Fuel tank capacity and location
 - Accommodation for future generators
 - Local and building regulations, codes, or standards
- Outdoor generators
 - Increased exposure to physical and weather-related damage
 - Requirements for weight, vibration, lateral structure, and fire rating of surrounding surfaces of the space intended for a generator
 - Fuel tank capacity and location
 - Accommodation for future generators
 - Energy considerations; incentives for off-grid operation
 - Air quality or noise abatement restrictions
 - Local and building regulations, codes, or standards

6.2.3.1.2 Requirements

Generators installed outdoors shall be installed within shelters.

Generator exhaust systems shall be located so that they do not flow into building ventilation air intakes, preferably on the prevailing downwind side from building ventilation air intakes.

6.2.3.1.3 Recommendations

It is recommended that generators are installed indoors. With sufficient clearances, indoor generators are easier to monitor and maintain, especially during extreme weather conditions when their operation may be required.

6.2.3.2 Onsite Fuel Storage

6.2.3.2.1 Introduction

Space planning will need to account for onsite fuel storage. The quantity of fuel that is required and can be stored will be affected by the following:

- Availability of backup or disaster recovery site for applications supported by the data center and expected time required to recover applications at the backup site
- Proximity of the data center to locations or services, which provide fuel replenishment
- Priority status of the organization and response time for fuel replenishment during regional disasters, such as earthquakes, floods, and hurricanes
- Criticality of applications and regulatory requirements
- Business drivers requiring self sustaining operations

<List continues on next page>

- Security considerations
- Protection from the elements (e.g., floods, storms)
- Location of fuel pumps
- Local codes and acceptance by the AHJ
- Environmental requirements

Storage of large amounts of fuel onsite may trigger extensive jurisdictional and environmental permit reviews. Also, the permitting process may be more stringent for underground storage tanks (UST) than for aboveground storage tanks (AST).

6.2.3.2.2 Recommendations

The minimum amount of generator fuel storage required should be between 8 and 96 hours running at full load, depending on the data center availability requirements.

Depending on specific owner needs, the required amount of fuel storage or availability required may be far greater than four days.

6.3 Cooling Capacity

6.3.1 Introduction

The space required to support the cooling systems will vary depending on the type of cooling system selected. Items to consider include:

- Central air handlers versus perimeter CRAC units versus in-row, ceiling mount, or point-of-use cooling systems
- Chilled water versus air-cooled systems
- Liquid-cooled cabinets in the computer processing area (including, but not limited to, controlled racks, rear door heat exchangers, cold plate technology, or even liquid directly to the ITE)
- Immersion-based cooling in which the electronic equipment is continuously and horizontally submerged in tanks of liquid coolant instead of the traditional mounting style in vertical air-cooled racks
- Cooling tower (chilled water system)
- Thermal storage (chilled water system)
- Piping and pumps
- Other required equipment or resources

As with the electrical systems, consider whether these systems are to be built on site or are to be factory built modules or containerized solutions. While they typically reside outside of the data center space, these mechanical systems may be included in more comprehensive solutions that include the mechanical and IT space in one built solution set and may also require a commitment to a cooling solution early in the facility's lifetime.

See Table 6-2 regarding the decisions affecting capacity planning for mechanical systems.

6.3.2 Recommendations

Mechanical infrastructure for the data center should be isolated and separate from the base building mechanical systems if the building is not exclusively dedicated to the data center function.

The cooling system design capacity should be sufficient to support the electrical distribution system and subsystem cooling requirements within each cabinet, rack, or ITE zone. Cooling equipment and ITE should be powered separately.

When a factory-assembled, modular, or containerized IT system is chosen for the IT program solution, the considerations for these systems is typically different than non-modular portions of the data center with mechanical systems that were built in place for specified component size, system configuration, and cost. Considerations include installing these systems during construction activity, the effects of adding to the mechanical system during ongoing operations, and aligning additions with ITE system additions.

Just as there are considerations for the number of utility feeds for the electric service, there should also be equal consideration for how to keep the cooling system up to the required reliability and resiliency of the desired design point. Especially if the cooling system is going to be configured in an N + x or 2N fashion, then there should also be considerations about the number and placement of water ingress and outlet points, primary/variable loops as opposed to dual redundant loops, maintenance capabilities on all different parts of the system with minimal or no impact on the rest of the system, failover capabilities, etc.

Table 6-2 Liquid and Air-Cooled System Options and Primary Design Parameters

<i>Type of System and Related Parameters</i>	
<i>For a liquid-cooled system</i>	<i>For an air-cooled system</i>
What type of liquid-cooled system? • Cooling water system ○ Cooling towers ○ Direct evaporative cooling (mist cooling etc.) ○ Indirect water cooling (sea/river or groundwater used to remove heat from the cooling water via heat exchanger or similar method) • Chilled water system ○ Air-cooled (dry) chillers ○ Water-cooled (wet) chillers ○ Absorption chillers (for facilities with on-site cogeneration capabilities) • Immersion cooling	What type of air-cooled system? • DX cooling system Usually less efficient than water based cooling, but is more flexible and scalable. • Free air cooling Highly efficient, but it only works at certain climates, and needs ITE with high environmental tolerances. Usually supplemented with DX or evaporative cooling. • Indirect air cooling Uses heat exchangers with outside air. Less restriction on climate than free air cooling, but at higher initial cost.
Decide on following parameters: • Chilled water/cooling water temperature settings (supply and return) • Water pipe diameters • Pump capacity and speed • Chemical additives It is desirable to maintain laminar flow inside pipes to reduce pump power requirements. Minimizing the number of bends and valves in the main pipes and increasing the bend radii reduces the minimum pump power needed. Both pipe sizes and pump ratings must look forward into 5-7 generations of ITE needs (15-20 years) • Whether to adopt thermal storage ○ Capacity? (minutes or hours) ○ Where? (underground or outdoors)	Decide on following parameters: • Air duct cross sections • Fan capacity and speed • Heat exchanger capacity (if applicable) As fan power rises proportional to the 4th power of air speed, secure as much duct space as possible in order to reduce air speed. Minimizing the number of bends and dampers in the main pipes and increasing the bend radii reduces the minimum fan power needed. As air-based cooling is more amenable to modular design, forward capacity planning is less critical than for water-based cooling, but module size needs to be carefully determined.

The next consideration should be how to achieve cooling in the computer room itself without exposing the ITE to potential water leaks. There are various methodologies to achieve this, including putting the CRAC/CRAH units just outside the computer room such that all the water piping is outside of that space, using various types of heat exchangers outside of the room that connect into the cooling inside the room to remove heat from the air or refrigerant back into the water loop, etc. Various refrigerant systems are fully compatible with ITE rooms because if there is a leak, then the refrigerant turns to a gas at typical room temperatures, thereby protecting the equipment from moisture. Also remember that water has been placed inside the computer room for almost 40 years with few ill effects (such as for mainframes), so it is now coming back into vogue especially in data centers where water goes directly into a cabinet-based cooling system or even directly into the ITE itself to remove the heat with very little need for air movement.

6.3.3 Additional Information

The space required for the cooling systems will be proportional to the required capacity and level of redundancy/reliability for the overall design specification. It is not necessarily proportional to the size of the computer room space alone. For example, the cooling system for a 1,000 m² (10,000 ft²) computer room with a total critical capacity of 1MW will require roughly the same physical space for the cooling infrastructure as a 500 m² (5,000 ft²) computer room with the same critical load (when utilizing the same type of cooling system in both cases). Note, however, that large changes in the assumed rack power density will probably lead to different design choices for the cooling system as well. A key consideration is that as rack power density increases, so does its heat load and the air volume that the ITE will require (unless they are directly liquid cooled, which is still fairly rare except in HPC applications). This means that for the best efficiency and ability to avoid equipment malfunctions or shutoffs because of over-temperature that a closely coupled cooling system should be utilized (which include a variety of methodologies, but usually encompass some type of air containment strategy).

6.4 Data Center Supporting Spaces

6.4.1 Adjacencies of Functional Spaces

6.4.1.1 Introduction

The appropriate adjacencies of spaces can be determined by performing an exercise of required staff and material flow. Figure 6-2 and Figure 6-3 show examples of staff and material flow through a data center; they are not meant to show the physical adjacencies, but they can be used to assist in identifying required functional adjacencies.

The adjacency of programmatic space between traditional and modular and containerized construction varies. In traditional construction, the developer may choose to deploy in phases in a single structure. Circulation paths, the grouping of support elements and the relationship to other buildings and non-data center elements is more flexible for the simple reason that the developer of the data center can define the overall shape of the building and the site.

For modular and containerized data center solutions, the expansion elements are set, either by:

- The physical size of the element, such as the amount of ITE racks that can be accommodated or the size of the supporting utility infrastructures.
- The quantity of modules or containers, especially as it is deployed against the common utility and telecommunications infrastructure that support those modules and containers.

Similarly, modular units and containers may:

- Be installed either indoors or outdoors
- Have dedicated utility and critical power electrical systems to each module or container
- Have a centralized or distributed alternate power source
- Utilize a central cooling plant
- May have multiple telecommunications entrance rooms and MDAs, depending on how the site is configured
- May have support space grouped unlike a traditionally built data center

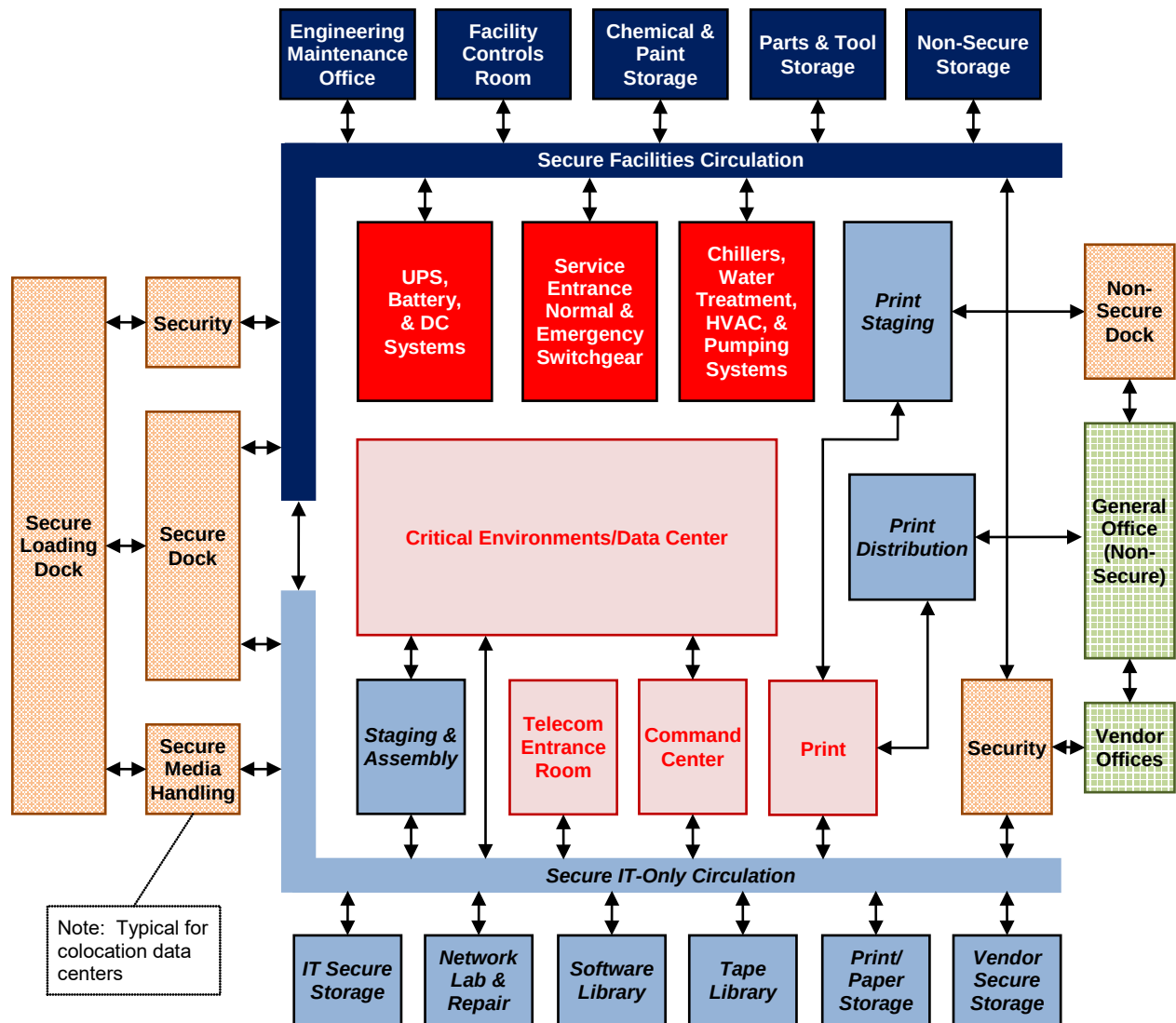


Figure 6-2
Space Adjacencies of a Traditional Data Center

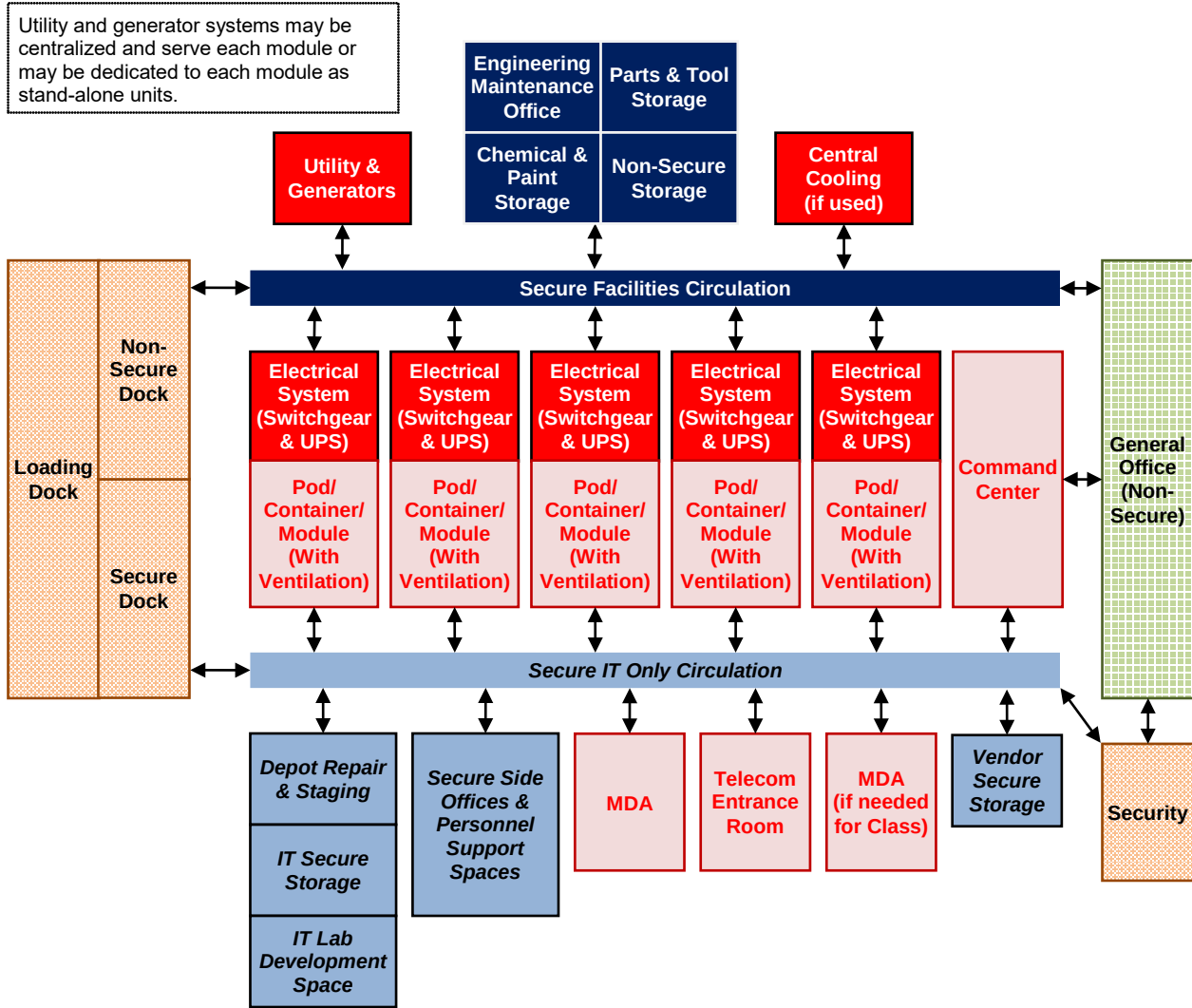


Figure 6-3
Space Adjacencies of Modular or Containerized Data Centers

6.4.2 Security

6.4.2.1 Recommendations

A security room should be located at or adjacent to the main personnel entrance to the facility.

Visitor sign-in area should be physically separate from the facility security operations.

The security room should include the security operations facility, including video monitoring and access control system database and front end user interface. When planning this space consider:

- Video monitoring space requirements
- Access control system space requirements
- Access control storage requirements
- Unobstructed access to key storage
- Unobstructed access to access-card (temporary and blank) storage
- Fire/smoke alarm monitoring systems
- Restricted access to the security control room

Refer to Section 12 for a detailed description of data center security requirements.

6.4.3 Telecommunications Entrance Room

6.4.3.1 Introduction

The function of the telecommunication entrance room is twofold:

- Provide a secure point where entering media from access providers can be converted from outdoor cable to indoor cable.
- House the access provider-owned equipment such as their demarcation, termination, and provisioning equipment.

Refer to Section 14 for a detailed description of data center telecommunications requirements.

6.4.3.2 Location

6.4.3.2.1 Requirements

The location and space requirements for distributors including MDA, IDA, and HDAs, shall be considered. The location of these distributors shall consider the maximum channel length of applications supported on the backbone cabling types to be installed.

6.4.3.2.2 Recommendations

The location of the entrance room with respect to the computer room should be designed to accommodate the distance limitations of circuits to be provisioned from the entrance room. Where possible, the entrance room should be adjacent to or be in a secured space within the computer room.

Pay particular attention to distance limitations for T-1, T-3, E-1, and E-3 circuits, the type of media these circuits utilize, and the number of DSX panels and patch panels in the channel. See applicable cabling standards (e.g., TIA-942-A for coaxial circuits) for guidance on the maximum distances allowed for T-3 and E-3 circuits in data centers.

The entrance room with the telecommunications main grounding busbar (TMGB) should be close to the main electrical grounding busbar to minimize the length of the bonding conductor for telecommunications (BCT), the conductor that interconnects the main electrical ground bar to the TMGB. The BCT shall be sized per applicable standards (e.g., TIA 607-B, NECA/BICSI 607).

6.4.3.3 Access Provider Considerations

6.4.3.3.1 Recommendations

Where access provision is contracted for the delivery of a service, the access provider's equipment and any associated cabling should be provided with adequate space. Separate or secured cable routes may be required between the entrance room and the access provider's equipment.

Where a separate entrance room is provided, access to the entrance room will be required by both the data center network operations staff and the access providers' technicians. Access to customer-owned equipment in the entrance room and the computer room should be secure from access provider technicians.

The entrance room should be sized to accommodate each anticipated access provider. The designer should meet with each access provider to determine its space requirements before sizing the entrance rooms. Additionally, cabinet and rack space will be required for customer-owned equipment and termination of cabling to the computer room and the rest of the building.

Where required by an access provision contract, each access provider will terminate its entrance cables and connect its equipment in cabinets or racks separate from the other access providers.

The entrance room may be divided into separate areas to provide separation between access provider-owned and customer-owned equipment. If the room is subdivided, there are typically only two spaces, one for the data center owner and one shared by all access providers. However, if there are multiple access providers, they may each request their own space. These requested spaces may be provided within the same room by using secure fencing, or they can be created through the use of walls.

The customer may ask all carriers to place demarcation equipment (patch panels, DSX panels, and IDC blocks) in shared meet-me or demarcation racks. Consolidating all patching to carrier circuits into meet-me racks and locating patch panels for cabling to the computer room in the same racks or adjacent ones simplifies cabling in the entrance room. Placing the demarcation panels and blocks adjacent to the patch panels that support cabling to the computer room allows circuits to be cross connected to the computer room cabling system using short patch cords. Carrier equipment included in the entrance room consists of carrier-owned patch panels, digital cross-connect (DSX) panels, routers, SONET, DWDM, and circuit provisioning equipment. The power requirement for the entrance room typically ranges from 500 to 1500 watts per access provider. However, the designer should meet with each access provider to determine its electrical, space, interface, and other facility requirements.

6.4.4 Command Center

6.4.4.1 Recommendations

The command center should have monitoring, but not control, capability for all the data center building systems so that the network and system administrators are fully aware of all data center critical building system alerts or alarms.

The telecommunications room (TR) that supports the command center and other nearby data center support spaces should be outside the computer room.

The work area communications devices within the command center may need connectivity back to two different supporting cross-connect fields. Network monitoring may need connectivity directly to the core network hardware located in the MDA space. Corporate LAN and telephony will need connectivity to the general telecommunications cross-connect serving non-computer room communications.

Some applications may require installation of large video displays easily visible to all command center personnel.

Depending on the data center, there may be need for CATV systems (local cable provider and satellite service).

6.4.5 Helpdesk

6.4.5.1 Recommendations

The helpdesk does not need to be located near the computer room and may be integrated into the general office space adjoining the data center. Alternatively, it may be acceptable to build the helpdesk and other general office space in a different building when there is no need for its location within the hardened portion of the data center facility.

Operator workstations for the helpdesk should be provided with critical electrical circuits fed from the backup generator and UPS systems to ensure that support functions are not disrupted by power fluctuations or blackouts.

6.4.6 Print

6.4.6.1 Requirements

Printer manufacturers' environmental criteria shall be included in the design parameters of the facility. Typical environmental parameters that are unique for a print room are humidity and temperature.

6.4.6.2 Recommendations

Printers should be located within a dedicated print room separate from the main computer room. The print room should have its own dedicated air handling system.

Power systems supporting the print functions should be considered critical and supported by the backup generator and UPS systems.

The facility layout should include:

- A separate paper storage room near the print room
- A suitable route from the loading dock to the print room and paper storage room to facilitate the movement of bulk paper products on pallets

6.4.7 Loading Dock

6.4.7.1 Requirements

A dedicated data center facility shall include a secure loading dock area.

6.4.7.2 Recommendations

Location of the loading dock should provide a step-free route through to the computer spaces with sufficient floor loading capacity to withstand material and equipment weights.

A dedicated data center facility should only have secure delivery capabilities such as a secure loading dock. A multi-purpose building with a data center should have a non-secure loading dock, separate from the data center, for general building deliveries.

For all high-value equipment, a secure loading dock should be provided. Some considerations when planning a secure loading dock include:

- Provision of an enclosed area for the delivery truck to protect deliveries from extreme weather
- Use of a dock leveler so that equipment can be safely moved from any type of delivery truck
- Monitoring of the area by the building CCTV security system with preference for security guards from the building's guard station to be able to visually monitor all activity
- Controlling access to the loading dock by the facility access control system with the system able to generate a history of all access attempts

6.4.8 Storage

6.4.8.1 Secured High Value

6.4.8.1.1 Recommendations

A secured storage area for high-value equipment should be located adjacent to a secured loading dock.

The space required for secured high-value storage is recommended to be a ratio of 1:10 in comparison to the computer room space. The minimum space recommended is 23 m² (250 ft²). The ratio may be reduced for large data centers depending on the specific operational practices.

The secured storage area should be monitored by the building CCTV security system or access controlled by the facility access control system. The system should generate a history of all access attempts.

6.4.8.2 Staging

6.4.8.2.1 Recommendations

All storage and unpacking activities should occur outside the computer room space, either in storage rooms or in staging areas. Preferably, a staging area should be located adjacent to the computer room. For high-value equipment, a staging area should be provided for unpacking and should be separate from any test-bench or lab space.

A staging area should have an air conditioning system separate from the computer room as cardboard boxes and packing materials can generate large amounts of particulates.

Because of the limited space within a lab, the staging area may be used to test and burn-in equipment for larger mainframe or high-end server space. However, this should not be a regular occurrence, and alternatives should be considered.

The staging area should be monitored by the building CCTV security system or access controlled by the facility access control system. The system should generate a history of all access attempts.

6.4.8.3 Vendor Storage

6.4.8.3.1 Recommendations

A secured storage area should be provided for vendors' equipment. The space needed depends on the number and type of vendors who will be storing equipment onsite.

The vendor storage area should be monitored by the building CCTV security system or located near or adjacent to a secured loading dock.

The security requirements for vendor storage should be the same as the staging area.

6.4.8.4 Print Storage

6.4.8.4.1 Recommendations

Print storage may be located adjacent either to a loading dock or preferably the print room.

6.4.9 Engineering Offices

6.4.9.1 Recommendations

The engineering offices should be located near the electrical switchgear, UPS, generator, chiller, and HVAC rooms with sufficient space provided for power and cooling engineers and support staff.

For offices, at least 10 m² (100 ft²) of office floor space should be provided with sufficient noise baffling from adjacent equipment rooms to meet ASHRAE NC rating of not more than 35 dB.

6.4.10 Administrative

6.4.10.1 Recommendations

The administrative or general office space may not require the same level of detailed construction as the data center and supporting back-of-house areas.

Items to be considered in the design of administrative space include:

- Disaster recovery and business continuity plans
- Operational policy during extreme weather conditions (e.g., what areas require staffing)
- Locations of emergency or “shelter in place” areas for personnel
- Future administrative space growth requirements, either as an expansion to the overall data center or as a stand-alone project
- Special function rooms such as a large conference or “war room” with wall-to-wall, floor-to-ceiling white boards

6.4.11 Environmental Design

6.4.11.1 Recommendations

Recycling and compliance with local environmental initiatives is recommended. Local, state, or national incentive programs might be available to underwrite some of the cost. Examples of environmental building best practices and metrics include:

- United States Green Building Council (USGBC), Leadership in Energy and Environmental Design (LEED)
- Building Research Establishment Environmental Assessment Method (BREEAM)
- U.S. Environmental Protection Agency (EPA): Energy Star for Buildings
- American Society of Heating, Refrigerating, and Air-Conditioning Engineers (ASHRAE): Building Energy Quotient (bEQ)

6.4.12 Waste/Recycle

6.4.12.1 Recommendations

As these facilities generate a large amount of boxes, packing material, and other waste, adequate space should be allocated for its handling. Frequency of removal, fire prevention/protection, local AHJ requirements, and dumpster requirements, such as size, access, and location, should also be considered.

Materials used in the construction of the data center facility should be recycled and/or locally-sourced whenever practical. Recycling and compliance with local environmental initiatives (e.g., Leadership in Energy and Environmental Design [LEED], BRE Environmental Assessment Method [BREEAM]) are recommended.

6.5 Placement of Equipment When Using Access Floors

Raised access floors are useful for distribution of cooling air, power and data cabling, and mechanical piping. However, as power density increases in data centers and operational efficiency becomes a high priority, and where seismic bracing is required, the use of forced air cooling via access floors is becoming less attractive. In addition, when cooling air shares the same space with cabling and piping, cooling management becomes a problem. Despite these concerns, raised access floors are still the most common feature of data center design.

6.5.1 Cooling

6.5.1.1 Access Floor Vents/Perforated Tiles

6.5.1.1.1 Requirements

When using floor cutouts below racks, cabinets, or vertical cable managers, the grommet system used shall not protrude above the access floor and interfere with proper installation of vertical cable managers and leveling of racks or cabinets.

6.5.1.1.2 Recommendations

While the exact locations of the required floor vents or perforated tiles are not typically known at the time the construction documents are issued for the flooring system, the general layout and approximate locations should be identified. The HVAC designer should coordinate the anticipated quantities with the technology consultant or end user and ensure that the construction documents require the appropriate number and type of cutouts for floor vents and quantity of perforated floor tiles. The exact locations can be validated prior to installation of the flooring system.

It is recommended that a computational fluid dynamics (CFD) model of the floor design be produced to ensure proper placement of floor tiles and that the cooling design will meet the design requirements.

Tile cutouts should have a means of restricting airflow for cutouts that are not fully populated with cabling. Open cutouts can cause more than 50% of the air supplied by the air handlers or CRAC units to bypass the perforated tiles.

The location of the tile cutouts and perforated tiles need to be coordinated with the specific design of the equipment cabinets and racks. If floor tile cutouts are used for cabling, open frame racks should have the floor cutouts positioned directly below the back half of the vertical cable management between each rack. Cabinets should have the floor cutouts positioned below the vertical channel that will be used for power and communications cabling within the cabinet.

Consider positioning cabinets with the front or back edges aligned with the edge of the floor tiles to allow the adjacent clear floor tile to be removed without interference from the cabinet.

Perforated floor tiles should not be installed until they are required. The efficiency and performance of the air distribution system will be affected by additional perforated floor tiles.

6.5.1.2 Ducting

6.5.1.2.1 Recommendations

Ducting may be required, particularly for computer rooms without access floors.

There are many factors that may impact the choice of ducting (or not) as well as the type, placement, size, etc. For air containment purposes, it is becoming common to have duct work added to the back or top of a rack which then goes into either a ceiling return plenum or a dedicated set of duct work overhead, which takes the expelled hotter air back to the cooling units. Another variation is to use duct work to bring in the cooled air into a cold air containment aisle, which is more commonly used in "free" air cooling systems or in very high density environments. In any of these circumstances, an understanding of the maximum volume of air, acceptable flow rates (velocity), additional fan assist or not, etc., needs to be considered for the duct system. Lastly, for space planning purposes, duct work that may be exposed to low temperatures and/or high humidity will probably need to be wrapped in insulation to avoid condensation problems, which can take up a lot more space than the ductwork itself.

6.5.1.3 Air-Handling Units

6.5.1.3.1 Recommendations

The exact location of the air-handling units should be coordinated between the mechanical engineer, technology consultant and end user to ensure that an optimal equipment layout can be determined without hindering airflow requirements or utilization of floor space.

If air handlers are required to be located within the computer room area because of the size and density of the data center, coordination is required to ensure that the technology equipment layout and low-voltage cable routing is not constrained.

6.5.2 Power Distribution

6.5.2.1 Remote Power Panels (RPP)

6.5.2.1.1 Recommendations

RPP locations should be coordinated with the technology equipment layout. The preferred RPP configuration is to place the RPPs at one or both ends of cabinet rows.

6.5.2.2 PDU Placement

6.5.2.2.1 Recommendations

The preferred location for PDUs is in a service gallery (a space outside, but adjacent to the computer room). This location is subject to the approval by the AHJ and if the feeder distances to the remote power panels allow such a placement. Security for this space should be the same as for other critical electrical and mechanical spaces.

6.5.2.2.2 Additional Information

The advantages of this approach are that it removes a maintenance item from the computer room, removes a source of heat (if provided with transformers), and allows the PDUs to be located in less expensive space. The disadvantages are less efficient use of building foot-print and much longer PDU cables. The cables must pass through computer room walls (which may not be permissible by local codes), and the PDUs may not be listed for applications outside of the ITE room.

6.5.3 Fire Protection Systems

6.5.3.1 Requirements

Spacing requirements for fire protections systems shall meet applicable fire codes and requirements of the AHJ.

For computer rooms with an access floor, fire suppression below the floor shall be required and shall be the same method as that used in the work space above the floor.

NOTE: See Section 11, the *International Fire Code*, and NFPA 75 for additional requirements and information.

6.5.3.2 Recommendations

Space for fire protection system detection and protection equipment in the data center space should be coordinated with the fire protection system engineer.

Sufficient aisle space should be provided and coordinated with ceiling mounted fire detection and protection devices.

The placement of fire detection and protection devices, which are installed below the access floor (including sprinkler or gaseous suppression piping and tanks), should be coordinated with all power and communications underfloor pathways and placement of technology equipment situated on the access floor.

6.6 Information Technology Equipment Placement in a Computer Room With an Access Floor

6.6.1 Telecommunications Spaces

NOTE: See Section 14 of this standard and TIA-942-A for more information on telecommunications spaces.

6.6.1.1 Introduction

The computer room will support one or two main distribution areas (MDA) and can support several horizontal distribution areas (HDAs). Some computer rooms require only a single MDA, however a second MDA is often deployed to provide redundancy.

The main distribution area will support the main cross-connect for the computer room and network equipment for the computer room (e.g., core routers, core LAN switches, core SAN switches, firewalls), and it can support a horizontal cross-connect for portions of the computer room near the MDA.

The horizontal distribution areas support horizontal cabling to equipment areas (e.g., server cabinets) and LAN, SAN, console, or KVM (keyboard/video/mouse), or other edge layer switches.

The entrance rooms, MDAs, and HDAs need to be carefully situated to ensure that maximum cable lengths for applications to be used in the data center are not exceeded (e.g., WAN circuits, LAN, SAN).

Whereas a small data center may only have an MDA and no HDAs, TRs, or entrance room, a large data center may require multiple entrance rooms to be able to provision circuits in all locations of the data center.

Larger data centers will require more HDAs, not only to ensure that maximum horizontal cable lengths are not exceeded, but also to avoid cable congestion. HDAs should not be so large as to completely fill all cable pathways feeding the HDAs during initial occupancy. Because of the high density of cabling in data centers, HDAs are more often required in data centers to avoid cable congestion than to avoid maximum cable length restrictions.

Various types of fire protection systems will take up different amounts of space, both internal to the computer room as well as in the mechanical spaces and outdoor mechanical yard. For instance, a water-based sprinkler system will need space throughout the ceiling areas for proper spacing and dispersal. A clean agent gaseous system requires some space at the periphery of the ceiling areas, but it also requires a space set aside to contain the gas holding tanks as well as possible duct work to release the gas to the outside atmosphere once it has quenched the fire.

Additionally, utilizing hot or cold aisle containment systems can have an impact on space planning since it may mean that more detection and suppression components be put into place for each contained area. For example, many fire codes and fire marshals require most detection and mitigation points to align with the rows and be able to penetrate into the containment system itself. Some AHJ's even require detection equipment inside of very large ITE such as large scale robotic tape arrays. Also note that most data centers implement some type of very sensitive smoke detection system (e.g., very early warning fire detection system) in addition to regular smoke and fire detection, so space needs to be planned for this pipework and detectors.

6.6.1.2 Requirements

The specific fire protection system used shall meet AHJ requirements.

6.6.1.3 Recommendations

If the computer room has two MDAs, they should be physically separated. It may not be necessary to place the MDAs on opposite ends of the computer room if such a configuration causes cable lengths for distance-limited applications, such as T-1, T-3, E-1, E-3, and SANs, to be exceeded.

Computer tapes, printer paper storage, and other flammable media should be located in rooms separate from the computer room.

Production, development, and test systems should be in separate areas of the computer room, preferably in separate rooms served by dedicated networks.

Separate areas of the computer room may be designated to accommodate special structures or cabinets for equipment with high heat loads.

NOTE: See Section 11 of this Standard, the *International Fire Code*, or NFPA 75 for additional requirements and information concerning record storage and fire issues.

6.6.2 Racks, Frames, and Equipment

NOTE: Section 14.12 contains additional information regarding cabinets and racks.

6.6.2.1 Rack Unit Capacity

6.6.2.1.1 Recommendations

The amount of ITE that should be placed within a cabinet will depend on many factors that vary for each hardware platform, data center, and organization. For example, each organization has its own practices for populating cabinets, and some may prefer not to install servers in all positions, leaving room for patch panels, switches or ease of maintenance.

ITE implementation planning should consider occupying cabinets based upon:

- Platforms (e.g., appliance servers, mid-range, blade servers)
- Departments, independent of platforms
- Occupancy to the desired density independent of platform or departments

Adequate space should be allocated for patch panels, switches, power strips, and cabling for the cabinet when it is at its desired maximum capacity. Patch panels and power strips should not be placed directly behind servers as this may impede access and airflow to the rear of these systems.

The availability of power and cooling, rather than space, may limit the amount of ITE per cabinet or rack. As equipment power densities continue to increase, it is recommended to design the data center so that space constraints are realized before power and cooling constraints.

For any data center design, there are always tradeoffs, such as:

- Availability of power (and its redundancy factors)
- Availability of cooling (and its redundancy factors)
- Weight load capabilities
- Space for ITE

A number of decisions should be made at the very beginning of the design phase. The mission critical aspects of the applications running on the equipment will have a direct bearing on:

- Power and cooling redundancy and space planning
- Maximum cabinet density and weight that will be supported
- Ability of the power and cooling to be flexible enough to allow for high variability or low variability of cabinet densities. (i.e., Can several high density racks with blade servers coexist in a general low density environment without disruption?)
- Usage profile of the ITE. For example, if it is a testing environment with a high rate of change, then the racks may not be fully populated. If in a stable production operating environment, it may be possible to make a lot more efficient use of available cabinet and rack space.

The point is that eventually a resource will be exhausted prior to the others, so that resource should be anticipated and addressed at the very beginning of the design cycle to ensure that the most important features to the business are identified.

To ensure that the initial and ultimate power and cooling system capacities will meet the anticipated demands, validate power consumptions either by performing measurements or by obtaining actual power consumption data from manufacturers. Note that nameplate data typically gives maximum power consumption versus typical operating power consumption. Use of nameplate data alone can result in oversizing power infrastructure by as much as 30–50%.

Any unused rack space should be filled with blanking devices to reduce any nonfunctional airflow migration through the equipment rack.

Initial and ultimate system weight loads should be used when verifying the structural design parameters of the various platforms that will be installed within the computer room.

6.6.2.2 Network Racks

6.6.2.2.1 Recommendations

When arranging the computer room space and organizing the hot/cold aisle locations with respect to the cabling and cabinets, consider future changes. There are generally two (2) types of common network racks, open frame (either 2 or 4 post) or enclosed cabinet racks. If the computer room will primarily utilize open frame racks, then for future flexibility, it makes sense to put them into areas that would allow for the rest of the ITE racks to be easily grouped together to create either a hot or cold aisle containment system. Typically, this means putting them out on the edges of the computer room, at the end of rows, or if cable runs must be kept short, then both at the end and middle of the row.

Alternatively, if network equipment will be primarily located in enclosed cabinet racks, then another space consideration is to utilize wider (700–800 mm wide instead of the more typical 600 mm wide) racks to allow for internal baffling to be installed allowing a side-to-side cooled piece of equipment to fit into a row of front-to-back cooled equipment.

If redundant network equipment is not located in the same cabinet or rack, these cabinets or racks should be separated to ensure facility infrastructure (power, cooling) diversity. This also provides for physical separation of the cabling pathways and cabling from the redundant network equipment to the servers that are connected.

The areas in the computer room where the entrance rooms, MDAs, and HDAs are located may be secured with caging. This may be an end user requirement, depending on internal operating procedures and security requirements.

6.6.2.3 End Equipment Cabinets and Racks

6.6.2.3.1 Requirements

For new installations, a preliminary layout of cabinets and racks shall be completed prior to establishing the reference point for the access floor grid in computer rooms, entrance rooms, and TRs. The preliminary layout shall anticipate logical groupings of equipment, flush front alignment of cabinet and rack rows, heat and energy density, proximity to ducting and cooling, and worst-case cabinet depth.

The required clearances for the equipment cabinets, access floor grid, and internal columns will determine where the front alignments of rows of cabinets and racks are best located. When an access floor is deployed, the access floor grid shall line-up with the preferred layout of the rows of cabinets and allow for easy removal of tiles.

Rear access (or hot aisle width when deployed in hot aisle/cold aisle arrangement) shall allow for minimum service clearance appropriate to the voltage of the equipment per applicable local codes and regulations. Typical hot aisle clearance requirements are 0.9 m (3 ft) to 1.2 m (4 ft) or greater. Because all equipment may not be known at the time of the initial layout, a final layout with adjustments may be required after the access floor grid has been established.

For existing installations, the access floor grid has already been determined. An equipment layout and alignments shall be made with the same considerations as in the previous paragraph based upon the existing floor grid.

6.6.2.3.2 Recommendations

Cabinets should be sized as described in Section 14.12 to provide adequate space to install redundant power strips and vertical cable management in the back of the cabinets.

High density of servers within cabinets, higher density port counts per server, and the number of power cords per server create significant cable and cooling management issues within the server cabinets, particularly those with a 600 mm (24 in) width.

NOTE: Some of the newest generation ITE now have cabling (network, power, or both) on the front of the servers to allow for easier access and management, which necessitates the front mounting rails to be placed deeper into the rack to allow for cabling management in the front of the rack. However, this placement may affect cooling, especially if hot aisle containment or rear mounted chimney systems are being used.

Prior to committing to a standard cabinet size, the end user(s) should review, and have vendors provide mock-ups of the various cabinet configurations that will be implemented. A mock-up of the worst-case configuration with maximum number of anticipated servers and cabling should also be provided. Upon completion of the mock-up, power and heat loads should be recalculated to ensure that adequate power and cooling are delivered to the cabinet.

Additional room for cable management can be gained by increasing the depth or width of the cabinet. However, increasing the width of the cabinets will reduce the number of cabinets that can be installed in the computer room.

When equipment cabinets or racks are installed adjacent to each other, thus forming a continuous aisle, the number of cabinets or racks within one row should not exceed twenty. Where one end of an aisle is closed off or has no personnel exit, the number of cabinets and racks within one row should not exceed ten racks/cabinets. There may be AHJ restrictions on the length of an aisle, which will take precedence over these guidelines.

The layout of the computer equipment, electrical equipment, and air conditioning equipment should be done concurrently. One recommended method is to place the RPPs on the ends of the cabinet rows.

Cabinets and racks should be placed to permit access floor tiles in front and in back to be lifted. When an access floor is used, it is a good practice to align one edge of the cabinets flush with one edge of the floor tiles, preferably the front edge to maximize cold aisle airflow by leaving at least two tile positions for perforated tiles.

In hot/cold aisle floor layouts, there should not be any gaps in the cabinet row. All gaps should be eliminated to minimize hot air migration into the cold aisle.

6.6.2.4 Large Frame Servers

6.6.2.4.1 Requirements

The layout of the large frame servers shall be coordinated with respect to weight loads, cooling airflow, power and network connectivity requirements, as they will not fit within the standard server cabinet space. Consult the manufacturer to determine what side access is required (if any).

6.6.2.4.2 Additional information

Some large frame servers have extremely complicated airflow patterns, which may include a combination of bottom to top, front to back, front to top, and even side to side. It is critical to get a detailed description of the requirements from the vendor in order to correctly situate the server to allow for proper cooling. It is not uncommon that a large frame server may have to sit off by itself, away from other racks, to allow for all of the airflow to work properly, and this takes up quite a bit of floor space to accommodate.

6.6.2.5 Storage Devices

6.6.2.5.1 Requirements

The layout of storage devices shall be coordinated with respect to weight loads, cooling airflow, power, and network connectivity requirements as they may not fit within the standard server cabinet space. Consult the manufacturer to determine what side access is required (if any).

6.6.2.5.2 Additional information

Some storage devices and disk arrays have extremely complicated airflow patterns, which may include a combination of bottom to top, front to back, front to top, and even side to side. It is critical to get a detailed description of the requirements from the vendor in order to correctly situate the storage devices to allow for proper cooling. It is not uncommon that some storage devices are located away from other racks, to allow for all of the airflow to work properly, which takes additional floor space to accommodate. Additionally, the amount of physical disk drives in a single cabinet can easily exceed the floor weight loading characteristics, and it is not uncommon to put down some type of reinforcing plate across extra floor tiles or channel bases under the floor to allow for the placement of the disk cabinet.

6.6.2.6 SAN Frames

6.6.2.6.1 Recommendations

SAN frames are network racks that provide the infrastructure to terminate the media that provide connectivity to the servers. SAN frames typically consist of large quantities of high-density optical fiber termination panels, so they should be located within the SAN equipment area.

SAN frames need to provide proper optical fiber cable management to facilitate interconnects from the patch panels to the SAN equipment.

Where the SAN frames consist of fabric core switches and edge layer switches, the edge layer switches and core switches should be installed in separate racks because the number of edge layer switches may increase. In addition, the amount of moves, adds, and changes at the edge layer is typically much higher than at the core layer. Some SAN frames contain equipment that is primarily side-to-side cooled, so it is common to have them mounted in a wider rack (typically 800–900 mm wide) with internal ductwork to allow for front-side provided air to be directed into the rack, through the side-to-side cooled equipment and then out the back of the rack. Therefore, it is important to consider the additional space that these SAN frame racks can take up in the computer room.

6.6.2.6.2 Additional information

Some SAN implementations require centralization of SAN storage and switches. Other SAN implementations use core-edge SAN architecture with core switches in the MDA and edge layer switches in the HDA.

6.6.3 Aisles

6.6.3.1 Orientation

6.6.3.1.1 Recommendations

For rectangular computer rooms, equipment rows may be run parallel to either long or short walls. The optimum configuration should be determined by examining both options.

However, there can be many complicating factors to consider, including:

- Column placement
- Size and shape (e.g., circular, rectangular, or H-beam)
- Effective "throw" of the CRACs (if used)
- Locations where the most and least air volumes will be available

If utilizing alternative cooling methodologies such as rear door heat exchangers, actively cooled racks, immersion systems, etc., it may be necessary to reconsider the standard hot/cold aisle arrangement. Additionally, it is not uncommon to encounter non-rectangular computer rooms, which add additional complications to the planning process for rack layouts. For best results utilize a combination of a CAD system for overall space efficiency and a CFD modeling system for power and cooling capabilities.

6.6.3.2 Clearances

6.6.3.2.1 Requirements

The minimum width of an aisle shall be 0.9 m (3 ft), depending on local code requirements and voltage level present in cabinet.

6.6.3.2.2 Recommendations

There should be at least a 1.2 m (4 ft) clearance at the front of cabinets and racks to permit unobstructed access, equipment movement, and maintenance. Ceiling heights that are in excess of 3.7 m (12 ft) may require additional aisle space to maneuver support lifts to access ceiling mounted systems (e.g., lighting, fire detection and suppression systems).

Aisle widths may need to be 3 or 4 tiles (with a tile typically sized at either 600 mm × 600 mm or 24 in × 24 in giving a total space of 1800 mm to 2400 mm or 6 ft to 8 ft), depending on the HVAC engineer's analysis, requirements for planned equipment and the design of the cooling system.

As equipment is typically installed within cabinets from the front, the front aisle width should, at a minimum, be equal to the greatest value of the following:

- The anticipated depth of equipment to be installed within the cabinets
- The current or planned cabinet depth to permit replacement of cabinets
- The width required by local code(s) requirements and the AHJ
- 0.9 m (3 ft)

NOTE: Additional allowance should be provided if moving equipment (e.g., hand truck) will be used.

Clearance in front of racks and patching frames should provide for safe access and clearance to work. When the swing of a door encounters an obstruction, such as a building support column, a removable door or double (wardrobe) doors may be considered in place of a single door to facilitate full access to the cabinet content.

If the end user has an access floor environment that changes equipment between server cabinets and floor standing equipment frequently, it may be desirable to designate two rows of floor tiles for equipment and two rows of floor tiles for aisles (both hot and cold). This provides the flexibility that this particular situation requires, but does reduce the floor space utilization of the computer room,

6.6.3.3 Hot/Cold Aisles

6.6.3.3.1 Recommendations

The front of the cabinets and racks should be oriented toward the cold aisle. The cold aisle on an access floor should have at least two rows of floor tiles that can be configured with perforated tiles, providing the required flexibility in airflow management. Additional front (cold) aisle clearance may be required subject to HVAC and operational considerations.

For access floors, a minimum of two complete rows of floor tiles that can be removed should be provided in the hot aisles at the rear of the cabinets and racks. This allows the designer to make use of two rather than one row of tiles for cable trays.

With 1300 mm (52 in) deep server cabinets and the front of the cabinets aligned with the edge of a 600 x 600 mm (24 in x 24 in) floor tile in the cold aisle, there would be 100 mm (4 in) of overlap into the hot aisle, blocking the tiles, which would necessitate an additional row of floor tiles that can be removed (see Figure 6-4).

If cabinets or equipment have a depth that is greater than 1050 mm (42 in), then there will need to be coordination with the hot and cold aisle configuration to ensure that the required clearances are provided.

6.6.3.4 Aisle Containment

6.6.3.4.1 Introduction

The effectiveness and efficiency derived from hot and cold aisle separation may be enhanced for air-cooled ITE by a method known as “containment”. The objective of containment systems is to prevent mixing of hot exhaust air with cold intake air. This technique can dramatically increase the efficiency of the cooling systems, improve the lifetime of the cooling equipment, and reduce operating cost. Air isolation management via containment can eliminate hot spots, support high load densities, reduce cooling unit fan energy consumption, increase cooling unit coil efficiency, reduce chiller plant operating energy costs, increase access to economization free cooling hours, and reduce dependence on raised access floor construction. Space planning for hot or cold aisle containment may not need to be much different from that for standard hot aisle and cold aisle space planning, depending upon the method used. The most common containment methods are known as “hot aisle containment” or “cold aisle containment”, as appropriate. A third variation is known as “hot air collar” (also called a “chimney” or “air removal unit”). These techniques are discussed in the following subparagraphs.

In aisle containment systems, the hot or cold aisle is enclosed, usually with transparent, fire-resistant materials. The materials can be solid or flexible. A number of variations are possible, including:

- Fully enclosed hot aisle with in-row cooling — In this method the aisle is fully enclosed. The characteristics include:
 - Cabinet-mounted ITE with front-to rear airflow (i.e., cold intake air in the front and hot exhaust air in the rear)
 - Blanking panels in all empty equipment slots of the IT cabinets; no openings in or between cabinets that could allow transfer of air between the hot and cold aisles
 - A ceiling over the hot aisle (typically transparent, flame retardant plastic)
 - Doors at each end of the hot aisle that open out (to allow emergency exit of workers inside the hot aisle)
 - Air conditioning units mounted in the two rows that draw in hot air from the hot aisle and blow cold air into the cold aisle. Computer modeling may be necessary to determine the appropriate quantity, size, and placement of the cooling units.
 - Raised floor not required
 - Exhaust air returns to cooling units at high temperature, thereby optimizing efficiency of the cooling unit
- Contained hot aisle with ceiling duct — This method is similar to the fully enclosed hot aisle, except that there is no “ceiling” over the aisle and there are no cooling units in the rows.
 - Aisle containment barriers extend all the way to the ceiling plenum
 - Hot air is drawn into ceiling-mounted cooling units, or is ducted to CRAC units located at the room perimeter or to cooling units elsewhere in the facility
 - Raised floor is not required

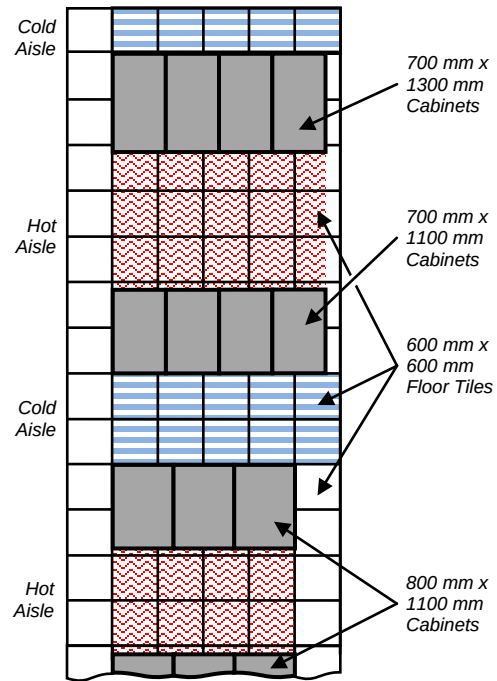


Figure 6-4
Example of Aisle Width With Different Cabinet Sizes

<List continues on next page>

- Partially contained hot aisle without ceiling duct — This method encloses the hot aisle as described above, but barriers do not extend all the way to the ceiling. Ceiling-mounted cooling units above the hot aisle draw in the hot air and blow cold air down into the cold aisle. Some mixing of hot and cold air occurs.
- Hot air collar — This method is a variation of the contained hot aisle with ceiling duct, except that each rack has a duct that extends to a plenum above the ITE rows. When installed on all equipment racks there is no need for hot aisles, hot aisle ceilings, or hot aisle doors. Installation of hot air collars on individual equipment racks is one method of eliminating hot spots. In order to prevent back pressure a fan may be required to ensure one-way hot air movement. The fan will consume some energy, but this slight loss of overall efficiency can be offset by eliminating the need for fully enclosed aisles. Workers are not exposed to extreme heat. Service or removal of one or more equipment racks has no effect on any of the adjacent equipment.
- Cold aisle containment — Cold aisle containment is nearly identical to the hot aisle methods described above except that, as the name implies, it is the cold aisle that is contained. Cold aisle containment minimizes the amount of cold air needed by the ITE by confining the cold air to the space directly in front of the ITE. Air from the hot aisle mixes with room air and is delivered to cooling units via return air ducts. The main advantage of cold aisle containment is that it is more easily applied to an existing data center, whereas methods such as fully enclosed hot aisles must be pre-designed. It can be used with raised floors, and it can be set to the air inlet temperature specifications of the ITE without affecting the rest of the room.

6.6.3.4.2 Requirements

One consideration for aisle containment is the impact on fire protection (see Section 11). An analysis shall be made to determine whether the installation of barriers will negatively impact the performance of fire detection and/or suppression equipment. ITE fans can draw inert, clean agent gas through the ITE. If water sprinkler systems are deployed, water spray patterns shall not be obstructed by the aisle containment. Elements of aisle containment and hot air collars shall be constructed of noncombustible material, limited combustible materials, or materials that have a maximum flame spread index of 50 and a maximum smoke development of 450. Smoke detectors within containment systems shall be rated for the intended temperature and air velocities of the space in which they are installed.

Per requirements of NFPA 75 and NFPA 76, elements used for air flow management (e.g., aisle containment, cabinet exhaust chimneys) shall be constructed of materials with a maximum flame spread index of 50 and a maximum smoke development of 450 as verified by either ASTM E84 or UL 723.

6.6.3.4.3 Recommendations

Aisle containment is recommended for air-cooled ITE in data centers where there are enough ITE racks to create rows and aisles. It may be necessary to install fire detection and/or suppression devices inside the contained space, or to modify existing detection and suppression systems in order to comply with local regulations. When aisle containment is implemented, best practice is to prevent any mixing of hot and cold air to the maximum extent possible. Partially contained aisles are the least effective. CFD computer modeling can help in the selection and placement of air containment techniques. Methods utilized should be reviewed and approved by the local AHJ prior to installation.

6.6.3.5 Location

6.6.3.5.1 Recommendations

Equipment cabinets and racks should have a minimum of 1.2 m (4 ft) and preferably 1.8 m (6 ft) of clearance between the cabinets and racks when air conditioning equipment and power distribution equipment are located along the perimeter wall. A 1.2 m (4 ft) clearance typically provides a sufficient aisle for the movement of large equipment, such as electrical distribution or air conditioning equipment, within the computer room.

Traditionally, air conditioning equipment and power distribution equipment are placed along the perimeter walls for distribution under raised, perforated tiles. When subfloor air distribution is used, there should be a minimum of 1.2 m (4 ft) and, preferably, 1.8 m (6 ft) of clearance between the server cabinets and the air conditioning equipment. The cold aisle should be a minimum of 2.4 m (8 ft) from the cooling units. This will help reduce the possibility of the effect in which air is drawn from above the access floor through the perforated floor tile because of low pressure caused by the high-velocity air below the floor near the discharge of the air conditioning equipment.

These distances are dependent on mechanical considerations such as the depth of the access floor, the absence or presence of turning vanes on the discharge of the CRAC unit, the speed of the air discharge, or the deployment of fans that are recessed under the access floor. Equipment cabinet and server row lengths may be limited by the maximum distance at which the air conditioning equipment can provide adequate air pressure for delivering cold air. This distance is a function of the CRAC unit blower, the access floor depth, the distribution of the perforated tiles, and cables or other obstructions under the floor.

When overhead or in-row cooling is provided, the CRAC units should be close coupled to the racks to be cooled, meaning that the cooling equipment should be as close as possible to the heat source. Close coupling minimizes hot and cold air mixing and improves efficiency because it minimizes the volume of air that must be cooled and the required fan energy needed.

6.6.4 Power and Telecommunications Cable Distribution

6.6.4.1 Introduction

Various configurations can be used to distribute power and telecommunications cables. See Section 14.7 for considerations of overhead versus under-floor cable routing.

6.6.4.2 Requirements

A telecommunications cable pathway under an access floor (such as cable trays or other containment), regardless of location, shall contain a maximum depth of cable of 150 mm (6 in) when fully populated.

When access floors are used, the bottom of the access floor tiles shall be:

- A minimum of 50 mm (2 in) from the top of the cable tray (if cables exit the cable tray from the top of the tray)
- A minimum of 200 mm (8 in) from the bottom of the cable tray if the cable tray is expected to be filled to the capacity of 150 mm (6 in) depth

Cable pathways shall meet the clearance requirements of fire detection, suppression, and prevention systems, and these systems must be coordinated with other systems (e.g., electrical, mechanical, telecommunications) and meet the requirements of the manufacturer and the AHJ.

Power cabling, when distributed under an access floor, may have to be plenum-rated and/or be run in raceway and/or meet other requirements of the local jurisdiction. Power cabling run overhead shall be run in cable trays compliant with local AHJ requirements.

6.6.4.3 Recommendations

Cable pathways should be sized for the maximum number of cable expected with a 50% additional capacity to allow for future growth. Cable pathway size should be calculated in areas of maximum density such as near MDAs and HDAs.

Where fiber optic cabling is installed under the floor, it should be protected from damage by placing it within a cable tray or other containment. There is no separation requirement between power and fiber optic cabling, except that which is required by the AHJ.

If both power and telecommunications cabling are distributed from below the access floor, then:

- The power cabling should be routed either adjacent to or within the cold aisle.
- The telecommunications cabling should be routed adjacent to or within the hot aisle.

This arrangement minimizes obstruction of airflow in the cold aisles by telecommunications cabling.

If both power and fiber optic telecommunications cabling are distributed from overhead, and copper telecommunications cabling is distributed from below the access floor, then:

- The optical fiber telecommunications cabling should be routed above the power cabling on separate containment and should be coordinated with mechanical and electrical systems above the cabinets.
- The copper telecommunications cabling should be routed adjacent to or within the hot aisles.

Power and communication pathways should be positioned at different heights off the floor so that they can cross each other without interference. Alternatively, at every point where the power and copper cabling cross the path of each other, the crossing should be at a 90° (right) angle.

6.6.4.4 Additional Information

Patch cabling within a row of cabinets and racks is often routed overhead to maximize the space available under the floor for horizontal and backbone cabling. This routing also separates patch cabling, which changes often, from horizontal and backbone cabling, which should be more permanent.

The data cabling standards used in the design provide guidance as to the recommended separation between power and copper telecommunications cabling to maintain signal integrity (e.g., TIA-942-A, ISO/IEC 14763-2, CENELEC EN 50174-2). Separation and segregation for safety shall be in accordance with the requirements of the AHJ.

6.6.5 Airflow Circulation and Equipment Placement Coordination

6.6.5.1 Recommendations

Consider the following items when coordinating placement of equipment, airflow, and cable routes:

- On-floor equipment:
 - Equipment type and dimensions
 - Orientation with respect to airflow direction
- Underfloor services:

For the following underfloor services, dimensions, clearances, and orientation with respect to airflow direction should be considered:

 - Electrical services:
 - Data cabling:
 - Ducting:
 - Fire suppression system:
 - Fire detection system:
 - Air conditioning pipes:

6.6.6 Information Technology (IT) Equipment Adjacencies

6.6.6.1 Proximity to EMI and RFI Energies

6.6.6.1.1 Recommendations

Where possible, exposure to sources of EMI and RFI should be avoided. Transformers, other than those in PDUs, should be placed a minimum of 0.6 m (2 ft) and preferably at least 1.2 m (4 ft) from ITE and data cabling.

6.6.6.2 ITE Access Space Requirements

6.6.6.2.1 Recommendations

The equipment access space for ITE and non-ITE should be coordinated so that access space can be shared whenever possible, maximizing computer room utilization.

6.6.7 Access Floor Grid Layout and Reference Point

6.6.7.1 Recommendations

The access floor reference point should be coordinated with the technology equipment layout, PDUs, CRAHs, chilled water piping, and associated valving.

The reference point should not be selected simply at one of the corners of the computer room without coordinating the placement of the technology equipment. While having the reference point at one of the corners is the most cost effective from an installation cost perspective as it results in the fewest partial floor tiles, it may not provide the most optimized technology layout. Additionally, the angle between the walls may be slightly more than a perfect 90° angle, resulting in an increasing gap between the access floor panels and the wall.

The best long-term solution may be to position the reference point some distance away from a corner to accommodate the maximum number of cabinet rows while still maintaining the required clearances.

6.7 Design For Efficiency

6.7.1 Holistic Energy Efficient Data Center Design

Historically, data centers have been designed in a piecemeal manner. Critical components, such as UPS systems, computer room air conditioners (CRACs), power distribution equipment, equipment racks, and the ITE are often specified and purchased separately without a view of how they could all fit together as one cohesive system. Likewise, the buildings in which many data centers are housed were not designed to provide the robust environment required to support and protect mission-critical operations. Many data centers are still designed this way.

Availability of the operation has always been the main concern with cost of the operation well down the list of priorities. With government sanctions such as “carbon caps” and “green mandates,” the idea of achieving higher operating efficiencies is gaining attention for reasons of energy reduction, lower cost of operation, competitive advantage, and regulatory compliance. To achieve dramatic advances in performance, data center architecture must be designed as a whole, not in pieces. The Green GridSM organization has published many papers and tools directed toward viewing the data center as one fully integrated system (see Appendix G).

6.7.1.1 Scalability

All systems and subsystems should be able to scale to or near their optimum operating efficiency throughout the life of the facility. Designs should be flexible enough to adapt to changing power and cooling requirements and technological improvements that cannot be anticipated at the time of the data center design. This approach has a greater chance of achieving the lowest practical energy consumption over the life of the facility when the planner/designer:

- Pays close attention to establishing a rational model for growth of space and power requirements over time.
- Models power and cooling system performance over the life of the data center in accordance with the growth model.

6.7.1.2 Instrumentation and Control

All systems and subsystems should be instrumented so that they can gather real-time operating power and performance data. All components should be able to communicate status through standardized management interfaces. Data should include indicators of optimum energy efficiency such as power consumption, temperature, percent load, and other metrics as appropriate to the device.

In particular, if measurement of PUE is desired (discussed below), instrumentation should be installed that permits measurement and trending of the energy consumption of the specific equipment that directly supports the data center.

6.7.1.3 Annunciation

All systems and subsystems should be discoverable through the single management system to report and trend such metrics as location, minimum and maximum energy used, and performance level capabilities.

6.7.1.4 Management

All systems and subsystems should be able to network through standardized management, interoperability interfaces, and language. Operations should be automated at all levels via policies set through management infrastructure.

6.7.2 Data Center Efficiency Metrics

The expression is, “You cannot control what you cannot measure.” In order to know if a design is good or if it is working as well as intended, there must be a means to measure its effectiveness. Most manufacturers of ITE or IT infrastructure equipment provide some information about equipment power consumption. For code compliance purposes, nameplate data typically includes very conservative numbers on power consumption so that the cables, circuit breakers and fuses will be sized for worst case. Designing for worst case exacts a penalty in efficiency and operating costs.

Accurate measurement of power consumption in real time allows a baseline to be established. Future performance can be compared to the baseline to document changes in data center efficiency and against industry performance in general.

The industry has standardized on two measurements for data center efficiency: PUE and DCIE.

6.7.2.1 Power Usage Effectiveness (PUE)

PUE is simply a measure of the power consumed by the data center as a whole divided by the power consumed by servers, storage devices, and other ITE. It is expressed in Equation 6-1.

$$PUE = \frac{\text{Total facility power}}{\text{ITE power}} \quad (6-1)$$

PUE will be greater than 1.0. Many data centers operate with PUE near 2.0. Inefficient or poorly managed data centers have PUE as high as 3.0. A good target to strive for is a PUE within a range of 1.3–2.0.

The concept is easy, but actual implementation and interpretation is more challenging. PUE can be measured instantaneously or at any time interval — hourly, daily, weekly, monthly — all the way to the life of the facility in years. A rough analogy is vehicle fuel efficiency measured in distance traveled per volume of fuel consumed (miles per gallon or kilometers per liter). This metric can vary widely over time and is influenced by many variables. Similarly, PUE is highly dependent how facilities infrastructure performs at any point in time. This performance can vary widely over the life of the facility, depending on the magnitude of load relative to capacity and the degree to which efficiency is dependent on the load versus capacity of components and systems.

PUE is a ratio of power consumption in a specific data center, so comparison of two facilities solely on the basis of PUE can be misleading.

NOTE: At the time of this standards publication, ISO/IEC CD 30134-2, *Information Technology – Data Centres Key performance indicators – Part 2: Power usage effectiveness (PUE)* was under development and specifies measurement, calculation, and reporting of PUE for data centers.

The power consumption of electrical power distribution and cooling equipment for the purpose of calculating PUE is supposed to be limited to the equipment that is directly supporting the data center. In many, if not most data centers, some portion of the power and cooling produced by such support equipment is used for spaces that do not directly support the data center. For example, chilled water systems in dedicated data center facilities often supply cooling to areas such as equipment/parts storage, restrooms, corridors, command center, and meeting rooms. While these areas might seem to be directly supporting the data center in such a facility, they should not be included in calculating PUE. The energy associated with providing cooling and power to these areas is not likely to be metered separately, so an estimate of their contribution must be made to allow adjustment of the PUE calculation.

Some government agencies have begun using PUE as an energy effectiveness measurement.

6.7.2.2 Data Center Infrastructure Efficiency (DCIE)

DCIE is simply the reciprocal of PUE and is expressed in Equation 6-2.

$$DCIE = \frac{1}{PUE} = \frac{\text{ITE power}}{\text{Total facility power}} \times 100\% \quad (6-2)$$

DCIE will result in a number less than 1.0. It is often preferred because, intuitively, it expresses efficiency as a percentage.

Either PUE or DCIE can be used, but the industry seems to favor PUE.

6.7.3 Data Center Energy Saving Design Opportunities

Data center efficiency is most effectively optimized by concentrating on the areas where the greatest gains are possible. It is frequently stated that the cost of operating infrastructure to support ITE is greater than the cost of operating the ITE itself. This suggests a PUE greater than 2.0.

When designing a data center for efficiency, the techniques listed in Table 6-3 should be considered. The values given are subjective, but they give a reasonably good comparison of their impact on a design. Most of the techniques are described in more detail elsewhere in this standard.

Additional design guidance to improve energy efficiency can also be found in *EU Best Practices for EU Code of Conduct on Data Centres* and *ASHRAE Best Practices for Datacom Facility Energy Efficiency*.

Table 6-3 Data Center Energy Saving Opportunities

<i>% of Improvement Possible</i>	<i>Area for Attention</i>
10 – 40%	high-efficiency ITE such as blade servers, and IT management systems such as server virtualization
10 – 40%	hot-aisle or cold-aisle containment systems
10 – 40%	cabinets with isolated air supply or isolated air return
10 – 30%	modular and scalable architecture for power & cooling considering total life-cycle energy savings.
5 – 15%	hot-aisle/cold-aisle rows with optimally located row-oriented cooling
4 – 15%	locating sites where it is possible to take advantage of economizer modes of air conditioning (air-side or water-side)
4 – 10%	selection of high-efficiency power equipment such as UPS, capable of high efficiencies at low loads
0 – 10%	cooling management systems able to prevent demand fighting in which one unit is humidifying while another is dehumidifying
1 – 6%	where under-floor cooling is used, optimized quantity and location of floor vents only in the cold aisles, assisted by computational fluid dynamics (CFD)
1 – 6%	overhead wiring and cabling to prevent blockage of air distribution under access floors (Refer to 14.4.8.1 for considerations of overhead versus under-floor cable routing)
1 – 5% or more	use of blanking panels in equipment racks to prevent mixing of cold inlet air and hot exhaust air
1 – 5% or more	blocking access floor cable cut-outs and sealing floor tile openings to prevent escape of cold air where it is not needed
1 – 3%	use of energy efficient lighting along with timers, occupancy schedules, or motion detectors

6.8 Network Architecture

6.8.1 Considerations

Network architecture considerations include:

- Centralized/decentralized location and its impact on space planning
- Copper communications cabling distance limitations and their impact on space planning
- Optical fiber distance limitations and their impact on space planning
- Impact of power and large number of connections for core and distribution switches on space planning (i.e., larger cable pathways)

This page intentionally left blank

7 Architectural

7.1 Facilities Planning

7.1.1 General Overview

7.1.1.1 Introduction

The purpose of this section is to provide information to assist a designer in the planning and specification of a computer room and related spaces. This section will focus on the architectural and general construction elements of a data center. Some reference will be made to other elements as the purpose of the architectural elements of a data center is to provide a physical envelope that assists in meeting the needs of the end user (information technology/telecommunications).

The initial planning of the data center must be a cooperative effort involving the client facilities planners, the IT personnel, the telecommunications personnel, the client office users and all the various disciplines that will assist in the completion of the data center.

Several methods of planning the data center are currently utilized in today's environment. Two of those are:

- IT, telecommunications, and other users collect data and turn it over to the facilities manager who then puts together a team that locates a site, designs, and constructs the data center.
- The facilities and IT personnel select an initial planner or designer to assist in the gathering of information and prepare a document that assists in the search for the site and assists in the budgeting of the project.

From this point, the project is completed one of two ways:

- The initial design team continues to prepare a complete set of construction documents that are bid to a preselected group of contractors (design-bid-build).
- The initial planning information is handed to a preselected design build contractor who provides all documents and construction for the project (design/build).

See Appendix A for more information regarding design and construction approaches.

The appropriate approach for a given project varies, depending on the project. For an entity that has limited specific design requirements, has a preselected location, and trusts the contracting entity, the second planning method listed above is the most likely utilized. For companies that want to ensure that the data center plan meets some specific needs, and for those entities that want to ensure that the initial planning decisions meet their detailed user and market requirements, the first planning option listed above is recommended. To determine whether design-bid-build or design/build is best suited for a specific project, the client should consider the complexity of the project. Companies that have several data centers of the same type and complexity may find the design/build process can save time and money. If the space is complex and there are a variety of end users and multiple processing elements, then the design-bid process can ensure all the issues are addressed initially and reduce time delays and cost increases later.

It should be noted that the accessibility regulations (e.g., Americans with Disabilities Act [USA], Disability Discrimination Act [Australia]) or similar guidelines may need to be followed for the design and construction of computer rooms and support spaces. The designer should be aware that the AHJ may require adherence to these regulations and other standards and may publish its own enhancements to these documents.

7.1.2 Site Selection

7.1.2.1 Requirements

While most site selection criteria are covered in Section 5, from an architectural/general construction consideration, it is important to ensure that:

- All interfering elements be eliminated (vibration, air contamination, security, flood plains, electromagnetic interference, and hazardous materials)
- Sufficient space is provided around the building to allow for complete security
- Space is provided for a variety of support equipment, such as:
 - Generator(s)
 - Fuel tank(s) to support the generator
 - HVAC heat rejection systems.
- All electrical service requirements are met (see Section 9)

These elements shall also be secure from public access.

7.1.2.2 Additional Information

See Section 5 for other issues to be considered for site selection such as availability of power, telecommunications connections and stability, fire services, and secure neighborhood.

7.1.3 Location Within a Building

7.1.3.1 Requirements

When looking into a floor below grade level, water infiltration issues shall be considered, including:

- Height below surrounding drainage systems
- Water detection systems
- Secure and continuous vapor barriers
- Water and vapor extraction systems
- Main building systems that might create damage to the data center
- Hazardous materials stored or utilized in the basement
- Flooding potential during and following severe weather events

The required distributed floor loading capacity is specified in Section 8.

7.1.3.2 Recommendations

For equipment access, the floor nearest prevailing grade level (ground floor) is often the most advantageous. Floor loading considerations also tend to lead to the first floor as a location. Upper floors can be a solution to security and water issues, but in areas with major lateral force issues (hurricane, wind, seismic), the upper floor can contribute to structural instability. Many times, the upper floors are not designed for the floor loading required for a data center.

7.2 General Design Concepts

7.2.1 Levels of Reliability

7.2.1.1 Introduction

The level of required reliability plays a major part in the design of the data center. A generally accepted method of describing levels of reliability is the Class system, as shown in Appendix B.

Reliability is defined in relationship to the identified risks. For example, NFPA 75 identifies risks such as life safety, fire threat, loss of revenue, loss of equipment, and loss of telecommunications. It is safe to assume that the loss of the data center will affect one or more of the elements above.

In the United States, for further information on construction and protection of computer rooms, refer to NFPA 75.

7.2.1.2 Requirements

The building shall be of construction appropriate for the level of durability and reliability consistent with the best structural practices for processing facilities. (See Section 8)

7.2.1.3 Recommendations

The building should be designed to meet design criteria for seismic and wind lateral conditions.

7.2.2 Facility Purpose

7.2.2.1 Introduction

The general purpose of the data center affects the construction, operation, and physical security of the data center. Medical, financial, and government information regulations may impose special security requirements. Codes might dictate requirements for certain types of facilities such as hospitals, utilities, telecommunications, and other critical services.

The occupancy category of a data center is dependent on the use of the facility as defined by applicable standard (e.g., ASCE 07) or AHJ. This requirement can be increased by the owner based on the need or desire for the facility to operate after an event (occupancy category IV). Generally, data centers fall into occupancy category II, but they could be rated occupancy category IV if required by use or owner. Wind, snow, ice, flood, and earthquake design requirements for the building and its mechanical and electrical systems are affected by the selected occupancy category.

The importance factor to be used in calculating design requirements may be increased by the owner to provide a more robust design even if the occupancy is less than occupancy category IV.

A project that requires critical power systems per AHJ (e.g., critical operations power systems [COPS]) will affect site selection and the design of the building and its mechanical and electrical systems.

7.2.2.2 Requirements

The design team shall work with the users to determine the purpose of the facility with the focus on the effects of failure of the facility. By utilizing the Class definitions as described in Appendix B, determine the appropriate level of reliability to meet the purpose of the facility.

7.2.3 Multiuser Versus Single User Groups

7.2.3.1 Introduction

Multiuser facilities have more security requirements than single user facilities. Administrative functions require access be limited to a minimum number of authorized personnel. Groups, such as engineering and research may require a greater access to accommodate more frequent equipment setup and changes.

7.2.3.2 Requirements

Data centers that house data processing equipment from multiple companies will require physical security for equipment of each user. Physical user security can be accomplished by partitions (such as walls or cages) or at the cabinet level with electronic controls or physical locks.

Multiuser facilities may require surveillance systems and additional access control and records, including tenant power metering.

7.2.4 Equipment Change Cycle

7.2.4.1 Requirements

Flexibility needs to be planned into a data center that adds or changes equipment frequently. Designers and users are to determine the expected life cycle for equipment and determine the effect on facilities operations, including the need for space inside and outside the computer room to stage and bring into service new hardware.

7.2.4.2 Recommendations

The average data center may significantly change its ITE inventory every 3 to 5 years. The physical power and cooling infrastructure should be flexible and scalable in order to optimize it for the conditions of power capacity and density at any given time and place within the computer room.

7.2.5 Occupied Versus Unoccupied Data Centers

7.2.5.1 Recommendations

In order to minimize human error, data centers may be designed with a "lights-out" philosophy. A lights-out approach is to have no personnel working within the data center on a normal basis. The design of a lights-out data center will require sophisticated and secure remote monitoring and control capability. A lights-out data center will also have to address operational challenges such as coordinating the delivery of supplies and ITE to a facility that has no personnel on-site on a regular basis.

7.2.6 Data Center Location Within Building

7.2.6.1 Requirements

If the data center is on a floor above the first (grade level) floor, ensure that access is provided for the equipment required in the data center.

The data center shall be located as close as possible to incoming power to reduce the power cabling lengths.

The computer room shall be located on a floor that has the structural capabilities to support the equipment (per the structural engineer).

7.2.6.2 Recommendations

The computer room should be located in close proximity to the telecommunications entrance room(s) of the building.

The computer room is best located on the ground floor. It is generally desirable to locate the computer room away from exterior walls, although it may be appropriate to design a data center where the computer rooms have an exterior wall with knock-out panels for future expansion or integration of certain free cooling options. Where knock-out panels are used, precautions against storm/blizzard damage and temperature extremes (e.g., condensation) should be taken.

7.2.7 Type of Building

7.2.7.1 Requirements

Critical data centers shall be installed within a steel or concrete framed building such as a Type I, II, or III building as defined in the International Building Code. Under certain conditions, Type IV construction can be utilized if constructed in accordance with NFPA 75.

The exterior of buildings shall be nonflammable and of durable material, resistant to the foreseen weather conditions for the expected lifetime of the facility.

The building section shall allow a minimum clear access height of 3 m (10 ft) from slab-to-slab.

7.2.7.2 Recommendations

The slab to structure above should be a minimum of 4.5 m (15 ft).

7.2.8 Multitenant Buildings

7.2.8.1 Requirements

Where a data center is in a multitenant building, the data center shall be located away from hazards and mutual access points with other tenants.

All water lines, sprinkler lines, ductwork, and gas lines serving areas outside of the computer room shall not pass through the computer room area. No systems hazardous to the computer room shall be located in or around the computer room.

All supply lines, ductwork, and telecommunication pathways serving the computer room shall not pass through the rooms of other tenants if comprehensive monitoring, protection against intrusion, and accessibility for maintenance cannot be guaranteed.

7.2.8.2 Recommendations

Services to the data center should be separate from services to other tenants.

7.2.9 24/7 Operation Of Data Center

7.2.9.1 Introduction

Critical data centers are often operational 24 hours per day, 7 days per week.

7.2.9.2 Requirements

The data center, including office and command center functions, shall be arranged in a manner to provide security to personnel within the data center and security to arrival and departure locations. At high security facilities, walls, windows and doors of rooms typically permanently staffed (i.e., command center, guard station) should be hardened or bullet resistant.

Twenty-four hour operations shall have break facilities within the building in the vicinity of the data center.

7.2.10 Temperature And Relative Humidity Control

7.2.10.1 Requirements

The computer room shall be located so that temperature and relative humidity can be maintained with minimum energy usage.

The design of the computer room shall include proper insulation and moisture control to maintain steady temperature and relative humidity ranges within the data center.

7.2.11 Materials

7.2.11.1 Requirements

The computer room shall be designed and built with new materials, which are durable, of superior quality, and easy to maintain and operate. Where recycled materials will not affect the operation of the space, they may be considered for use.

7.3 General Paths of Access

7.3.1 General Access

7.3.1.1 Introduction

Once the site is selected, planning the layout of the data center will begin. Access is crucial. The points of access included in this section include main data center personnel access;, non-data center personnel access;, equipment vendor access;, equipment access;, access to support equipment, such as UPS and batteries;, HVAC equipment;, miscellaneous electrical equipment repair access;, telecommunications vendor access;, and separate user group access.

7.3.1.2 Requirements

| All entries into the data center shall be secured.

7.3.2 Data Center Access

7.3.2.1 Requirements

In buildings with a lobby and building guard, direct communications shall be established between the control center of the data center and the building guard station. For high-security sites, communications shall be both audio and visual.

The maximum slope for ramps is 8° from horizontal for movement of cabinets with equipment. However, some accessibility regulations specify a maximum rise of 1:12, or about 4.8°. Additionally, the ramp shall be at least 900 mm (36 in) clear width, have hand rails on both sides, and have a 1.5 m (5 ft) clear landing at the top and bottom.

If the computer room has only one ramp, it shall meet AHJ accessibility requirements. One ramp for equipment and an elevator or ramp for wheelchair access is acceptable.

7.3.2.2 Recommendations

The main access to the data center should be secured via some form of access control. This control can be a combination of personnel and electronics or solely electronics. Each client should consider the level of security necessary for protection of the data being processed.

Sites without a building guard should have both audio and visual controls at the initial point of access to the data center.

In data centers occupied 24/7, it is recommended the initial main access route lead into a secure location outside the computer room that provides additional control prior to entrance into the computer room. Observe life safety code regarding egress.

7.3.3 Equipment Access

7.3.3.1 Requirements

The data center shall allow for the delivery of computer and telecommunications equipment to the facility. The computer/telecommunications equipment delivery pathway, including doors, shall allow for delivery of equipment as large as 3 m (10 ft) long by 1.2 m (4 ft) deep by 2.4 m (8 ft) high, weighing greater than 3400 kg (7500 lb). The support equipment rooms (e.g., UPS and battery room, HVAC room) typically require access for equipment even larger than mentioned above. The routes for mechanical and electrical equipment shall be large enough to permit installation of new equipment and removal of old equipment—a clear height of at least 2.7 m (9 ft) is typically required along routes from the loading docks to the electrical and mechanical rooms. Clear height requirements shall consider the height of equipment, packaging, and moving equipment.

7.3.4 Telecommunications Access Provider Entry Into Computer Rooms

7.3.4.1 Requirements

The local access providers require access to the telecommunications entrance rooms, but they are generally restricted from access to the computer room unless:

- The entrance room is a portion of the computer room.
- The computer room houses access provider equipment such as DWDMs, SONET multiplexers, or other circuit provisioning equipment.
- The carrier demarcation points (e.g., DS-1 or DS-3 DSX panels) reside in the computer room.

7.3.5 Vendor Access

7.3.5.1 Requirements

Access control shall allow access by essential vendors that support the processing equipment. The access control system may require that such vendors be escorted. This control shall allow the data center personnel to know when and where the vendors access the data center.

7.3.6 Support Equipment Service Access

7.3.6.1 Recommendations

As much as possible, support equipment that requires servicing should be serviced on the perimeter of the data center to prevent untrained personnel from inadvertently damaging the processing equipment.

7.4 Planning Detail

7.4.1 Entry

7.4.1.1 Requirements

Consideration shall be made for the initial entrance through a controlled lobby or vestibule, allowing for the entrance to the computer room to be a distance from the visible exterior. The entry to the computer room from noncomputer room spaces shall lead into a controlled space within the data center, prior to providing access to the computer room areas.

Entry for equipment, if separate from main entry, shall be controlled by the data center personnel only.

7.4.1.2 Recommendations

The entry to the computer room should be positioned away from the direct access to the exterior.

Equipment entry should be located near a staging/storage area for unpacking and preparation of equipment prior to entry into computer room.

7.4.2 Command Center and Personnel Areas

7.4.2.1 Requirements

For data centers that are important or critical to company function, a command center shall be included in the plan. This command center should be near the main entrance and shall house environmental monitoring equipment, computer system monitors, and space for the number of data center operators present at any given time. A console is recommended to house all monitors.

The command center shall be located so that it has direct access to the computer room space.

As needed, office and conference facilities shall be provided adjacent to the command center for supervisory functions and to form a war room or emergency troubleshooting area.

7.4.3 Printer Room

7.4.3.1 Requirements

For centers that require printing, a printer room shall be provided adjacent to the personnel areas. The printer room shall be self-contained with a filtration system on the return air leaving the room. Space shall be provided for paper staging within the printer room to ensure the stabilization of paper.

7.4.4 Media Storage Room

7.4.4.1 Requirements

For facilities that produce in-house removable record storage media and store in-house for an extended time the media that has been removed from the library, a separate room shall be provided for media storage. When media is removed from the library and directly transferred to a permanent off-site storage location, a separate media room is not required.

Storage of critical media shall be contained within a 2-hour fire rated enclosure.

7.4.5 Restrooms and Break Rooms

7.4.5.1 Requirements

Restroom and break room areas shall be provided with easy access to the operations and office areas. Restrooms shall be accessible, for both genders per the governing local codes and standards.

7.4.5.2 Recommendations

For 24/7 operations data centers, where practical, access to the restroom and break room should be within the security-controlled area of the data center.

7.4.6 Computer Room

7.4.6.1 Introduction

In general, it is anticipated that circulation and support equipment (e.g., HVAC floor mounted air handlers, coolant distribution units, electrical PDUs, RPPs, static switches, fire suppression tanks) can require as much as 40% of the overall space in the equipment area. In the case of Class F3, and especially Class F4, the physical infrastructure space requirement may be over 50% of the total facility square footage.

7.4.6.2 Recommendations

In planning the cabinet and rack layout, care should be taken to allow for maximum flexibility. A data center may significantly change its ITE inventory every 3 to 5 years.

The data center planner should coordinate early on with mechanical and electrical systems designers.

The computer room should be designed in a manner to provide adequate space for current equipment, growth, technology refresh, personnel and equipment circulation, and support equipment.

Production, development, and test systems should be in separate areas of the computer room, preferably in separate rooms served by dedicated networks.

Expansion should be planned into computer rooms. With the multitude of elements that affect the IT environment, it is difficult to plan for exact expansion needs. It is generally good to determine the expected life of the facility, look at the past growth trends, analyze current and next generation technology trends, analyze technology refresh capacity requirements, and develop a 6 to 9 year technology capacity profile incorporating growth and technology refresh requirements. Extrapolate the 6 to 9 year technology capacity profile into a facility capacity profile, which often covers a 15 to 20 year life cycle.

For Class F3 and F4 facilities, consideration should be given to segregate mechanical from ITE in the computer room since installation, servicing, and maintenance will typically be performed by different personnel. This could be accomplished by erecting a physical barrier (e.g., a fence) between the mechanical and ITE, permeable to the airflow, or by installing the HVAC -components in a separate room adjacent to the computer room, with openings for the airflow.

7.4.7 Entrance Rooms

7.4.7.1 Requirements

The entrance room, if separate from the computer room, shall be accessed without going through the computer room.

Class 3 and higher data centers shall have separate entrance rooms.

7.4.7.2 Recommendations

Class 2 and lower data centers may have a single entrance room.

The entrance room should be contiguous with the computer room.

In determining the space for the entrance rooms, consideration should be made for cable termination hardware, protectors, splicing hardware, cabling pathways, space for cable pulling equipment, carrier equipment, electrical equipment, air conditioning equipment, security equipment, building automation systems, and telecommunications equipment.

7.4.8 Mechanical Equipment Space

7.4.8.1 Introduction

Mechanical equipment will be in the computer room (as mentioned) as well as in a mechanical equipment room/area outside the computer room.

7.4.8.2 Requirements

The architect and data center planner shall coordinate with the mechanical system designer for sizing and the amount of equipment in the computer room. Outside of the computer room, provide space for the heat ejection equipment and associated pumps, fuel tanks, and controls.

7.4.8.3 Recommendations

Mechanical components within a computer room should be located separate from the ITE rows in order to provide maintenance access. Cooling systems should be located separate from the ITE rows in order to provide for maintenance unless placement in or close to the ITE row is necessary for enhanced cooling effectiveness.

7.4.9 Electrical Room and UPS Room

7.4.9.1 Requirements

A separate room shall be provided to contain the data center associated electrical equipment, including the switchboard, various electrical panels, generator automatic transfer switch(es), UPS systems, and input/output boards.

Electrical and UPS room shall be as near as possible to both the main building electrical room and the generator.

7.4.9.2 Additional Information

The electrical room may require two exits, with doors opening in the direction of egress from the room, and the doors and equipment with panic hardware as required by AHJ. Secondary exit routes may pass through other associated spaces such as the battery room, if permitted by AHJ.

7.4.10 Battery Room

7.4.10.1 Introduction

If a centralized UPS system is utilized, a battery room most often accompanies the UPS room.

7.4.10.2 Requirements

Battery rooms with batteries containing liquid, free flowing electrolyte shall include electrolyte spill containment and exhaust systems as required by local codes.

7.4.10.3 Recommendations

If the batteries are in a dedicated battery room, the battery room should be adjacent to the associated electrical room.

The size of the battery room will depend on the type and number of batteries and racks/cabinets.

The battery room should be located at grade level if feasible. Below grade can create a flooding hazard. Above grade can create a floor loading hazard.

The battery room should be designed to accommodate the anticipated maximum floor loading.

The battery room should not be located above a computer room space.

The electrical engineer or local codes may prescribe additional requirements regarding the location of the battery room or battery room equipment. Coordinate with the electrical systems designer.

Consult applicable IEEE battery installation standards and see the additional battery information in Section 9.5.5.

7.4.10.4 Additional Information

The AHJ may require that the battery room have two exits.

7.4.11 Fire Suppression Room

7.4.11.1 Requirements

For Class 4 data centers, a separate room shall be provided for the preaction sprinkler control valve system; a separate room is recommended for critical or Class 3 data centers.

Space shall be provided for the placement of clean agent fire suppression tanks as required. Tanks shall be located to assist easy serviceability. Tanks shall not be located in the ceiling area above equipment.

7.4.12 Circulation

7.4.12.1 Requirements

Clear pathways allowing for the movement of racks, processing, and support equipment shall be provided throughout the space in a direct path.

Circulation pathways shall be a minimum of 1.2 m (4 ft) wide with a minimum clear overhead of 2.4 m (8 ft).

7.4.12.2 Recommendations

Rows should not exceed 20 cabinets or racks in length. Dead-end aisles should be avoided whenever possible for the safety of personnel. Where dead-end aisles are not avoidable, they should be no longer than 10 cabinets or racks in length.

7.4.13 Equipment Staging and Storage

7.4.13.1 Requirements

To prevent contaminants in the computer room, arriving equipment shall be stored, uncrated, and prepared in a room away from the computer room. This separate room shall have filtration on the return air leaving the room.

For both arriving equipment and backup equipment, such as boards and servers, a storage room shall be adjacent to the equipment entrance of the data center. The storage room can be a component of the staging room or a separate room near the staging area.

A staging area shall be provided that has space for the uncrating and preparation of arriving equipment.

Provide space for the large amount of boxes and packing material handled by these facilities. Consider fire protection requirements, frequency of removal, and recycling to comply with local requirements. Consider dumpster requirements, access, and location.

7.4.14 Equipment Repair Room

7.4.14.1 Recommendations

A separate room for repair should be provided with easy access to both the equipment access pathway and the computer room.

An equipment repair room should have a work surface with multiple power and communications connections.

Shelving/caged areas should be provided for spare parts as necessary.

7.5 Construction Components

7.5.1 Data Center Preparation

7.5.1.1 Requirements

If the data center is a new building, prepare the slab and all below grade components of the building with a continuously sealed rubberized moisture barrier.

The building slab shall comply with all local building code requirements for protection against flooding, such as height above flood plain and setbacks from a flood plain.

All exterior openings and penetrations shall be sealed prior to work on interior walls or finishes in the computer room.

7.5.2 Floor Slab

7.5.2.1 Requirements

Floor slabs shall be as per the calculations of the structural engineer, but no less than a floor loading of 7.2 kPa (150 lbf/ft²).

For elevated slabs, the concrete topping over metal deck flutes shall have a thickness of at least 100 mm (4 in) to allow for the adequate embedment of epoxy and anchor bolts.

The floor slab shall be leveled and sealed with a nonpenetrating seal, such as epoxy, which is a moisture barrier and prevents dusting and particulating.

See Section 8.3.1 for additional floor loading requirements.

7.5.2.2 Recommendations

In order to accommodate initial or future high-density equipment (e.g., disk arrays, fully loaded server cabinets), a minimum floor loading of 12.0 kPa (250 lbf/ft²) is recommended.

7.5.3 Computer Room Envelope Wall Construction

7.5.3.1 Requirements

The perimeter walls to the computer room shall be slab-to-slab.

See Table 7-1 regarding fire rated construction requirements.

The perimeter walls of the computer room shall provide the appropriate level of airtightness suitable for a clean agent fire suppression system. All wall penetrations shall be fire sealed and sealed to prevent chemical fire suppression leaks.

The thickness and shapes of wall structural elements shall meet AHJ requirements for the specific wall height to be built. For example, within the United States, metal studs used in constructing interior walls shall have a minimum thickness of 0.64 mm (0.025 in / 22 Gauge) for walls up to a height of 3.5 m (11.5 ft) and a minimum thickness of 1.0 mm (0.039 in / 18 Gauge) for walls exceeding a height of 3.5 m (11.5 ft).

Studs shall have a minimum depth of 140 mm (5.5 in) to accommodate boxes and piping to be installed in the wall. Coordinate the thickness as all electrical and mechanical items shall be recessed or flush mounted.

Walls shall meet the minimum fire rating as listed in Table 7-1.

Where partitions touch a deck or vertical structural members, a joint isolator shall be provided to prevent transfer of vibration and structural loads.

Walls and other structural elements shall be designed for minimum deflection and securely fastened with isolation from all mechanical units and isolation pads or caulking at the top of the partitions.

For envelope walls separating the computer room from a nonconditioned or exterior space, insulation is to be provided as necessary to stabilize temperature migration. A minimum of R-3.3 m²·K/W (R-19 ft²·°F·hr/BTU) insulation is recommended.

7.5.3.2 Recommendations

Class 3 and Class 4 data centers may want to consider concrete masonry unit (CMU), concrete filled CMU, or tilt up concrete panels for the interior walls of the ITE, electrical, and mechanical space to provide additional structural integrity and high fire ratings.

7.5.4 Nonrated Partitions

7.5.4.1 Requirements

In the interior of the computer room, partitions that are not required for rated separation shall be from top of access floor to ceiling above unless additional height is required for security or environmental control.

Nonrated walls shall be braced at a minimum of every 3 m (10 ft) and as required to meet lateral bracing requirements of the *IBC*.

7.5.5 Vapor/Moisture Seal

7.5.5.1 Recommendations

A moisture/vapor seal should be provided completely around humidity controlled spaces to prevent vapor infiltration to or from the computer room.

7.5.6 Door and Glazed Openings

7.5.6.1 Door Requirements

Doors shall be large enough to move equipment between various data center rooms. Doors must be high enough to allow equipment entry on pallets without tilting.

Doors shall have a minimum thickness of 45 mm (1.75 in) and be a minimum of 1.1 m (3.67 ft) wide by 2.4 m (8 ft) high for a single door or 1.8 m (6 ft) wide by 2.4 m (8 ft) high for a pair of doors. Doors shall be mounted within steel frames, have a solid core, and be either wood or steel

The primary access door to the computer room shall be a pair of doors, meeting the requirements listed above. These doors shall have neither a center post nor doorsills.

All doors and frames within a rated partition assembly (1-hour or 2-hour) shall be rated at the code required rating of that assembly for occupancy rated separations (NFPA 76 requires fully rated doors). Doors shall have air tight and fire-rated weather stripping all around the opening.

7.5.6.2 Door Recommendations

All doors along the entire route (i.e., from the loading dock to the computer room) should be a pair of doors.

7.5.6.3 Glazed Opening Requirements

Glazing within doors shall not exceed 0.065 m² (100 in²). These requirements are for equipment and main exit doors to the computer rooms. Where personnel access is required, it should follow the requirements of Section 12.7.

Glazing within rated doors shall be fire rated and set in metal frames.

Glazed openings within rated partitions shall not exceed code limitations as set by the *IBC*.

Glazed openings within partitions shall be of metal frame construction with glazing set in continuous stops (such as neoprene) to prevent vibration.

7.5.7 Fire-Rated Construction

7.5.7.1 Requirements

Walls separating computer room, electrical rooms, battery rooms, mechanical rooms, and separate TRs from other areas within the building shall be a minimum of 1-hour separation or as required by applicable codes and regulations.

Doors and frames within a rated wall shall match the rating of the wall construction.

Glazing within a rated wall shall match the rating of the wall. Electrical rooms and battery rooms, as defined by *IBC* Table 608.2, shall have glazing within the doors only.

Floors above and below each of the spaces listed in Table 7-1 shall be 2-hour rated, as defined in *IBC*.

See Table 7-1 for the fire rating of spaces.

7.5.8 Access Control Systems

7.5.8.1 Requirements

Access control shall be provided at all entrances to the data center and all entrances to the computer room. A system that allows for multiple levels of controls shall be installed to provide for different levels of security in different portions of the data center.

The access control system shall allow for easy modification of access control, be completely programmable, and provide a digital and hard copy of all access to the data center and its various components.

Table 7-1 Minimum Fire Rating of Spaces

<i>Area</i>	<i>Minimum Fire Rating of Walls</i>
ITE space (computer rooms, entrance rooms, dedicated distributors [MDA, IDA, HDA], telecommunications rooms)	1-hour rating, slab-to-slab, may be required by AHJ between adjacent ITE spaces
Command center	1-hour rating, slab-to-slab
Printer room and printer supply storage room	1-hour rating, slab-to-slab
Critical media storage	2-hour rating, slab-to-slab
Electrical room	1-hour rating, slab-to-slab
Battery room	1-hour rating, slab-to-slab
Staging and storage room	1-hour rating, slab-to-slab
Loading dock	1-hour rating, slab-to-slab

7.5.9 Airborne Particles

7.5.9.1 Introduction

Airborne particles can be detrimental to proper operation of the electronic equipment. There are 2 types:

- Non conductive: This dust can be absorbed by the ventilation fans and obstruct the airflow, thereby increasing power consumption or increasing the risk of overheating of the equipment.
- Conductive: This dust can deposit on the electronics and cause short circuits and arcing in electrical equipment. A main cause of conductive dust is zinc whiskers.

Metal whiskers “grow” from ferrous (steel) surfaces, especially those that have been coated with tin, zinc, and cadmium to help protect them from corrosion. These fine metallic filaments, normally only a few microns in width but of several hundred up to a few thousand microns in length can break off to become airborne.

7.5.9.2 Non-Conductive Airborne Particles Recommendations

Non-conductive airborne particles can be minimized by:

- Doing all unpacking, cutting, and drilling outside the computer room
- Keeping cardboard boxes and manuals outside the computer room
- Prohibiting food or drink inside the computer room
- Avoiding carpets in computer rooms
- Using ceiling panels that have an impervious surface such as drywall panels with a vinyl covering
- Use of air filtration with regular replacement of filters
- Keeping printers, copiers, and tape media in separate rooms with separate HVAC systems
- Occasional professional cleaning of the access floor, subfloor, and overhead ducts
- Preventive maintenance cleaning of equipment, cabinets, and racks
- Place brushes, grommets, or other material in access floor openings to minimize loss of air pressure and airborne particulates.

Fire marshals usually require that all combustible materials be stored outside the computer rooms and, in cases where aluminum floor tiles are used, keep printer toners out of the computer room to avoid thermite reactions.

7.5.9.3 Conductive Airborne Particles Recommendations

Typical equipment with ferrous material are floor tiles, supports, raceways, cable trays, racks, cabinets, and the chassis of servers and switches.

It is recommended that the designer verify that the manufacturer has tested for the resistance of zinc whisker development or has taken action through the manufacturing process to mitigate whisker development. Some examples of mitigation include:

- Electroplated zinc coated or hot dip galvanized zinc coated with special addition of other material preventing whisker growth.
- Powder coated with sufficient thickness
- Use of non-ferrous or stainless steel materials

NOTE: Non-ferrous or stainless steel have not demonstrated the capability to develop whiskers.

7.5.10 Access Flooring System

7.5.10.1 Introduction

An access floor system can be used for the distribution of power and signal cables, HVAC piping, and cooling air through perforated tiles to equipment racks if the capacity is sufficient for the load.

Access floors consist of interchangeable square panels selected to meet specific load requirements, supported by adjustable pedestal assemblies, which positively locate, engage, and secure panels and that accommodate horizontal stringers connecting the heads of the pedestals.

7.5.10.2 Requirements

Access floor systems are not required; the requirements of this section apply where access floors are used.

Underfloor concrete shall be cleaned and sealed after all major underfloor work has been done, including installation of the access floor system itself.

The access floor shall be a minimum of 450 mm (18 in) above the slab. When determining the minimum raised floor height for an air plenum, the mechanical designer shall analyze the height required to achieve the desired air distribution. Considerations shall include all under-floor airflow obstructions such as network cabling pathways, power systems and pathways, and cooling system piping. Raised floor heights of 900 mm (36 in) are common.

The access floor performance shall meet or exceed the minimum specifications listed in Table 7-2. Additionally, the floor tile or system must have the ability to withstand two times the loads specified in Table 7-2 without failure. While concentrated and rolling loads are dependent on the equipment being placed, any equipment being placed shall not exceed the rolling load and concentrated load listed in Table 7-2.

Table 7-2 Computer Room Access Floor Performance Specifications

<i>Performance Specification</i>	<i>Minimum (medium duty)</i>	<i>Recommended (heavy duty)</i>
Rolling load (access floor panel) Local surface deformation 0.5 mm (0.02 in) Total permanent set 1 mm (0.04 in)	567 kg (1250 lb)	680 kg (1500 lb)
Impact load (access floor panel) Drop weight, dropped from 305 mm (12 in) height on 645 mm ² (1 in ²) local surface with deformation 1.5 mm (0.06 in)	68 kg (150 lb)	79 kg (175 lb)
Concentrated load (access floor panel) Load on 645 mm ² (1 in ²) point with maximum deflection 2 mm (0.08 in) anywhere on the panel	567 kg (1250 lb)	680 kg (1500 lb)
Uniform load (access floor system) Load rating of access floor system, including panels, pedestals, and stringers	732 kg/m ² (150 lb/ft ²)	1221 kg/m ² (250 lb/ft ²)

The building's structural system supporting the access floor must support the access floor and all imposed loads.

The assembly shall be leveled and locked at a selected height, requiring deliberate action to change the height setting and preventing vibration displacement.

Pedestals shall be secured to the slab using a method acceptable to the access floor manufacturer and AHJ. This is typically performed using bolts, adhesives, or seismically isolated floor systems.

Stringers shall be used for all access floors exceeding the height of 500 mm (20 in).

All tiles shall be supported at all four sides/corners, and the tile surface shall have anti-static properties in accordance with IEC 61000-4-2.

Removal of tiles in unstringered systems or tiles and stringers in stringered systems in an operational data center will destabilize the structural integrity of the access floor. A structural engineer shall be consulted to provide a recommended maximum number of contiguous tiles and stringers that can be removed at any one time, and this information shall be incorporated into the operational guidelines for the data center.

The space below an access floor shall include a method of fire detection if required by local codes. See Section 11 for additional information.

7.5.10.3 Recommendations

For higher power density equipment where the underfloor space is used for cooling, the access floor should be a minimum of 900 mm (36 in) above the slab.

In locations where seismic activity is present, the access floor selected should be designed by the manufacturer for seismic applications, installed in accordance with the manufacturer's instructions, and certified by a professional structural engineer.

Additional structural and operational criteria/factors to consider should include:

- Panel drop tests
- Maintaining panel integrity for a given cut-out size
- Pedestal axial loads
- Pedestal overturning moment
- Stringer midspan concentrated loads
- Permanent sets and deformations of any system components
- Pedestal bases should be glued directly to the concrete slab and not to the epoxied/painted slab

Refer to Section 14.13.2 for the access floor grid coordinate system to be used to locate equipment in the data center.

Stringers should be used for increased stability regardless of access floor height. Access floors for computer rooms should use a bolted stringer system as they are more stable than stringerless systems. Additionally, access floor stringers should be 1.2 m (4 ft) long installed in a “herringbone” pattern to improve stability.

Access floor tile cuts should have edging or grommets along all cut edges. If the edging or grommets are higher than the surface of the access floor, they shall be installed so as not to interfere with placement of cabinets and racks. The edging or grommets shall not be placed where the cabinets and racks normally contact the surface of the access floor.

In the case of floor discharge HVAC systems, floor tile cuts should be limited in both size and quantity to ensure proper airflow. Static air pressure should be controlled at all floor tile cuts and openings. Various methods for containing static air pressure are available, including brush systems that can be field fabricated or are commercially available. It is recommended that the HVAC system be properly balanced once all equipment cabinets and racks are in place. The HVAC system should be rebalanced with the addition and removal of floor cuts, equipment racks, and cabinets.

Floor tile openings under cabinets and racks should be no larger than required for entry of cables to minimize loss of underfloor pressure.

7.5.10.4 Additional Information

Access floor performance ratings are based on Ceilings and Interior Systems Construction Association (CISCA) standards and TIA-569-C.

Load information as applicable to Table 7-2:

- Concentrated load – the access floor panel’s capability to handle a point or static load. Use CISCA testing guidelines for concentrated load.
- Uniform load – the load applied over the entire area of the panel in lb per m² or ft².
- Rolling load (or dynamic load) – the access floor panel’s capability to handle movement of equipment on wheels. Rolling loads are determined by the number of passes, and the physical properties (e.g., size, hardness) of the wheels. Rolling loads typically have a more damaging effect on a panel than a static load.
- Impact load – defined by the weight of the load and the height the object is dropped.
- Ultimate load – the load at which the panel structurally fails and is sometimes expressed as a multiple of concentrated load.

Hollow steel panels are light and do not create particulates that wood filled or concrete filled tiles can create, but they do not have the static or dynamic load capability of filled tiles. Some data centers use a mix of concrete filled steel tiles (in more heavily trafficked aisles and print areas) and hollow steel tiles.

Damage to access floor tiles during move-in can be reduced by temporarily covering pathways with 13 mm (0.5 in) thick plywood or hardboard.

High-pressure laminate (HPL) is a good material for the top surface covering of access floor tiles as it is easy to maintain and helps dissipate static electrical charge.

7.5.11 Ceilings

7.5.11.1 Requirements

In data center computer rooms and telecommunications spaces (e.g., entrance rooms, TRs), the minimum ceiling height should not be less than 3 m (10 ft) from the finished floor to any obstruction such as sprinklers, lighting fixtures, or cameras. At least 450 mm (18 in) clearance from sprinklers to raceways, cabinets, and racks shall be maintained to ensure that they do not disrupt the sprinkler distribution pattern subject to the AHJ.

7.5.11.2 Recommendations

The recommended ceiling height for computer room spaces (from slab-to-slab) is 4.5 m (15 ft or greater).

A suspended ceiling may not be required for computer rooms that do not use the ceiling space as an air-return. Benefits of an open ceiling (where not required for cooling) are the visibility of any technical problem and the ease of access to installations and pathways mounted underneath the ceiling slab.

Where the HVAC and cabinet solution has been designed to suit, having a ceiling partition where hot air can be fed into and directed to the air handling units, thus preventing the hot air from recirculating into general room space, is better than having a high ceiling alone.

Office-type ceilings should not be installed in new data center spaces. Depending on the design for the cabinets and the HVAC solution, there may be a HVAC solution design requirement to provide a ceiling return air plenum. (Refer to Section 14.7 for considerations of cable routing). The materials used and the design of this type of ceiling shall consider any need to support cable trays or other cable pathways for overhead cabling in the data center.

Ceiling requirements should be developed taking into consideration nonflaking or dusting tiles, vapor resistance, and hold down clips for gaseous fire suppression discharge or high-volume airflow and acoustics. Materials known for metal whiskers (e.g., zinc, tin, cadmium), whether electroplated, pregalvanized, or hot dip galvanized, should be excluded from ceilings.

7.5.12 Equipment Bracing System

7.5.12.1 Introduction

Various locations, including high seismic and wind-loading areas, will require special attention to the bracing of equipment.

7.5.12.2 Requirements

Equipment cabinets and racks shall be braced in accordance with local codes.

Cabinets braced at the top can utilize the cable ladder rack system, if present, with an attachment that provides rigid four-directional lateral bracing. Equipment mounted on access floors in seismic areas shall be braced to the underfloor slab with an approved method.

7.5.12.3 Recommendations

The bases of cabinets and racks should be braced to the slab as appropriate for the seismic demand in accordance with local seismic codes or requirements such as ASCE 7.

7.5.12.4 Additional Information

As an option, lateral movement at base of cabinet may be controlled utilizing a base isolation platform rated for the loading of the cabinet.

7.5.13 Computer Room Finishes

7.5.13.1 Requirements

Equipment rooms and related walls shall be finished with nonparticulating water-based epoxy paint finish, smooth finish. Prior to painting, drywall board shall be sealed with a compatible sealing primer.

All penetrations in the perimeter walls shall be completely sealed up to the deck height.

7.5.14 Roof Systems

7.5.14.1 Requirements

Data center roofing shall be designed to handle the loading requirements of the roof top mechanical systems.

The roof system shall be designed to provide a continuous seal above the entire data center. Parapets and coping systems shall be of construction to ensure moisture infiltration is prevented.

No penetrations shall be made in the roof over the computer room or entrance room. Additionally, roof drains and leaders shall be kept away from the computer room.

7.5.14.2 Recommendations

Roof penetrations are not recommended in the command center or any electrical rooms.

This page intentionally left blank

8 Structural

8.1 Building Code Compliance and Coordination

8.1.1 Requirements

Local building codes shall be consulted in the planning and implementation of changes to the building and its mechanical, electrical, and life safety systems.

NOTE: Building code references within this standard are generally to the current edition of the *IBC* and *ASCE 7*.

8.1.2 Additional Information

State, provincial, and local municipalities often adopt their respective national building codes by incorporating them into their specific building codes for their jurisdiction. However, these adoptions often have amendments to specific sections, and the scope of the amendments may be significant. Always check the local amendments before making decisions based on code requirements.

Compliance to the *IBC* and *ASCE 7* does not assure functionality following an environmental event such as wind, snow, and earthquakes. If a facility is intended to be functional, additional guidance is provided in documents such as the *UFC 3-310-04* and the *UFC 3-301-01*. The most critical of facilities should consider using the requirements for Occupancy Category V per *UFC 3-310-04* and *UFC 3-301-01* if a regional equivalent does not exist. Additional guidance particular to data centers is contained within *Structural and Vibration Guidelines for Datacom Equipment Centers* from *ASHRAE*.

8.2 Impact of Site Location on Structural Loading

8.2.1 Introduction

All loads on the structure are divided into various types as defined in *ASCE 7*:

- Dead loads, soil loads, hydrostatic pressure loads
- Live loads
- Flood
- Snow
- Rain
- Ice
- Seismic
- Wind

The magnitude of forces on any structure is a function of its geographic location. Both *ASCE 7* and the *IBC* identify the forces expected to be applied to buildings and nonstructural components. The applied forces are a function of probability at a given location for environmental loads (e.g., wind, ice, snow, flood, tsunami, earthquake).

8.2.2 Recommendations

Critical facilities requiring higher performance should consider loads and performance requirements contained in the *UFC 3-310-04* and *UFC 3-301-01*, or regional equivalent.

Additional loads that may warrant consideration for data centers include tsunami and ice impact loads because of shedding on adjacent structures such as telecommunication towers.

8.3 Structural Concerns Specific to Data Center Design

8.3.1 Floor Load

8.3.1.1 Requirements

Floor loading (superimposed live load) shall be a minimum of 7.2 kPa^2 (150 lbf/ft^2) with 1.2 kPa (25 lbf/ft^2) hanging dead load (weight that can be supported from the underside of the floor or roof). This floor load is adequate for most data center areas.

8.3.1.2 Recommendations

Although some industry standards specify a minimum floor superimposed live loading of 7.2 kPa (150 lbf/ft²) with 1.2 kPa (25 lbf/ft²) hanging dead load, the recommendation in this standard is a uniform load of 12.0 kPa (250 lbf/ft²) with 2.4 kPa (50 lbf/ft²) hanging dead load to provide flexibility in the location of higher floor loads such as large storage arrays, printing facilities, and densely populated blade server cabinets. In specific regions of the access floor area where this equipment is located, the structural engineer should be notified of the specific operating weights.

Floors for battery rooms should be designed for a minimum superimposed live load of 12.0 to 23.9 kPa (250 to 500 lbf/ft²).

Roof areas over battery rooms should be designed to support a minimum suspended dead load of 1.4 kPa (30 lbf/ft²).

8.3.2 Raised Access Floors

8.3.2.1 Requirements

Raised access floors are commonly used in data centers. When raised access floors are in use, all raised access floors shall meet ASCE 7 special access floor requirements.

Raised access floors shall be designed and tested as a Designated Seismic System and shall have Special Certification Requirements as defined in the ASCE 7. The response spectra shall be calculated at the bottom and at the top of the raised access floor to determine the demand on the equipment mounted on the floor. The response spectra shall be computed for the in-structure response accounting for the structural support in addition to the response characteristics of the raised access floor.

The overturning of equipment mounted on the raised access floor shall be computed and restraints to be provided for seismic design categories *C* through *F*. Positive mechanical attachments shall be provided as required to prevent overturning.

8.3.2.2 Recommendations

The *IBC* and *ASCE 7* do not appropriately address seismic vertical ground motions and the amplifications of vertical ground motions in the structure. The nuclear industry and military industry require the calculation of the seismic demand because of vertical ground motions that is referred to as the seismic demand. *UFC 3-310-04* can be used as a reference to determine methodology to seismically qualify raised access floors.

Because of the importance of data centers, an in-structure response analysis should be used to compute the coupled response of a raised access floor. A coupled response can then be used to develop response spectra for equipment mounted on the raised access floor.

8.3.3 Mission Critical Equipment

8.3.3.1 Requirements

Equipment that is determined to be mission critical shall be designed and tested to determine the seismic demand and the equipment fragility. The seismic demand of mission critical equipment shall be determined at the point of attachment of the equipment.

Equipment determined to be mission critical shall specify the performance expectations. The seismic demand shall be determined at the point of attachment. The point of attachment may be a structural element, or it may be a nonstructural component (such as a raised access floor). If required, a coupled dynamic analysis may be required to determine seismic demand.

8.3.3.2 Recommendations

The *IBC* and *ASCE 7* do not appropriately address equipment seismic qualifications for mission critical equipment and the in-structure seismic demand. The fragility defines the ability of an element to resist seismic ground motion. *UFC 3-310-04* can be used as a reference to determine methodology to seismically qualify mission critical equipment. Further guidance is contained in within *Structural and Vibration Guidelines for Datacom Equipment Centers*.

8.3.3.3 Additional Information

UFC 3-310-04 defines equipment as Mission Critical 1 (MC 1), Mission Critical 2 (MC 2), or Not Mission Critical (NMC). Once each piece of equipment and distributed system is categorized, the methods to qualify the equipment relative to the classification are defined in *UFC 3-310-04*. The *UFC* also defines how inspections and peer reviews are to be performed.

8.3.4 Wind

8.3.4.1 Introduction

ASCE 7 provides a series of maps with wind velocity depending on the Risk Category. Critical for a facility to have some measure of functionality is the proper design for wind loads of the components and cladding. Air handling units are often the source of leaks because of extreme wind events. Additionally, emergency electric power generators should also be considered for the design of extreme winds and debris impact from extreme winds.

8.3.4.2 Recommendations

In the design of data centers, the Enhanced Fujita Scale level of EF3 is commonly used for wind-loading calculations. EF3 yields a ground wind speed for design purposes of between 219 km/hr (136 mph) and 265 km/hr (165 mph). The wind speed is then multiplied by a set of empirical coefficients to translate the effect into resulting kilopascals (pounds force per square foot) lateral load on the facility. If tornado winds are to be considered, a map of tornado wind velocities is contained in the ASCE 7 Commentary.

8.3.4.3 Critical Facilities

For any critical facility, the integrity of the building envelope shall be maintained. Wind-borne debris is a common source of breaching of the building envelope. If the building is required to be functional following a given wind event, the building windows, doors, walls, and roof that comprise the envelope shall be designed to resist breaching by wind-borne debris. Guidance is provided in the ASCE 7 Commentary for the design considerations of wind-borne debris.

Consideration for wind-borne debris should also be included for any critical components such as air handling units or emergency generators.

NOTE: UFC 3-310-04 defines enhanced wind loads in order to provide a higher level of performance.

8.3.5 Earthquake

8.3.5.1 Introduction

Earthquake-resistant design of structures is complex, as seismic energy is imparted to the structure through the foundation as a dynamic load. This means that the response of the building to the earth shaking will be a function of type of foundation system used, type of soil encountered, the magnitude of the earth displacement, the length of time associated with the earthquake, and the location of the structural or equipment elements within the building. It is common for structural engineers to design facilities in such a way that the facility may undergo a permanent deformation. While this may be adequate for the building code-required design of the building to maintain life safety, it is not adequate design for an essential facility, such as a data center, to function following a major earthquake.

8.3.5.2 Recommendations

Data centers are placed in IBC Risk Category IV because of their criticality. The owner may elect to use a reduced Risk Category rating of II if the facility does not have to operate after an earthquake. Designating a facility as Risk Category IV will still not necessarily ensure a data center will be functional following a major earthquake. If a facility is intended to be operational with a high degree of confidence following a major seismic event, it should be designed in accordance with the provisions of UFC 3-310-04 for Risk Category V.

For data centers, special attention must be paid to the design of specific nonstructural components, such as raised access floors, that will have a direct impact on the survivability of the computer functions after an earthquake. Depending on the height of the raised access floor and the amount of mass supported as well as the magnitude of the earthquake, it may be necessary to isolate the access floor from the rest of the structure. The process of isolation is generally referred to as base isolation. Base isolation is also a valid consideration for the entire building. Base isolation creates other concerns for elements that cross the plane of isolation.

Care must be taken in the anchorage of generators, chillers, fans, switchgear, piping and conduit, and racks. The force on the supports for these elements will be substantially increased as a function of their mass multiplied by the dynamic coefficients addressed in the code enforced earthquake design. The in-structure demand response spectra must be compared to the fragility of the nonstructural component. Guidance for Risk Category V nonstructural components may be found in UFC 3-310-04.

Where local seismic safety codes require or presence of seismic activity dictate, consider using passive dampers to provide base isolation and building energy dissipation.

8.3.6 Blast and Terrorist Attack

8.3.6.1 Recommendations

Many data centers are designed to resist the effects of a terrorist attack. Terrorist attacks can be in many forms, but the most prominent attack is in the form of a blast from some manner of vehicle-borne improvised explosive device (VBIED). Security experts and law enforcement should be consulted to quantify the size of explosive device. Security and physical site barriers should be constructed to maximize the distance that a VBIED can be from the data center. The blast dynamic pressures can be calculated and compared to the response of the data center structure and building envelope elements. Guidance for blast-resistant design may be found in ASCE 59. Smaller explosive devices can be mitigated by screening processes that place the threat at a defined distance from the facility.

Terrorist attacks can take many forms that can include introducing chemical, biological, or radiological agents into a facility. Protection should include screening for compounds that could be brought into a facility clandestinely and controlling air supply into a facility.

8.3.7 Ice Shard Impact

8.3.7.1 Recommendations

In addition to the loads defined by ASCE 7, data centers adjacent to communication or broadcast towers should calculate the dynamic loads because of ice impact from ice shedding from the adjacent tower and design appropriate mitigation. Towers have a tendency to accrete ice in many geographic areas. The ice that forms on the towers will eventually fall from the tower in the form of ice shards. Ice falling from adjacent towers has resulted in significant damage to roof structures of facilities. Mitigation can take many forms, including armoring the lower roof, locating the facility outside of the ice shedding area, or heating elements on the tower to preclude the formation of ice.

9 Electrical Systems

9.1 Overview

9.1.1 Introduction

Section 9 explains the application of redundancy and the reliability and availability Classes (described in Appendix B) to electrical power distribution and availability within a data center. This section also provides both experience-based suggestions and performance-based metrics for each of the Classes in the standard.

The only criterion for securing a given Class is conformance to the performance metrics and values of this section. No endorsement of a given design style is offered nor is any particular type of technology given preference. The project designer and owner should select the system and topology needed for a comprehensive critical power delivery system, whereas the project team should determine the appropriate MTBF and MTTR figures, which when combined with the given set of needs will offer the most appropriate solution.

At the end of this section is an extensive table denoting requirements for each Class. Table 9-15 complements the individual sections, further noting system features and requirements for the Classes.

This section will include references to other systems in this standard that when considered and used together will yield a strong, coordinated and appropriate critical environment utility system. In the areas of batteries and stored energy systems as well as in bonding and grounding, this section has attempted to extract relevant information from published standards of the IEEE, UL, and other existing industry organizations.

9.1.2 Requirements

Section 9 defines requirements solely as performance-based criteria. The purpose of such approach to defining Classes is to uncouple them from electrical topologies and applications. Thus, to achieve a given Class, a proposed design must conform to the normal, maintenance, and failure modes of operation. This provides system designers, owners, and equipment manufacturers sufficient latitude in selecting a design or product without stifling innovation.

A data center shall meet the general requirements of this section.

Any data center that does not meet the minimum requirements of Class F1 shall be considered Class F0.

There are several methods for the physical development of electrical systems, traditionally or “stick” built, modular or “factory” built systems, or a combination of traditional and modular construction. Modular electrical construction now addresses all aspects of the data center’s electrical construction—electrical rooms, ITE space (either as containers or skid-type systems installed inside a traditional building), critical power distribution systems, and supporting electrical systems outside of the data center proper. The employment of modular electrical systems are a cost, schedule, and risk management tool for the development of the project and are subject to the same demands of this chapter as traditionally-built electrical systems.

The impact of altitude on insulation and heat removal capabilities shall be considered in all electrical equipment specifications and deployments. Most electrical equipment, including batteries, has a specified altitude range for which the voltage/capacity is applicable. If equipment needs to be used above the specified altitude range, consult with the equipment manufacturer concerning operational limits and restrictions.

9.1.3 Availability and Uptime

The presence of single points of failure has a direct bearing on the Class achieved by any given system or design. Single points of failure should be eliminated whenever possible, in order to improve redundancy and reliability, both within the data center and support infrastructure as well as in the external services and utility supplies.

The following issues should be addressed:

- Availability and uptime have been used in the industry on an interchangeable basis. With the varying Class ratings, systems or applications availability may not change state as a result of the failure or maintenance of the supporting electrical infrastructure. During these times, selected portions of the underlying electrical infrastructure may be out of service or unavailable. This would retard the electrical system's ability to respond to any subsequent events or failures, which may result in an outage to the IT systems.
- The reduction of single points of failure within the electrical systems, to the greatest extent possible, is a requirement for Class F3 and Class F4 (explained in Appendix B).
- Single points of failure have greater consequences the farther they are upstream from the load. The closer they are to an individual load, the smaller the impact is likely to be on the entire system. For example, whereas a failed single branch circuit might affect one load or one equipment rack, the failure of a main circuit breaker can take down an entire distribution panel and all connected loads.
- Redundancy increases both fault tolerance and maintainability, but it also increases system complexity, which is a leading cause of human error outages in data centers. Redundancy and overall system complexity must be weighed against the system capacity, ease of operation, cost and schedule.

9.1.4 Redundancy

Within this document, the following terms describing levels of redundancy are used:

- **N (N=Need) or Baseline Requirement**
System meets base requirements for minimum load kW and has no redundancy.
- **N+1 Redundancy**
N+1 redundancy provides one additional unit, module, path, or system in addition to the minimum required to satisfy the base requirement. The failure or maintenance of any single unit, module, or path will not disrupt operations.
For smaller fault-tolerant systems where a single module can accommodate the critical load, the N+1 and 2N models are synonymous.
- **N + 2 Redundancy**
N + 2 redundancy provides two additional units, modules, paths, or systems in addition to the minimum required to satisfy the base requirement. The failure or maintenance of any two single units, modules, or paths will not disrupt operations.
- **2N Redundancy**
2N redundancy provides two complete units, modules, paths, or systems for every one required for a base system. 2N is also referred to as "dual-path topology." Failure or maintenance of one entire unit, module, path, or system will not disrupt operations.
For smaller fault-tolerant systems where a single module can accommodate the critical load, the 2N and N+1 models are synonymous.
- **2(N+1) Redundancy**
2(N+1) redundancy provides two complete (N+1) units, modules, paths, or systems. The failure or maintenance of one unit, module, path, or system will still leave intact a system with full redundancy and will not disrupt operations.
- **Multi-N Redundancy (xN)**
A multi-N system topology is used primarily in fault tolerant or large-scale power systems where more than two large systems are employed together. In such a system topology, the critical load connection at the PDU or the branch circuiting level is the primary means of achieving the redundancy and Class of the system.

9.1.5 Capacity Versus Utilization Efficiency

9.1.5.1 Definitions

The following terms are used in this section:

- Capacity: the kW required to serve the load, plus the design margin and growth factors. This does not include redundant power or the power required for support services, such as HVAC.
- Module loading ratio: comparison of the power (kW) required by the load (ITE) to the total installed power (kW).
- Design utilization ratio: a comparison of the total number of power supplies, including those used for redundancy, to the minimum number required to support the load.

9.1.5.2 Overview

Capacity is the power required by the load and is designated as “N”. High-density loads require substantial kW to operate; therefore, a substantial power system infrastructure is required to support them. Higher levels of availability (based on the criticality of the activity supported by the data center) require higher levels of redundancy, which drives the Class described in Appendix B.

The size of the system required to serve the load on an N basis (the capacity) should not be confused with the overall system size that would be required for the selected Class. Because higher Classes require higher levels of redundancy and power protection, the highest level of availability will seldom have the highest utilization efficiency.

An effective method for communicating the load-required kW versus the total installed kW is the design maximum module loading ratio. Generally speaking, within a given Class, the higher the ratio, the better. Table 9-1 shows some examples of design efficiency ratios. Design efficiency or utilization efficiency should not be confused with “operating efficiency”, which is a performance characteristic of an installed device or system.

Table 9-1 displays four different levels of design efficiencies for an N+1 topology. For example, if N is 100 kVA, N+1 redundancy can be achieved in any one of the following ways:

- 2 × 100 kVA modules (50%)
- 3 × 50 kVA modules (66%)
- 4 × 33 kVA modules (75%)
- 5 × 25 kVA modules (80%)

Table 9-1 Design Efficiency Ratios

<i>Topology</i>	<i>UPS or power systems ratio</i>	<i>Design efficiency (required kW/installed kW)</i>
N	1:1	100%
N+1	2:1	50%
N+1	3:2	66%
N+1	4:3	75%
N+1	5:4	80%
2N	2:1	50%
2(N+1)	6:2	33%
N + 2	3:1	33%
N + 2	4:2	50%
N + 2	5:3	60%
N + 2	6:4	66%

Class F3 systems are similar to Class F2 on a systems basis, except they possess the second power path. Class F3 and Class F4 systems rarely have design efficiencies over 66%. There is a mathematical point of diminishing returns for large UPS systems with the number of distinct plants versus the power paths to the load.

Increasing the number of components beyond the minimum needed results in more components, which usually implies less reliability and a higher probability of failure. Having two 100kVA modules is typically less expensive and more reliable than having five 25kVA modules. However, other factors might be considered. For example, one might choose a higher number of modules because:

- Smaller modules may be easier to install or to replace.
- Consequences of a failure in any one of the modules may be less.
- Smaller modularity allows for scalability.
- Overall operating efficiency (and operating cost) may be better.

9.1.6 Electrical Class Ratings

9.1.6.1 Introduction

Appendix B describes data center facility Availability Classes in general terms and provides details on how they are calculated. This section details the application of data center facility Availability Classes to electrical systems and provides specific design information concerning the electrical system for achieving each Class. The standard includes five Classes relating to various levels of reliability of the data center facility infrastructure. The Classes are completely performance related.

The five Classes are:

- Class F0 - a single path data center that meets the minimum requirements of the standard, but doesn't meet the requirements of an F1 or higher level data center
- Class F1 - the single path data center
- Class F2 - the single path data center with redundant components
- Class F3 - the concurrently maintainable and operable data center
- Class F4 - the fault tolerant data center

Several factors can affect Class over the life of the data center, including:

- Redundancy
- Capacity
- Expandability
- Maintainability
- Survivability
- Quality

While some elements of higher Classes are only more expansive versions of lower Classes, there are segments of the electrical systems that make a specific and notable change when jumping between Classes. This can be seen in the change between Classes in the critical power system.

Classes might not be consistent throughout the utility infrastructure systems. Electrical systems are circuited to the loads that they serve, and specifically, the mechanical and electrical systems are matched as an integrated approach for the data center and facility as a whole. For example, if the mechanical ventilation system is offered at $N + 2$, the electrical system must maintain the mechanical system's Class through the electrical system's normal, maintenance and failure modes of operation.

Oftentimes, the electrical system may not possess a consistent Class between different electrical subsystems. This is completely appropriate. While it is desirable to render the electrical system at a consistent Class for the entire electrical system, it is often not practical because of cost, space, operability, or reliability. To discover the Class need of a given system, criteria needs to be developed that meets the end user's availability and reliability needs for the facility. The purpose of this evaluation is to discover the actual needs for the critical load or constituent components. This "needs assessment" then allows the end user and system designer to choose the most appropriate system for their particular situation. (See Appendix B for the general guidelines for the evaluation process.)

As a part of this evaluation process, the end user and system designer need to determine the ability of a given system to respond to normal, maintenance, and failure modes of operation and how that system affects their critical facility operations. Therein lies the performance-based definition. The kinds of questions asked when defining a Class are:

- Is the load disconnected with a given outage?
- Is the load disconnected during a given maintenance activity?
- Is redundancy lost with a given outage?
- Is redundancy lost during a given maintenance activity?
- For components that are deferred from the initial construction, can they be added transparently to the existing, operating loads, or is a shutdown or some form of accommodation in excess of optimum facility operation required?
- If the system loading changes on the UPS or generator, will that affect the Class?
- How long can the system run with an absence of utility power?

Redundancy increases both fault tolerance and maintainability. However, it also increases system complexity, which is a leading cause of human error. Redundancy and overall system complexity must be weighed against the overall system capacity, ease of operation, cost, and schedule. Therefore, while redundancy and the resulting availability figures might be quite good, the time the system is available might be reduced because of the system's complexity and configuration.

While the concept of Classes is useful for specifying the levels of redundancy within various data center systems, circumstances might dictate a combination of Classes. For example, a data center located where utility electric power is less reliable than average might be designed with a Class F3 electrical system but only Class F2 mechanical systems. The mechanical systems might be enhanced with spare parts to help ensure a low mean time to repair (MTTR).

The total data center Class is only as high as the lowest rated Class subsystem. For example, the overall data center would be rated Class F2 with a Class F2 mechanical system even though it has a Class F3 electrical rating.

NOTE: There is no allowance for a plus or minus rating to a Class, and the use of terms, such as Class F3+, are not recognized by this standard.

It should also be noted that human factors and operating procedures could also be very important. Hence, the actual availability of two Class F3 facilities may vary widely.

9.1.6.2 Class F0 Description

A Class F0 electrical system is an electrical infrastructure that meets the general requirements of Section 9, but it does not meet one or more requirements listed for Class F1.

The system cannot be maintained while it is operating and a failure of any element in the power path will likely result in the loss of electrical service to the load. Some form of power conditioning, such as voltage regulation or surge suppression, may be available, but a loss of utility power will almost definitely result in dropping the load. Single points of failure are common throughout the system. Any downtime, whether planned or unplanned, will result in critical load interruption.

A representation of a Class F0 topology is shown in Figure 9-1.

Table 9-2 Class F0 Electrical System Overview

Industry description:	Single path
Component redundancy:	None
System redundancy:	None
Power sources available to critical load:	One
UPS sources available to the critical load:	None (Optional)
Ability to be maintained while under load:	No
Ability to recover from failures:	No
Resulting definition:	Single path/single module/single source

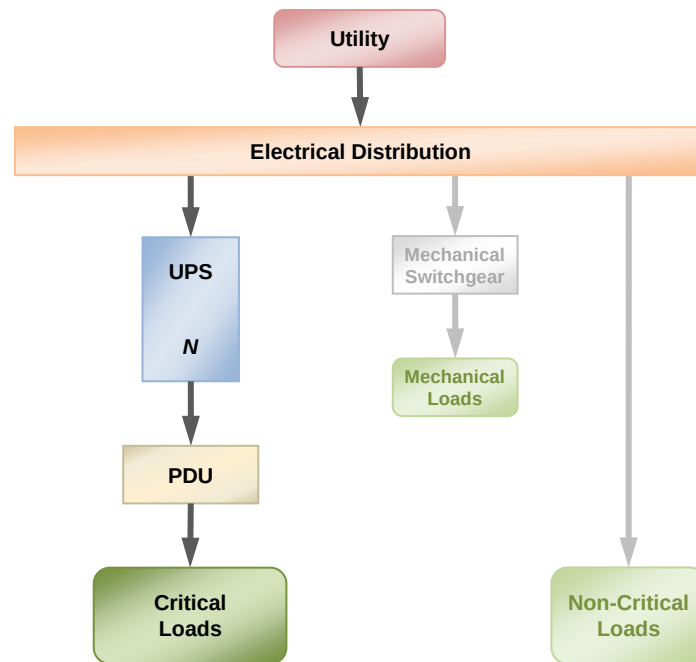


Figure 9-1

Class F0 Electrical Concept Diagram (Configuration Without Backup/Alternate Power)

9.1.6.3 Class F1 Description

A Class F1 electrical system is an infrastructure with no redundancy. This system cannot be maintained while it is operating, and a failure will likely result in a loss of electrical service to the load. Single points of failure are common throughout this system. Critical load interruptions are likely during planned and unplanned downtime.

A representation of a Class F1 topology is shown in Figure 9-2.

Table 9-3 Class F1 Electrical System Overview

Industry description:	Single path
Component redundancy:	N
System redundancy:	N
Power sources available to critical load:	One
UPS sources available to the critical load:	One
Ability to be maintained while under load:	No
Ability to recover from failures:	No
Resulting definition:	Single path/single module/single source

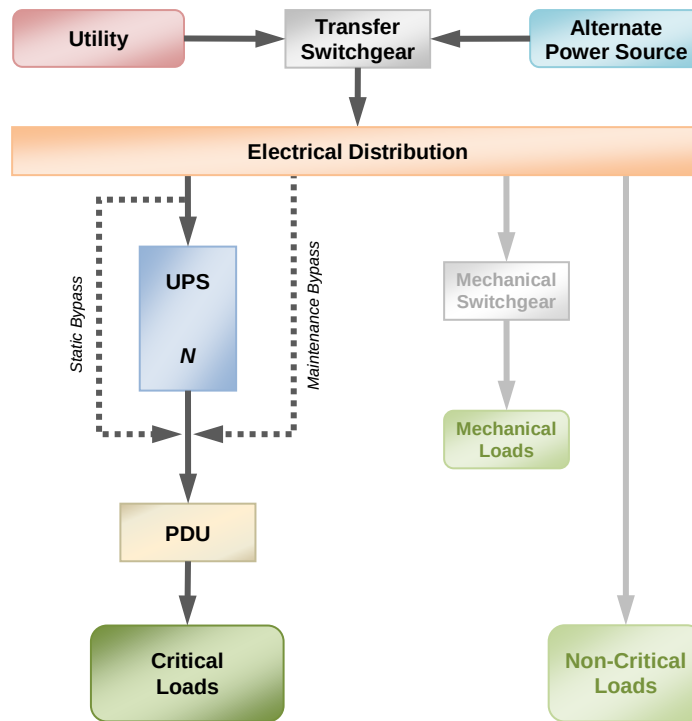


Figure 9-2
Class F1 Electrical Concept Diagram

9.1.6.4 Class F2 Description

A Class F2 system possesses component redundancy, but it does not have system redundancy. Redundant components may exist on an N+1 and paralleled basis in the UPS and generator systems, but a Class F2 system does not offer redundancy in the distribution system. A failure in one of the N+1 components may not result in a load failure, but it would reduce the redundancy level in the systems to N. This system has a single electrical supply to the load and no source diversity. Any failure in the distribution system will likely result in a loss of electrical service to the load. Large-scale system maintenance cannot be performed without interruption to the load.

Single points of failure are present in the distribution system, and critical load interruptions are likely during both planned and unplanned downtime. A representation of a Class F2 system is shown in Figure 9-3.

Table 9-4 Class F2 Electrical System Overview

Industry description:	Single path with redundant components
Component redundancy:	N+1
System redundancy:	N
Power sources available to critical load:	One
UPS sources available to the critical load:	One
Ability to be maintained while under load:	At the system level only, but not in the distribution system
Ability to recover from failures:	Only at the system level.
Resulting definition:	Single source/multiple module/single path

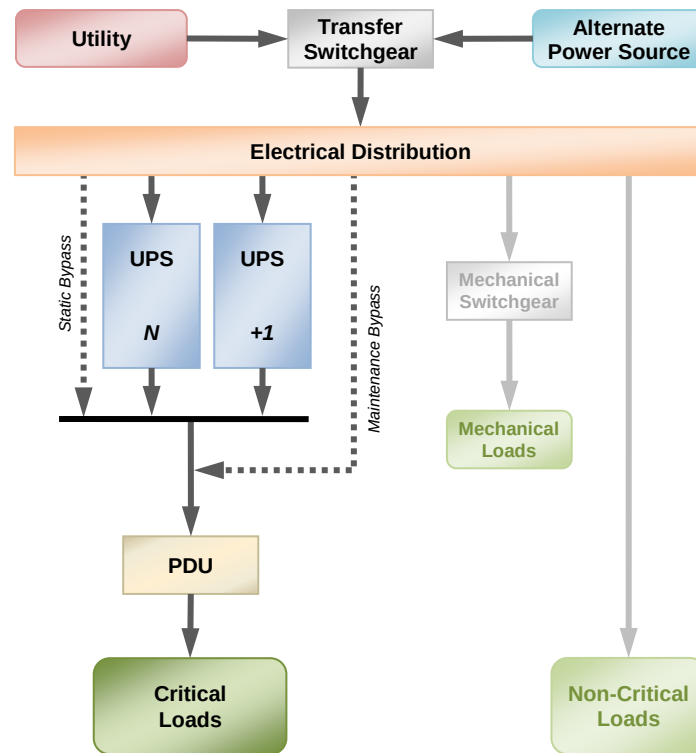


Figure 9-3
Class F2 Concept Diagram

9.1.6.5 Class F3 Description

The Class F3 system possesses redundancy in the power paths to the critical load, but only one of those paths needs to be UPS powered. The alternate path may be UPS powered, but this Class requires that it only be available and dedicated to the IT load. On a dual-corded IT device, one input would be fed from the UPS power system, while the other input is fed from the non-UPS source.

The individual critical power systems are rated for a portion of the total load with a common and centralized dedicated UPS system providing the redundant supply to the line systems. The redundant system, similar to the line systems, may possess either a single or multiple modules. This concurrently maintainable system provides load source selection either via static transfer switches or by the internal power supplies in the IT systems themselves. There are no single points of failure in either the critical power system or the power systems supporting the mechanical or vital house/support loads.

The Class F3 system allows for complete maintenance during normal operations (on a planned basis), but it loses redundancy during maintenance and failure modes of operations. STSs are required for single-corded loads to provide power redundancy where no IT component redundancy exists. STSs are not required for dual-corded loads.

All maintenance and failure modes of operation are transparent to the load.

Two representations of a Class F3 system are shown in Figure 9-4 and Figure 9-5.

It is not a requirement to parallel all UPS outputs so long as UPS units can transfer loads without interruption. UPS units can be configured in “Catcher” configuration (see Section 9.1.6.7).

Table 9-5 Class F3 Electrical System Overview

Industry description:	Concurrently maintainable and operable
Component redundancy:	N+1, as a minimum
System redundancy:	N
Number of utility sources:	One source with two inputs or one source with single input electrically diverse from backup generator input.
Power sources available to critical load:	Two
UPS sources available to the critical load:	One UPS system with one UPS power path to the load.
Ability to be maintained while under load:	Yes, with a reduction of the system redundancy from N+1 or better to N during maintenance activities.
Ability to recover from failures:	At the plant and distribution level, but with a reduction of the system or distribution redundancy from N+1 or better to N after failure and prior to the recovery.
Resulting definition:	Multiple source/N rated single or multimodule system/dual or multiple path

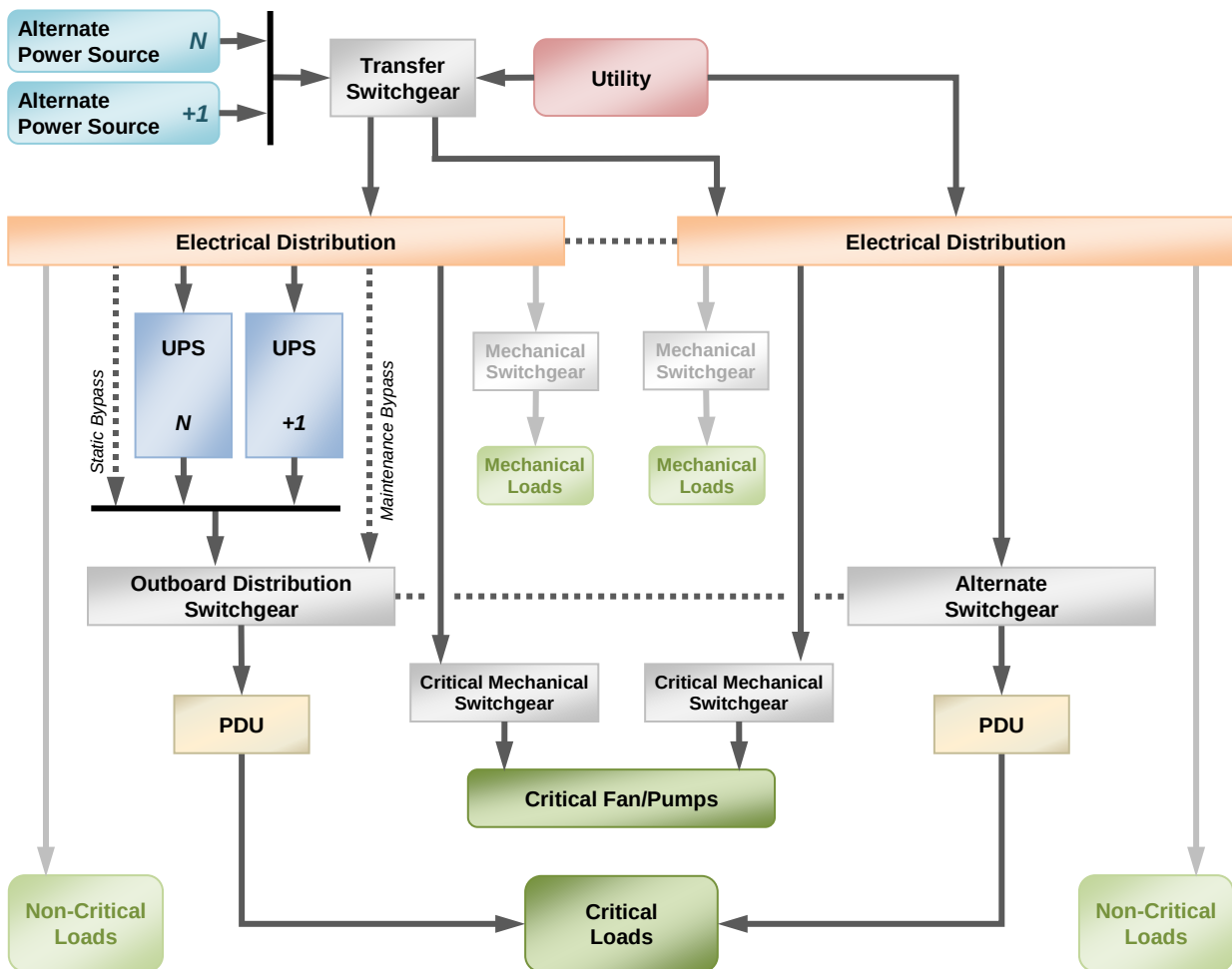


Figure 9-4
Class F3 Single Utility Source with Two Utility Inputs

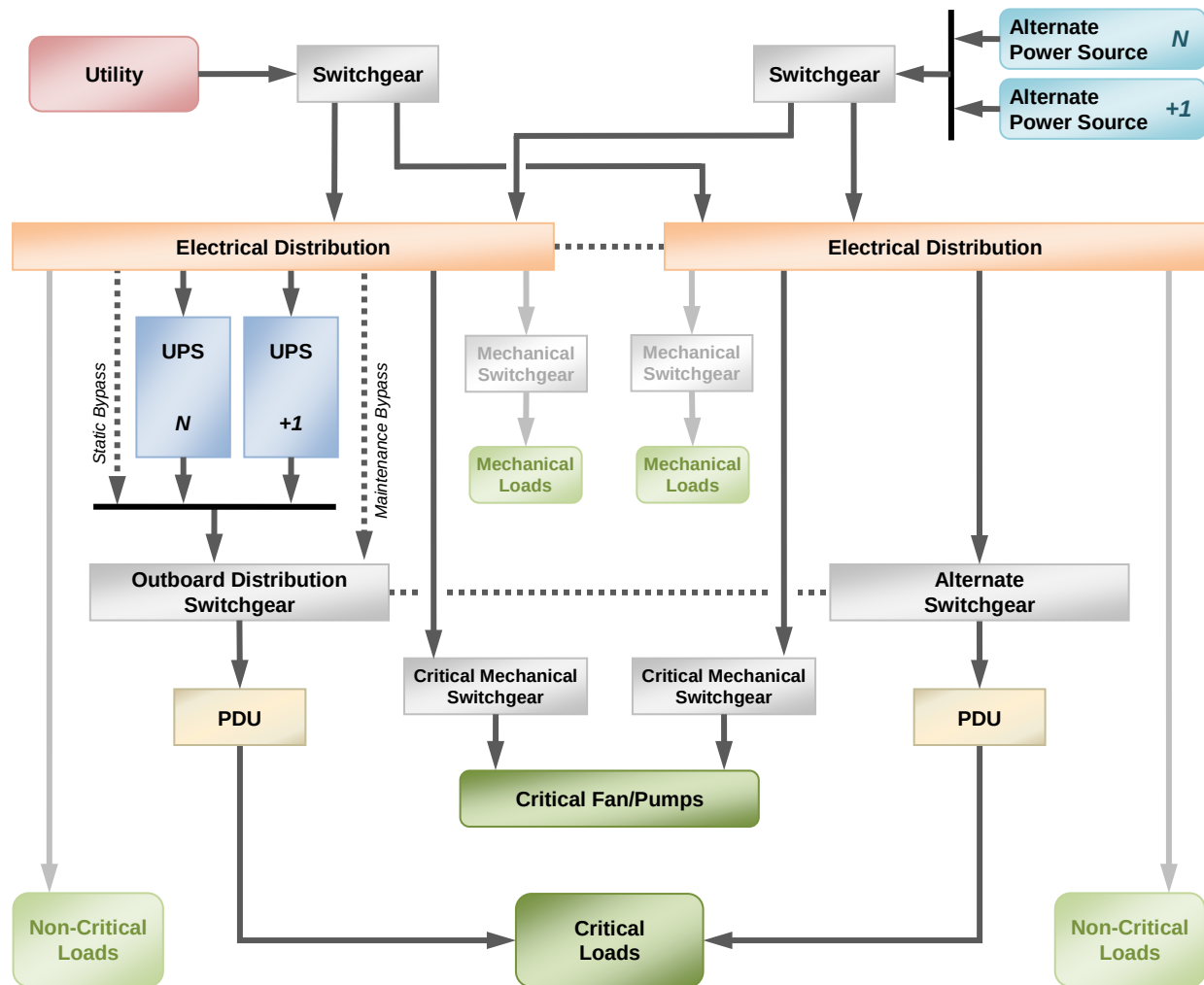


Figure 9-5
Class F3 Single Utility Source with Single Utility Input

9.1.6.6 Class F4 Description

A Class F4 system possesses redundancy in the power paths, and there may be more than two independent sources of UPS power to the critical load. The individual critical power systems are rated for the complete load for the $2(N+1)/\text{system-plus-system}$ option. For larger loads, the system may have multiple UPS systems where the system diversity is provided solely by the connection of the critical loads to the multiple UPS systems. Each UPS system could be a multimodule UPS system or a single/high-kW UPS system. The fault tolerant system provides load source selection either via static transfer switches or by internal power supplies in the IT systems themselves. There are no single points of failure in either the critical power system or the power systems supporting the mechanical or vital house/support loads. The Class F4 system allows for complete maintenance during normal operations and does not lose redundancy during either failure or maintenance modes of operations.

All maintenance and failure modes of operation are transparent to the load.

Redundant components should be compartmentalized and separated in different rooms to enhance survivability.

Continuous cooling is required for ITE. Typically, this will require fans and pumps to be on UPS power.

The Class F4 representation for a shared/distributed redundant and $2N$ are illustrated in Figure 9-6 and Figure 9-7.

It is not a requirement to parallel all UPS outputs so long as UPS units can transfer loads without interruption. UPS units can be configured in “Catcher” configuration (see Section 9.1.6.7).

Table 9-6 Class F4 Electrical System Overview

Industry description:	Fault tolerant
Component redundancy:	Equal to or greater than $N+1$
System redundancy:	Yes
Number of utility sources:	One or more sources with two inputs
Power sources available to critical load:	More than two
UPS sources available to the critical load:	Two or more
Ability to be maintained while under load:	Yes, with a reduction to no worse than $N+1$ during maintenance activities.
Ability to recover from failures:	Yes, automatically with a reduction to no worse than $N+1$ after the failure and prior to the recovery.
Resulting definition:	Dual or multiple sources/ $2(N+1$ or better) power systems/multiple paths with redundant components.

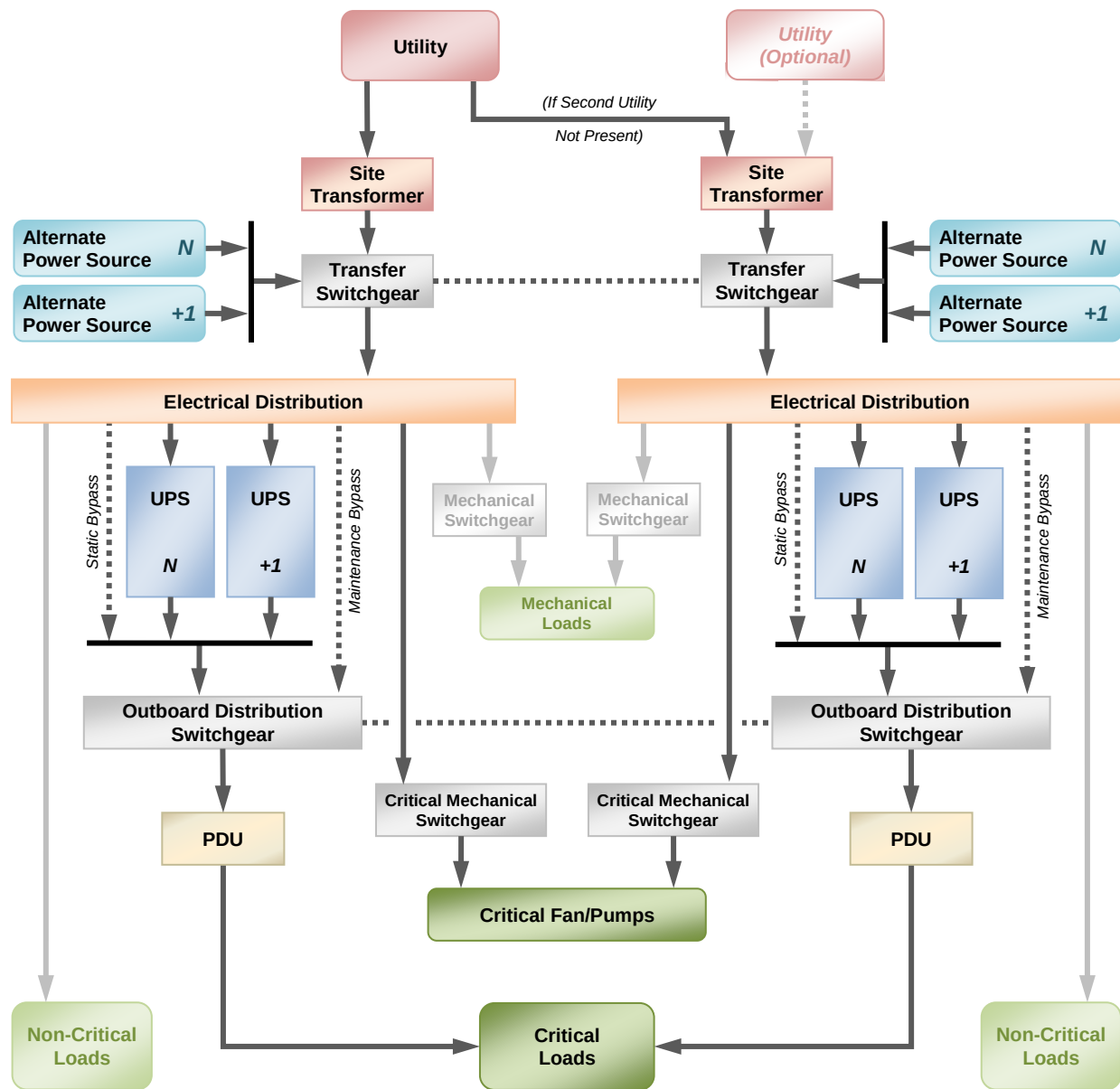


Figure 9-6
Class F4 Electrical Topology (System-Plus-System)

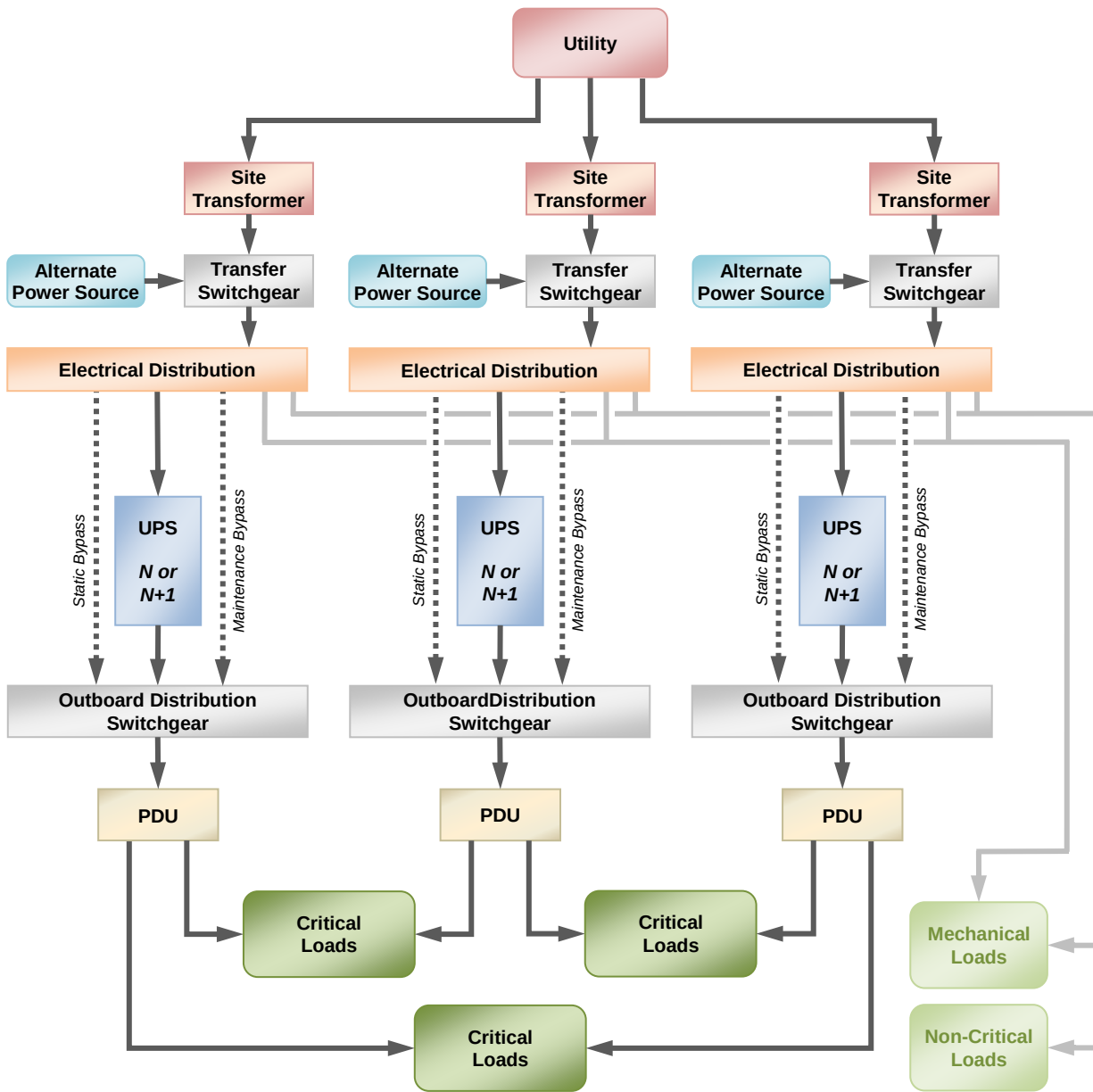


Figure 9-7
Class F4 Electrical Topology (xN Or Distributed Redundant)

9.1.6.7 Electrical System Topologies with Uninterrupted Transfer of Loads**9.1.6.7.1 Introduction**

The UPS output need not be paralleled in order to qualify for F3 or F4 level so long as the uninterrupted transfer of load between normal and standby UPS modules is facilitated. A “Catcher” UPS system in which multiple “live” UPS units share a single standby unit (which also acts as a synchronizing unit) via internal static bypass is one such example.

The Catcher UPS topology is a combination of what has been known as “isolated redundant” and “block redundant.” The Catcher topology is similar to the isolated redundant topology in that the output of the redundant UPS module is connected to the static bypass inputs on the normal UPS modules. It is also similar to the block redundant topology in that the output of the redundant UPS module is also connected to the critical UPS output distribution boards. However, in a block redundant topology, the UPS output distribution boards are automatically fed from either the normal UPS module or the redundant UPS module through an automated transfer scheme. In the Catcher topology, the selection of the UPS output distribution board’s input source is a manual operation, selecting either the normal or redundant UPS module. This manual operation is an added feature to provide planned concurrent maintainability, and the isolated redundant functionality provides the automated failover in the event of a component or system failure.

9.1.6.7.2 F3 Electrical System Based on “Catcher” UPS configuration

In Figure 9-8, a sample F3 design with single utility source is shown. In an F3 design, the A and B side of a critical load can both come from the same UPS unit as there is a static transfer to the standby UPS unit available in the event of the failure of the normal UPS. Putting A and B sides on different UPS units will further improve reliability, particularly if the two UPS units are normally supplied from different medium voltage (MV) distributions.

Under normal operating conditions, each “live” UPS unit synchronizes to its bypass circuit, which is, in turn supplied from the “Standby” unit output. Therefore, each UPS unit is individually synchronized to the standby unit without using any centralized synchronization system.

NOTE: See Figure 9-20 for the internal configuration of a typical ‘Catcher’ UPS unit.

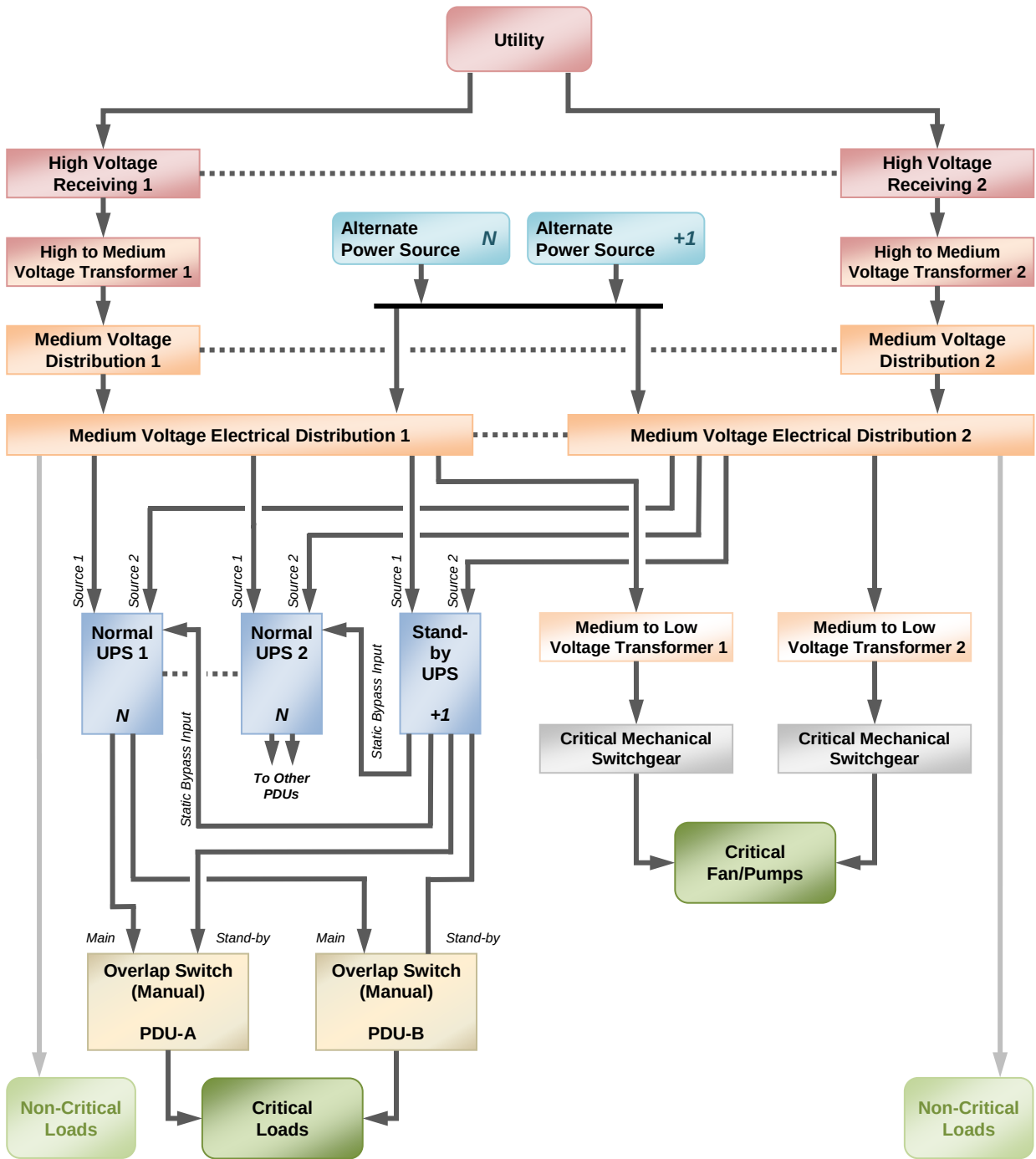


Figure 9-8
Class F3 Single Utility Source with Two Utility Inputs “Catcher” System

9.1.6.7.3 F4 Electrical System with “Catcher” UPS Configuration.

In Figure 9-9, a sample F4 design with two utility sources is shown. With the current trend toward high density computing with average load per rack of 10 kW or more, there is no longer enough thermal capacity in the server rooms to keep server inlet temperature below 40 °C (104 °F). In these scenarios, critical cooling systems (e.g., CRACs, chilled water pumps, fans) are placed on their own dedicated and redundant UPS.

NOTE: When the number of modules to make N is greater than 1, the Catcher system requires more UPS modules than a 2(N+1) Class F4 configuration.

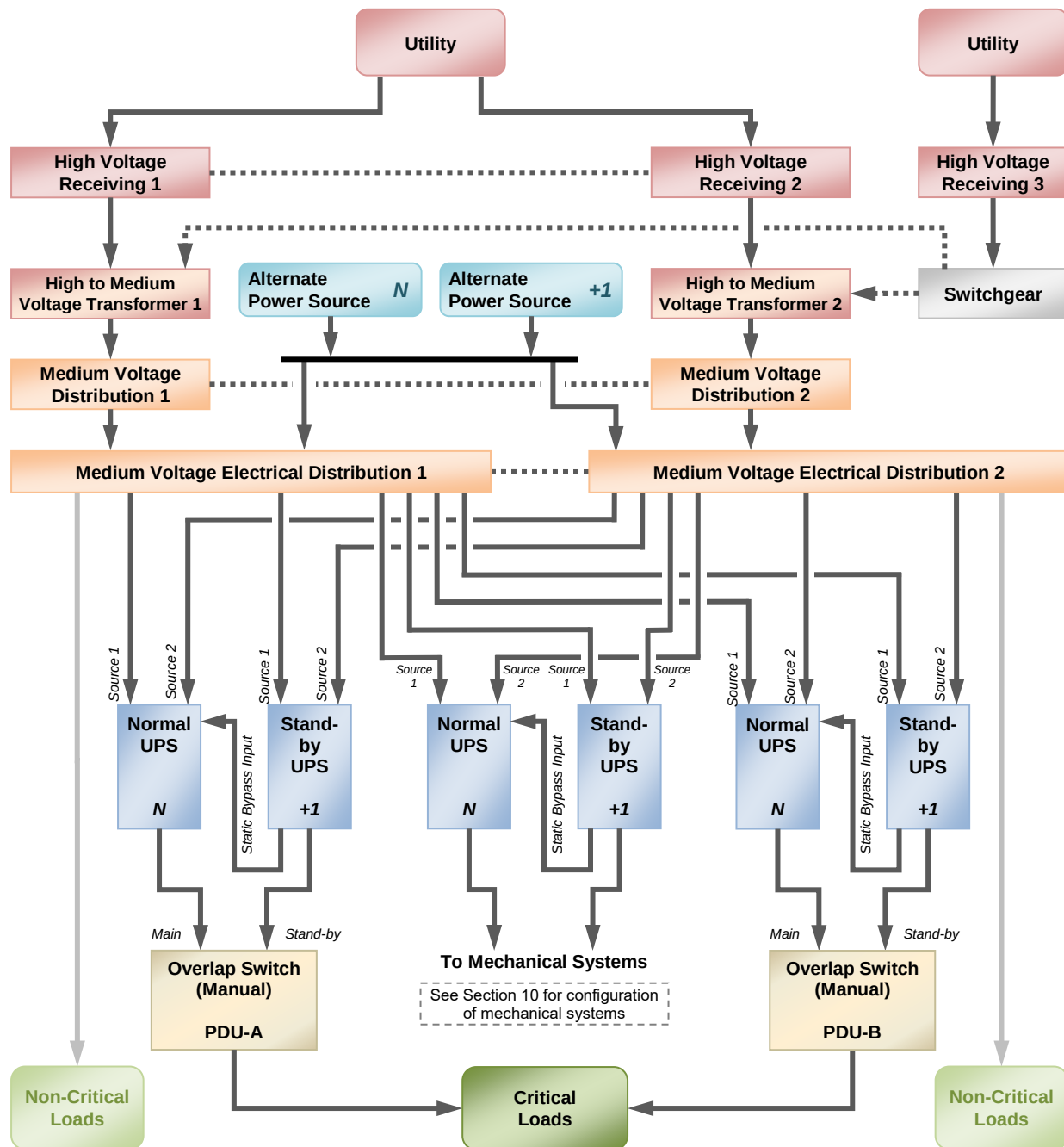


Figure 9-9
Class F4 2(N+1) Electrical Topology with Dual Utility Inputs

9.2 Utility Service

9.2.1 Utility Service Planning

9.2.1.1 Recommendations

NOTE: Section 5.7.1 contains additional information applicable to utility service planning.

When considering the power services to a given site, the utility should be treated the same as the generator sources. While it is not possible to control the utility, it does constitute an N source to the facility.

Several planning issues concerning the utility service should be considered. For example, consideration should be given to what other utility customers are served by the same utility feeder. Hospitals are desirable neighbors because they typically receive high priority during outages or are classified as a no-shed block in the utility's distribution system. Industrial users are not desirable neighbors because of the transient voltage disturbances and harmonic conditions they often impose on the feeders and the utility systems. Many of these conditions either can reduce the life of the data center's systems, especially the batteries and UPS modules, or require other sophisticated power quality mitigation measures.

While planning for utility services, the following issues should be addressed:

- Is there a need for a dedicated service based on the load size or redundancy requirements for the site?
- Is the site on a shared service and, if so, is anyone else on the service?
- Are there any high impulse loads on the bulk substation such as foundries, paper plants, and smelters that would have an impact on power quality?
- Is service to the site primarily overhead or underground?
- What are the initial and the ultimate capacities of the service, and how can these services be expanded if needed?
- Are diverse services available?
- Are diverse services routed separately to the site?
- What are the service voltages in the area?
- What are the requirements for closed transition operation, if employed?
- What are the circuit protection requirements that the site must provide?
- What are the service construction requirements?
- What are the reliability and availability of the service to the site?
- What is the available fault duty at the main switch?
- What are the ground and short-circuit fault current discrimination requirements both upstream and downstream?
- What automatic reclose/transfer is performed at the local utility substation, and how will it affect ATS timing?

This analysis occurs during the preliminary project phases with the utility company's service representative to the user or area. The purpose here is to ascertain the electrical performance, short circuit duty, and power quality for the utility.

Underground utility feeders are preferable to overhead feeders to minimize exposure to lightning, weather, trees, traffic accidents, and vandalism.

There is no mandatory service voltage. It is left to the designer and user to select the service voltage that is appropriate for the site's data center power system from among the voltages available from the utility. However, in most countries, the incoming supply voltage options are decided by the electricity supply company based on the required load.

When diverse services are utilized, the designer should establish the point of common coupling of the supplies with the utility company. The supplies should be routed to the site separately and should enter the data center on opposite sides of the property and building. In this situation, a bond is required between systems to ensure an intersystem grounding reference.

An intersystem grounding reference for diverse services can be accomplished by a building ground (electrode) ring. See Section 9.9.6 for requirements and recommendations for a building ground (electrode) ring.

9.2.2 Low-Voltage Utility Services

9.2.2.1 Introduction

In North America the demarcation between low voltage and medium voltage utility services has always been 600 V_{AC} between line conductors, whereas elsewhere around the world it is 1000 V_{AC}. This changed within the United States with publication of the *National Electrical Code* in 2014 when the demarcation was raised to 1000 V_{AC} (although changes to regulations, standards, and equipment designs will not be immediate). Table 9-7 provides a listing of low voltage distribution voltages present within some major data center locations worldwide.

Service entrance distribution equipment provides several functions: the interface between the utility and the site, the distribution of utility power to downstream systems and, in some cases, the transfer controls and transfer point between the utility and generator.

9.2.2.2 Recommendations

The distribution equipment should be designed for growth, maintenance, and the ultimate load expected for the facility while maintaining the Class level's redundancy. The utility distribution equipment should either be sized for the ultimate load for the site or should possess the ability to add capacity later without undue disruption to ongoing operations.

When the service entrance distribution equipment is double-ended (with two utility entrances), the tie breakers should be provided in pairs. This allows the complete isolation and maintenance of one side of the distribution equipment while the opposite side carries the load.

Consider:

- Using switchgear with compartmentalization in lieu of switchboard with open construction for greater resiliency and separation of components to minimize internal damage because of faults.
- Using drawout or withdrawable circuit breakers to allow addition or maintenance of circuit breakers without interrupting power to operating equipment.
- Arc flash hazards when designing distribution equipment. Lower arc flash hazard ratings may allow preventative maintenance and infrared scanning to be performed more often and allow safe operation of operating equipment.

Circuit breakers should be interchangeable where possible between spaces and distribution equipment line-ups. Careful consideration should be given to breaker standardization throughout the entire project. Concurrent maintainability of any system is directly related to its Class level.

9.2.2.3 Additional Information

Low-voltage services may require utility-controlled disconnecting means at the property line. The local fire department might also require a shunt trip for the complete disconnection of power to the site when they respond to a fire.

Surge protective devices (SPDs) should be provided for all Classes to mitigate problems because of switching surges or transients from sudden power outages.

9.2.3 Medium-Voltage and High-Voltage Utility Services

Medium-voltage refers to utility services that are between 1001 V_{AC} to 35 kV_{AC} between line conductors. As utility services vary between regions and countries, check with the AHJ for the local voltage definitions and standards of medium voltage and high voltage.

A medium voltage service has the same recommendations as the low-voltage service, but the medium voltage service may have different grounding criteria. The service configuration may be in concert with the generator plant configuration acting together as multiple sources or providing an input to various unit substations located in the data center facility.

Table 9-7 Low-Voltage Distribution Voltages in Some Major Data Center Locations

Country	Voltage(s) (V)	Tolerance (%)	Phase/Wire	Frequency (Hz)
Australia	415/240	+/- 6	3P4W	50
	440/250	+/- 6	3P4W	50
	440 ¹	+/- 6	1P1W	50
EU	380/220	+/- 10	3P4W	50
	380	+/- 10	3P3W	50
	220	+/- 10	1P2W	50
Hong Kong	346/200	+/- 6	3P4W	50
	380/220	+/- 6	3P4W	50
Japan	100	+/- 10	1P2W, 3P3W	50 (East)/60 (West)
	200	+/- 10	1P2W, 3P3W	50 (East)/60 (West)
	100/200	+/- 10	1P3W	50 (East)/60 (West)
	400	+/- 10	3P3W	50 (East)/60 (West)
	230/400	+/- 10	3P4W	50 (East)/60 (West)
Singapore	400/230	+/- 3	3P4W	50
South Korea	380/220	+/- 5	3P4W	60
USA	480/277	+/- 5	3P4W	60
	480	+/- 4	1P2W	60
	460/265	+/- 5~10	3P4W	60
	460	+/- 5~10	1P2W	60
	240/120	+/- 5~10	3P4W	60
	240/120	+/- 5	3P4W	60
	240/120	+/- 4~5	3P4W	60
	240/120	+/- 5	1P3W	60
	240	unavailable	1P2W	60
	230	+/- 5~10	1P2W	60
	208/120	+/- 4~10	3P4W	60
	208/120	+/- 5	3P4W	60
UK	415/240	+/- 6	3P4W	50

NOTE: Single wire to ground, mines only

9.2.4 Protective Relaying

9.2.4.1 Requirements

The use of protective relaying is based primarily upon how the service is delivered and whether transfers between the utility(s) and the onsite generator plant(s) are either closed- or open-transition. Multifunction relays are typical, but the utility may require utility-grade, individually mounted relays. The utility will also typically extend its relaying specification to any closed-transition systems. Relay specifications will be coordinated with the utility's protection system, and the manufacturer and model of the relay system may be dictated by the utility.

9.3 Distribution

9.3.1 Requirements

The distribution system design shall accommodate the number and diversity of the power paths to the loads, the ability to readily maintain the loads, and the ability to recover from failures.

Common to all systems is the type of termination for cables and busway connections. See Table 9-15 for busway and cable connections.

9.3.2 UPS Rectifier or Motor Inputs

9.3.2.1 Requirements

Paralleled module inputs shall be fed from the same unit substation or distribution point where all modules in the paralleled system must have the same input. Distributed or individual modules in larger UPS systems may be fed from their different upstream substations or distribution systems as long as those systems possess some form of output or load-side synchronization.

9.3.3 Static Switch Bypass Inputs

9.3.3.1 Introduction

All solid-state UPS systems and some rotary UPS systems have static bypass capability. Its function is to automatically transfer load between the UPS and an alternate power source without human intervention when the UPS system controls detect a condition in which the UPS cannot function properly.

9.3.3.2 Requirements

For UPS systems with a static bypass switch, either a single power module system's controls or a paralleled system's control cabinet shall be synchronized to the static system input.

9.3.4 UPS System Bypass

9.3.4.1 Introduction

A maintenance bypass provides a manually operated and closed-transition power path external to the static bypass power path. A maintenance bypass allows the UPS module(s), paralleling controls, and static switch to be totally de-energized so that unscheduled remedial or scheduled preventive maintenance can be safely performed.

9.3.4.2 Requirements

Maintenance bypasses shall be provided for all Class F1 through Class F4 systems.

Isolating circuit breakers shall be provided to allow for the maintenance of the UPS collector bus, static switch, or output breaker.

Static bypass switches may be located in the individual module or separately for paralleling multiple UPS systems with multiple power modules. For modules utilizing individual static switches, commonly called distributed paralleling, caution must be taken when an individual module in a paralleled installation is placed into static bypass in order to avoid uneven current flow through the modules. This may require that all modules in the distributed parallel installation be placed into bypass per the manufacturer's recommendation.

9.3.5 Power Strips

9.3.5.1 Introduction

Power strips allow multiple IT devices to plug into a single branch circuit. An example of a power strip is shown in Figure 9-10.

9.3.5.2 Requirements

Where used, power strips shall comply with the following requirements:

- Only AHJ permitted connections, such as junction boxes, shall be allowed under an access floor.
- Power strips shall be listed for ITE.
- Power strip ratings shall be coordinated with the upstream breaker and wiring system.
- Power strips shall be positively and mechanically attached to the cabinet interior.

Multiple power strips mounted in a cabinet shall bear proper labeling and shall be organized not to interfere with network cabling. Similarly, power strips shall be located in order to minimize crossing of the distinct power supply cords (e.g., A and B) as they are routed to the power strip from the IT platform.

9.3.5.3 Recommendations

Where used, power strips should comply with the following recommendations:

- Metering may be provided on individual power strips. The ability to monitor power strip loads remotely via a centralized monitoring system is recommended for high-density and large-scale facilities. The accuracy of metering on some power strips can be affected by voltage and current distortion caused by harmonics or other causes. The accuracy of power strip meters should be considered if the measurements are being aggregated for PUE calculations.
- Power strips should not have internal surge suppression.
- Power strips should not be placed under the access floor.

9.3.6 Input Source Transfer

9.3.6.1 Introduction

When considering the top layer of the electrical distribution system, the first consideration is the management of the utility and generator sources and the transfer scheme most appropriate for the facility. Similarly, the transfers may occur within a self-contained system such as an automatic transfer switch (ATS), or via a circuit breaker transfer pair. Another consideration is the ability to bypass the transfer location either via a bypass power path external to the ATS or in another circuit breaker transfer pair.

For many sites, the generator system as a whole powers the entire site or building. Should this be the case, the generator controls and the input source transfers become part of the utility's service entrance equipment. In this case, the utility metering and circuit protection may be included in the transfer controls. Figure 9-11 illustrates ATS of various sizes and in various locations within a facility.

For transfer protocols, there are four families of controls:

- Open transition
- Closed transition/quick transfer
- Closed transition/load walk-in
- Closed transition/parallel operation

Regardless of the transfer protocol, a utility outage almost always results in an open transition transfer upon the loss of the utility because of the momentary loss of source(s) and the resulting utility dead bus.



Figure 9-10
Example of a Power Strip for Mounting in ITE Cabinets

9.3.6.2 Open Transition

9.3.6.2.1 Introduction

Open transition occurs when the transfer between sources breaks before the opposite connection is made. This transfer technique is the most common, requires the least amount of electrical controls and relaying to assure its success, and typically does not require the utility's approval to deploy. The downside to this technique is that any transfer between energized and available sources results in a brief load disconnection. The loss of main's power forces the UPS to draw upon its stored energy source, thereby reducing the UPS battery system's life. It also typically causes the mechanical system (air conditioning systems) to stop and restart, thereby putting stress on the equipment and creating a potentially sharp increase in heat.

9.3.6.2.2 Recommendations

Open transitions should be several seconds long to allow power supply capacitive energy to dissipate.

9.3.6.3 Closed Transition/Quick Transfer

9.3.6.3.1 Introduction

In the closed transition/quick transfer the utility and generator (and consequently, the site) are paralleled for less than 100 ms to up to one minute, depending on the utility provider and designer. The paralleling time is typically the operating time of the ATS or the breaker transfer pair. The primary benefit of this method is that there is no load interruption between the two energized and available sources. The downsides to this technique include:

- Requiring more controls and relaying than open transition
- The electrical system's short circuit duty must account for both the utility's and the site generator's contribution
- The transfer can be delayed or prevented if the sources are present and do not remain synchronized within voltage and frequency tolerance
- Capacitive or harmonic feedback from the load(s) may cause logic errors
- The utility may not allow this type of operation in a customer's system

9.3.6.3.2 Recommendations

Close coordination with the utility is vital in this instance.

9.3.6.4 Closed Transition/Load Walk-in

9.3.6.4.1 Introduction

The closed transition/load walk-in varies from the closed transition/quick transfer technique in that the generator and utility share load for a period of several seconds or as long as a minute or two. This can be very desirable as it places a substantially less amount of stress on the site's electrical system and eliminates load inrush. The downside is that it requires a substantial amount of relaying and forces a complex sequence of operation in the electrical system.

9.3.6.4.2 Recommendations

Close coordination with the utility is vital in this instance.

Incoming power feeds and main low-voltage switchboard



Power distribution



Loads



Figure 9-11
Example ATS Sizes and Locations

9.3.6.5 Closed Transition/Parallel Operation

9.3.6.5.1 Introduction

In the closed transition/parallel operation, the generator and utility share load for an indefinite period of time. This can be for peak shaving or cogeneration purposes. The downside is that it requires a substantial amount of relaying and forces a complex sequence of operation in the electrical system.

9.3.6.5.2 Recommendations

Close coordination with the utility is vital in this instance. Review of environmental restrictions will be required. Coordination will include short circuit bracing for facility equipment for extended transfer times, conditions for manual transfers, and extended relay coordination and functionality.

9.3.7 Generator Controls and Paralleling

9.3.7.1 Introduction

Generator systems can be either distributed or paralleled for any of the Classes. Some generator control systems consist of traditional switchgear systems while some systems utilize controls on board the generators and ATS's. Regardless of the method or technology used, the controls must match the Class requirements to achieve the overall availability demanded by the critical, mechanical, and house power systems. Specific consideration should be given to paralleling switchgear systems that might represent single points of failure. While a paralleled generator system may offer an N+1 or N + 2 level of redundancy for components, the single paralleling bus or the master controls may represent a single point of failure. Paralleling switchgear should be provided with fully redundant paralleling controls for Class F3 and Class F4 applications. Generator controls address numerous critical functions for the site and generator systems.

These functions may include:

- Automatic load control and assumption upon loss of the utility source
- Retransfer to utility once it is restored after a preset retransfer delay
- Exercise and maintenance rotation of the engine(s)
- Distribution of generator power to any remote source transfer locations

9.3.7.2 Recommendations

Generator controls for individual machines should not be centralized, and each controller should be completely contained on the generator skid or within the generator control module in the switchgear line-up. The generator control section or module should possess all controls and metering for the individual machine and will not require any form of outside influence or connection for its individual operation. Individual machines should be able to operate regardless of the availability of the paralleling controls.

The enclosure or room where generators are installed should be temperate, but not necessarily conditioned. Draw-out type switchgear is recommended for Class F3 and Class F4 facilities, but it may also be used for lower Classes. Standby power systems should be installed in a manner that allows for 360-degree maintenance and technician access to the machine, both while it is in operation and when it is not.

The primary switchgear should be designed to handle all projected requirements as this equipment is difficult to replace once the data center is in operation. The system should be designed to allow for maintenance and expansion pursuant to the site's ultimate load requirements.

Paralleled generators should be capable of manual synchronization in the event of failure of automatic synchronization controls. Consideration should be given to manual bypass of each generator to feed directly individual loads in the event of failure or maintenance of the paralleling switchgear.

See Sections 9.3.15, 9.7.2, and 9.10 for other requirements.

9.3.8 Unit Substations

9.3.8.1 Introduction

Unit substations may combine several functions at one location: the medium voltage input selection or utility input, a step-down from the utility or site's medium to low voltage, utility metering, low-voltage power distribution, and input source control. These systems can utilize multiple medium-voltage inputs from different upstream sources, provide medium-voltage transfer systems (primary selection) or a low-voltage transfer system (secondary selection), and may be double ended for further source and distribution redundancy.

9.3.8.2 Recommendations

The unit substations may be located where the normal-alternate transfer is addressed on the input side of the system or serve as the upstream input to downstream ATSS. For larger systems, the input source transfer may occur at the input main (one from the utility and one from the generator or alternate system) where it is coupled with a dedicated alternate power input. Unit substations are routinely located immediately upstream of the UPS power plant, major mechanical loads, and the noncritical systems.

Unit substations are also defined as a pad-mounted transformer and the main switchboard.

There also may be an interposing main breaker system to relocate the main arc flash hazard to outside the electrical room. While consisting of different components than a traditional unit substation, this type of system is now in wide use and is analogous to the unit substation systems herein described.

See Sections 9.3.15, 9.7.2, and 9.10 for EPO monitoring, labeling, and similar considerations that could apply to unit substations.

9.3.8.3 Additional Information

An oil transformer is generally located outside because of fire risks. Because of extreme heat, the oil can leak and further spread the flames. A dry type or SF6 gas-insulated transformer can be located indoors and does not require the same degree of maintenance. In Europe, reference CENELC EN 50541-1 for dry-type transformers. It defines much lower allowable losses and noise limits.

9.3.9 UPS System

9.3.9.1 Introduction

The project designer and end user should determine the precise distribution topology that is most appropriate to the final design based on the client's needs.

While the static UPS system is the prevalent technology used, the requirements of this section apply to all types of UPS technology.

Power system distribution addresses six areas:

- UPS module rectifier inputs
- Static system inputs
- Maintenance and external bypass inputs and configurations
- Output switchboard configuration
- Output switchboard ties and alternate power paths
- Multi-system UPS power system synchronization

These systems are considered to reside between the unit substations and the critical power distribution switchboards.

One of the key issues for UPS systems is grounding simplicity and the prevention of harmonic circulation (this problem is reduced for modern ITE loads). In this case, the discussion for all of the UPS power system assumes a 3-wire input and output with 4-wire systems only being used for stand-alone UPS systems where the step-down transformer is part of the output transformer function of that module and for 400/230V UPS systems.

For Class F1 and F2 systems, UPS power distribution is basically linear with no cross-ties or mixing of loads. For Class F3 systems, multiple second power paths emerge although not all are required to be UPS powered. The goal for the Class F3 model is to provide multiple power paths as close to the critical load as possible.

For the Class F4 model, UPS power topology may include different numbers of UPS power plants versus the number of UPS power delivery paths. For example, there may be a site with 3 or 4 distinct UPS plants but many more individual UPS power distribution systems. Therefore, numerous UPS power distribution systems can be connected below a given UPS plant.

Bonding and grounding is further discussed in Section 9.9.

9.3.9.2 Bypass Switch Inputs

9.3.9.2.1 Introduction

The bypass system directly affects the Class of any UPS system. The static bypass, the maintenance bypass, the output breaker, and any load bank testing connections can all have a direct impact on the maintenance and failure response of the UPS system.

Class F0 systems (in which a UPS is optional) and Class F1 systems might have a single input into a UPS system in which a static bypass circuit is tapped internally to the UPS module (see Figure 9-12). For all other Classes, the static bypass has a dedicated input circuit.

As with all components of the electrical system, the ability to maintain a system while operating is a foundation of Class F3 systems, and maintaining a power path and redundancy are required for a Class F4 rating.

Bypass configurations can affect UPS functionality as follows:

- Combining maintenance bypass and static bypass paths from a single input feeder will typically result in a lower Class because it reduces the ability to remove a module or system without interrupting the service to the downstream critical loads.
- Load bank connections that are independent of the UPS output source can contribute to a high Class because they allow for testing without interrupting the service to the downstream critical loads.
- Locating circuit breakers on the collector bus or on the output bus of paralleled UPS systems rather than making them internal to a power module will contribute to a high Class by allowing a module to be removed from the service without shutting down the entire system. These are also known as isolation breakers.
- The presence of a maintenance bypass will allow for the removal or testing of a UPS module or for the replacement of a static switch in the event of a catastrophic failure. This has a dramatic effect on the mean time to repair (MTTR).

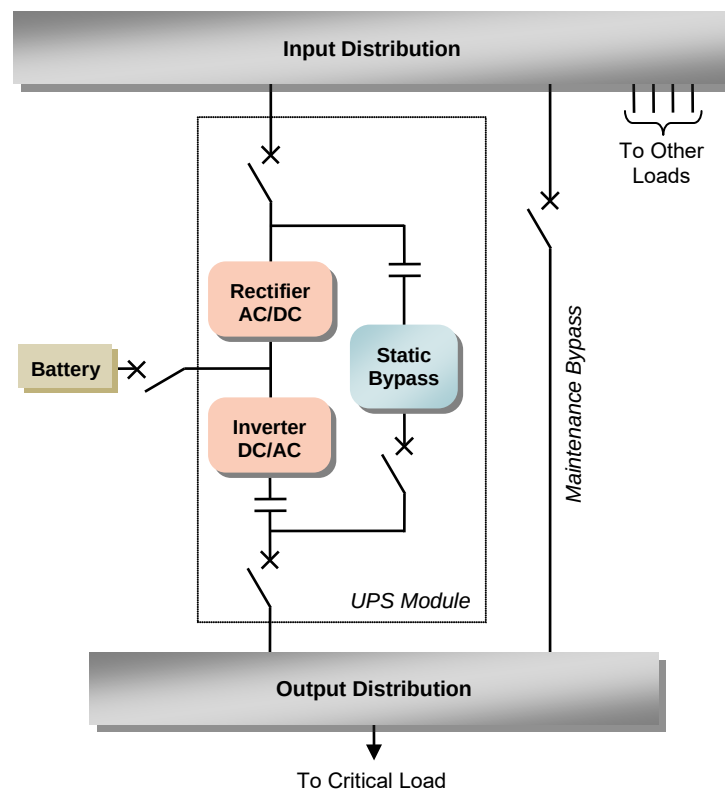


Figure 9-12
Single-Module UPS with Internal Static Bypass and Maintenance Bypass from the Same Source

External maintenance bypasses are optional for Class F0 (when a UPS is present), Class F1, and Class F2 systems. Maintenance bypass is mandatory for all Class F3 and F4 applications and for system control cabinets. As discussed in the preceding paragraphs, static bypass inputs may be combined with the rectifier inputs on Class F0 and Class F1 applications. The static bypass is the recommended means by which to synchronize the UPS to its maintenance bypass (see Figure 9-16 and Figure 9-17, and the discussion for Figure 9-17, Figure 9-18 and Figure 9-19). Classes F1 through F4 all require some form of maintenance bypass (whether it is factory provided in the bypass cabinet/system or externally developed).

Permanently installed load banks are optional for all Classes and are included at the discretion of the designer. They are not included in all of the examples shown in Figure 9-13 through Figure 9-19.

9.3.9.2.2 Requirements

Refer to Figure 9-13, Figure 9-14, and Figure 9-15. When the inputs to the rectifier, static bypass, and maintenance bypass are from the same input distribution bus, the designer shall consider the capacity of the input distribution bus and how the critical load could be affected during testing. The capacity of the input distribution bus shall be able to support the critical load on the maintenance bypass plus the full load testing of the UPS system. Also, if the input bus supports other loads, such as in a Class F1 or Class F2 design, those loads shall be considered in the capacity calculation of the input bus. The designer shall also consider how any disturbance on the input bus could affect the critical load while operating in this mode and this type of design, including disturbances caused by:

- Testing of the UPS
- Testing of other loads connected to the same bus
- Turning on and off other loads connected to the same bus
- Fault conditions

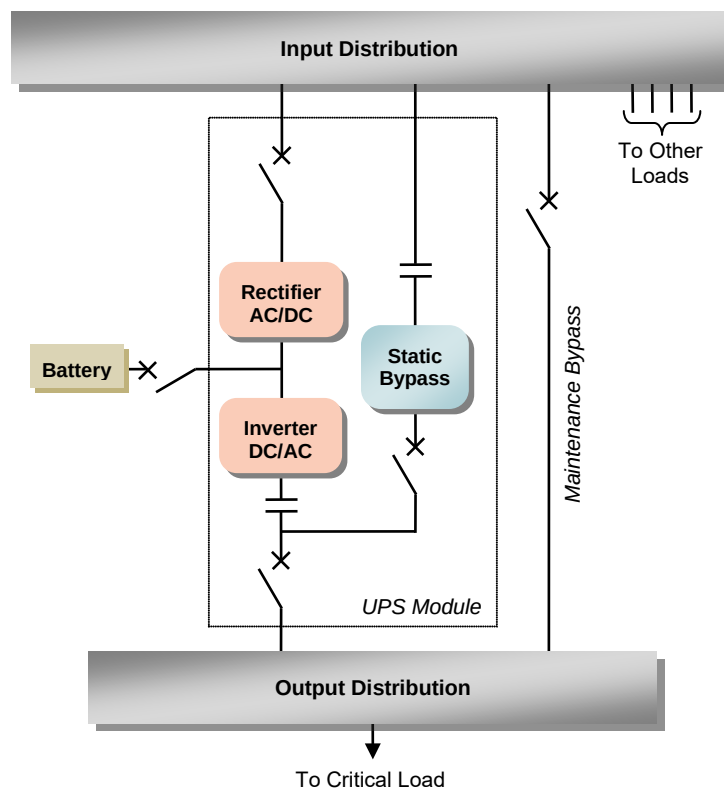


Figure 9-13
Single-Module UPS with Inputs to Rectifier, Static Bypass, and Maintenance Bypass from the Same Source

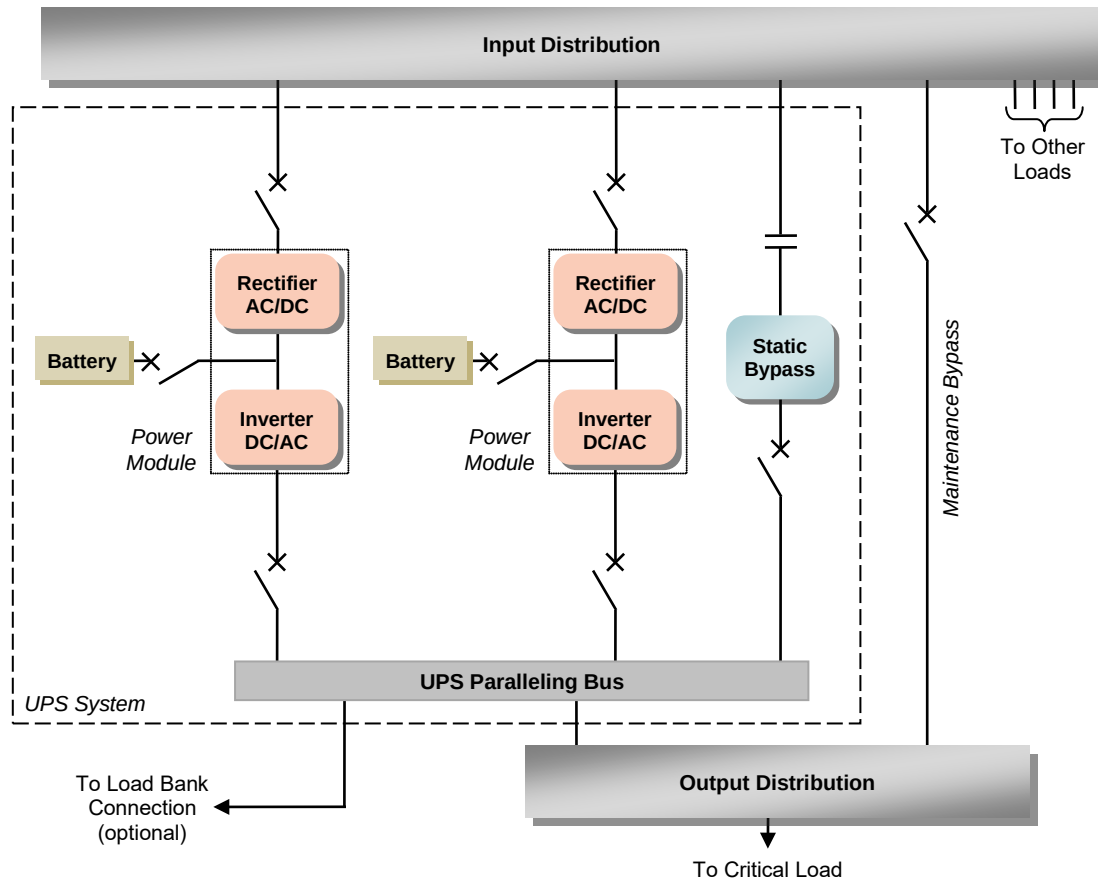


Figure 9-14
Multiple-Module UPS with Inputs to Rectifier and Maintenance Bypass from Same Source – Centralized Static Bypass

A single module with a static switch is shown in Figure 9-12. The paralleled installation for modules with individual static switches looks similar as shown in Figure 9-15. In this case, the static input for the system occurs at the module level. That static input can be combined with the rectifier input, or the module may receive a dedicated static input. Paralleling of UPS modules with an internal static bypass switch requires close coordination and synchronization with other UPS modules. Check manufacturer's requirements when applying different static and rectifier inputs in distributed paralleled UPS power systems.

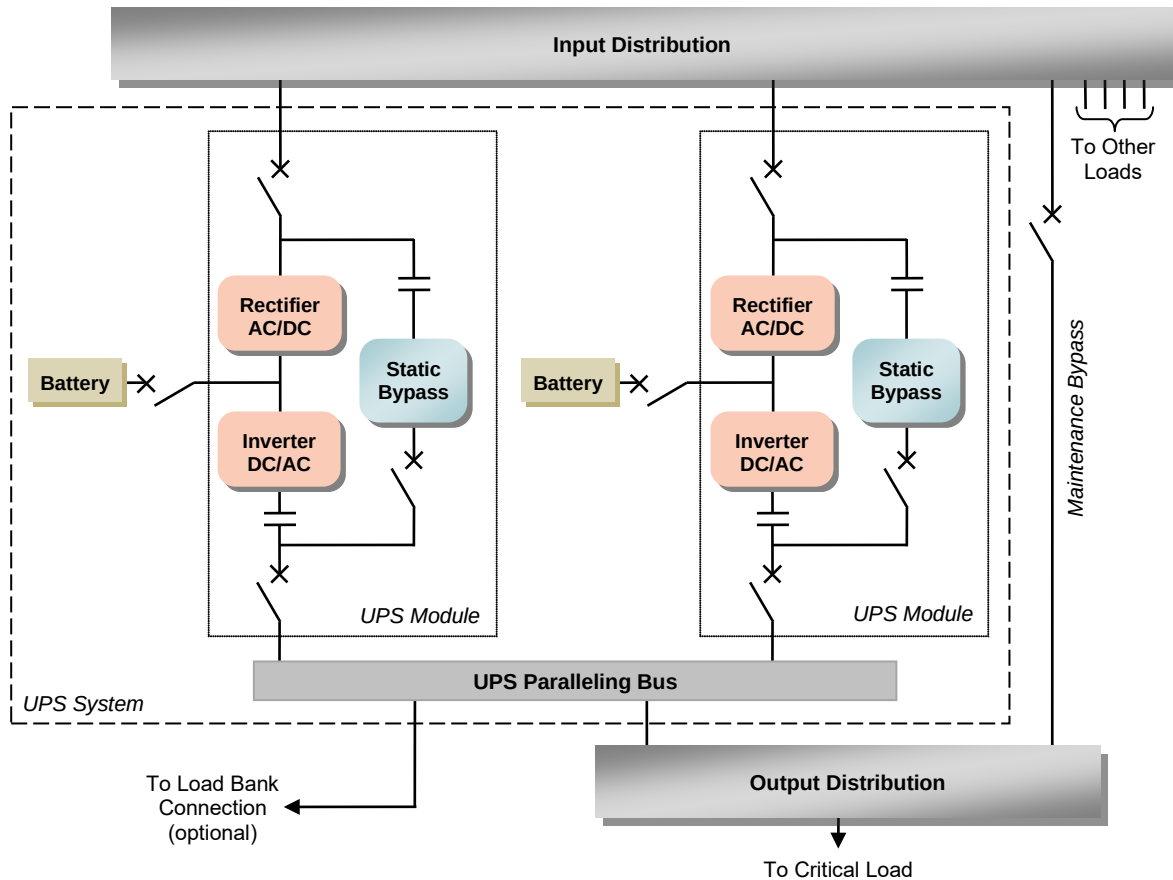


Figure 9-15
Multiple-Module UPS with Inputs to Rectifier and Maintenance Bypass from Same Source – Paralleled Installation

Refer to Figure 9-16 and Figure 9-17. When the input to the rectifier is from one bus and the static bypass and maintenance bypass originate from a different bus, the designer shall consider:

- The capacity of the input distribution bus
- The sources of power to the static and maintenance bypasses
- How the critical load could be affected during testing or if a fault were to occur on that bus

For testing purposes, when the two bypasses are derived from the same input distribution bus, the capacity of the input bus should be able to simultaneously support the critical load on the maintenance bypass plus the full load testing of the UPS system (e.g., full load transfers to and from static bypass). In addition, if any other loads are present, they shall also be considered in the capacity calculation of the input distribution bus. The designer shall also consider how any disturbance on the input bus could affect the critical load while operating in this mode and this type of design, including disturbances caused by:

- Testing of the UPS
- Testing of other loads connected to the same bus
- Turning on and off other loads connected to the same bus
- Fault conditions

In normal mode, the UPS shall synchronize its inverter to this bypass source. Therefore, if the bypass source has a disturbance, the UPS will more than likely go into an alarm state. When the static bypass input is lost for a system, the UPS system shall run in a free mode until either the static bypass input has been restored or the paralleled UPS input has been restored. There is one additional scenario to consider for this configuration. In the event a repair or fault removes the input distribution bus from service, the static bypass source will be lost and will place the UPS system into a less reliable operating mode.

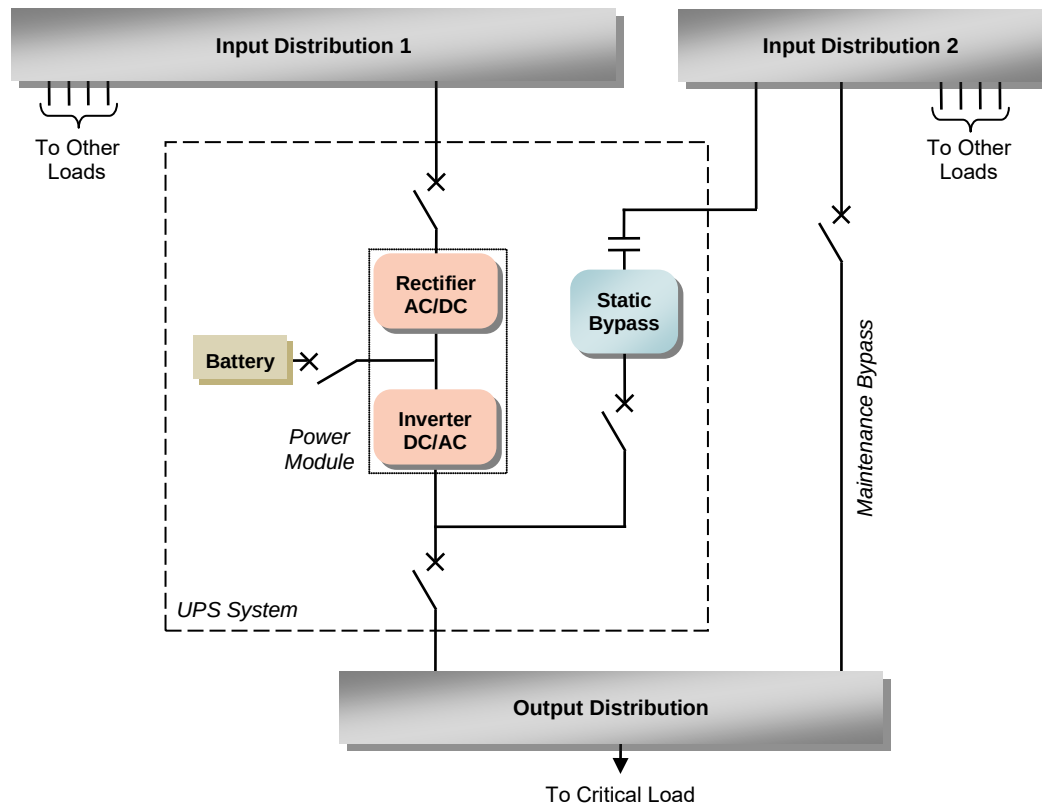


Figure 9-16
Single-Module UPS Bypass – Alternate Bypass Source - Input to Rectifier from Primary Source; Inputs to Static Bypass and Maintenance Bypass from a Second Source

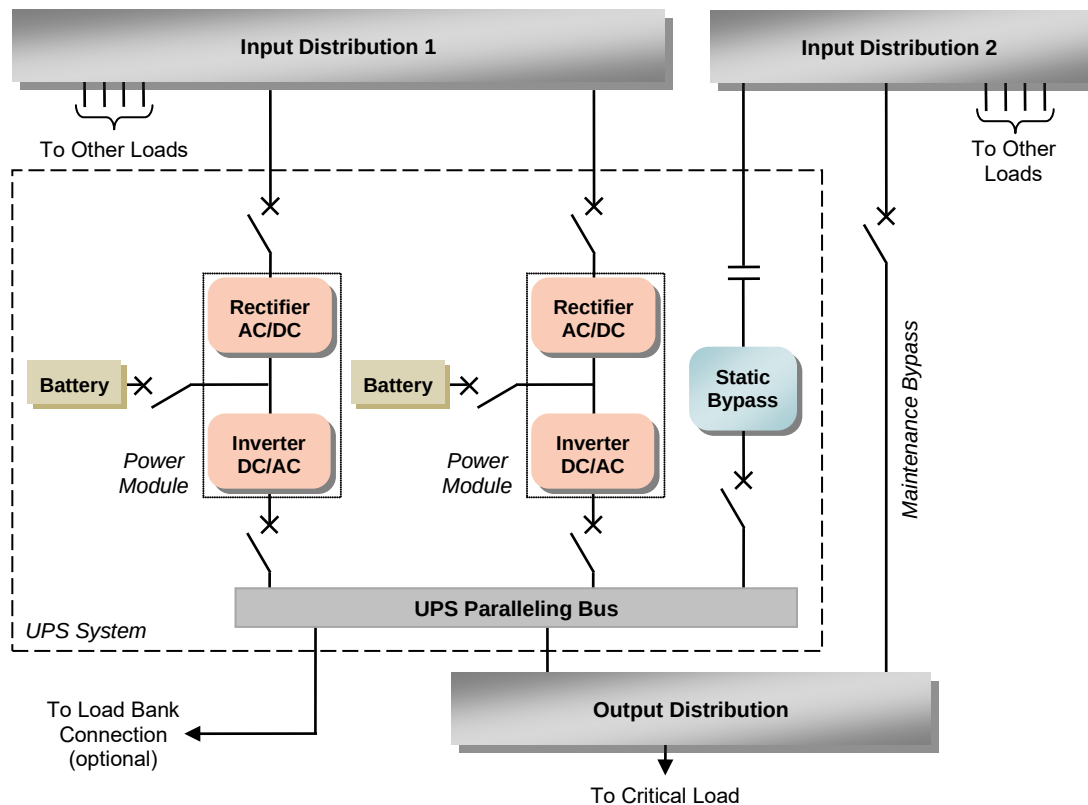


Figure 9-17
Multiple-Module UPS Bypass – Alternate Bypass Sources - Inputs to Rectifiers from Primary Source;
Inputs To Static Bypass And Maintenance Bypass From A Second Source

Figure 9-17 illustrates a central static switch for a paralleled UPS operation. Observe the conditions of use and design application for individual UPS modules and static switches in a paralleled mode of operation as noted in this section.

Refer to Figure 9-18 and Figure 9-19. When the input to the rectifier and the static bypass originate from one bus (Input Distribution 1) and the maintenance bypass originates from a separate bus (Input Distribution 2), the critical load shall be transferred without interruption or disturbance to an isolated source, either utility or generator, depending on the design, while the UPS is repaired or tested. When other loads are connected to the bus that supports either the rectifier and static bypass (Input Distribution 1) or the maintenance bypass (Input Distribution 2), the designer shall also consider how any disturbance on the input bus could affect the critical load while operating in this mode and this type of design, including disturbances caused by:

- Testing of the UPS
- Testing of other loads connected to the same bus
- Turning on and off other loads connected to the same bus
- Fault conditions

Inputs to the static bypass and maintenance bypass shall not be derived from separate sources unless the two sources are synchronized in phase and frequency (see Figure 9-18 and Figure 9-19). Lack of synchronization will result in an unreliable design that should require open transition (i.e., shut down the loads and then restart from the alternate source).

Note that synchronization of sources is difficult because load imbalances and phase shifts (such as transformers introduced downstream) can force circuits out of synchronization. The best practice is to power both the static bypass and the maintenance bypasses from the same source as shown in Figure 9-16 and Figure 9-17. (See also Section 9.3.9.3).

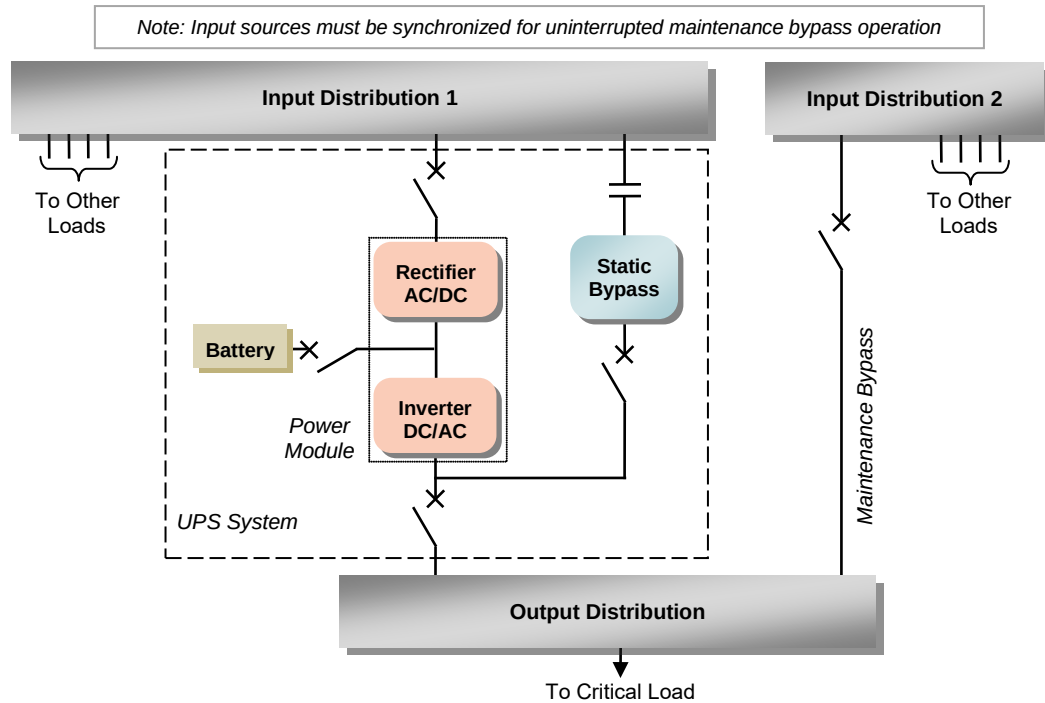


Figure 9-18
Single-Module UPS Bypass – Multiple Bypass Sources - Inputs To Rectifier And Static Bypass From Primary Source And Input To Maintenance Bypass From A Second Source

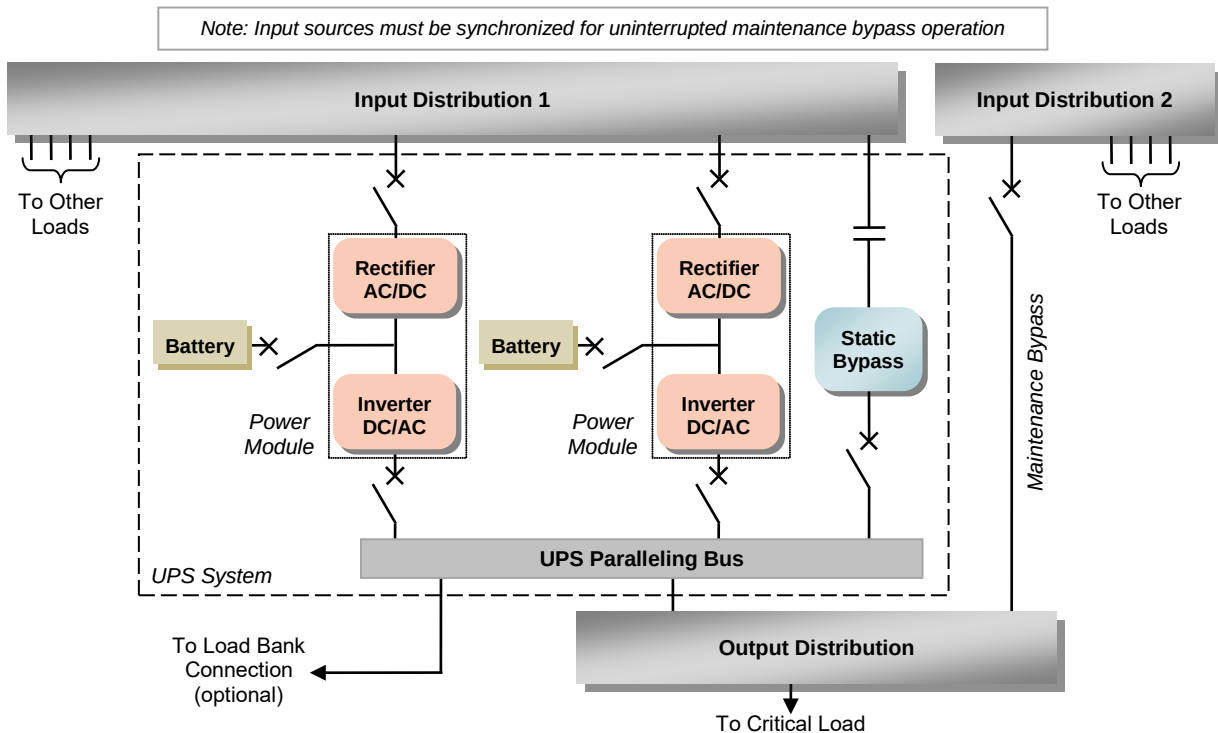


Figure 9-19
Multiple-Module UPS Bypass – Multiple Bypass Sources - Inputs to Rectifiers and Static Bypass From Primary Source, and Input To Maintenance Bypass From a Second Source

Figure 9-19 indicates a central static switch for a paralleled UPS operation. Note the conditions of use and design application for individual UPS modules and static switches in a paralleled mode of operation previously discussed in this section.

Figure 9-20 shows the internal configuration of a typical “Catcher” UPS unit.

A Catcher UPS has two inputs to the rectifier from primary and secondary sources, with the “mains” bypass sharing these same two sources with than input from a stand-by UPS. The static bypass in each unit ensures that the output will be bypassed either to the standby UPS unit or to the mains power without interruption in the event of the UPS unit failure.

9.3.9.2.3 Recommendations

The UPS system static bypass and maintenance bypass designs should consider using the same source or type of source for the closed transition transfer mechanisms. Normally, this would require the power module inputs, static bypass input, and the maintenance bypass input to be synchronized to the same source. Depending upon the configuration, some UPS could be exempted from this rule when the static bypass input and the output of the UPS are synchronized. For example, input to power module inputs could be fed from utility 480 V_{AC} wye source “A” while the static bypass and maintenance bypass could be fed from utility (or generator) 480 V_{AC} wye source “B”.

Other UPS configurations may have the maintenance bypass external to the UPS system to enable the UPS to be taken off-line for maintenance or replacement. It is acceptable to have the maintenance bypass internal to the UPS system in a Catcher system since the Standby UPS system can function as the external alternate path in the event the UPS system needs to be taken off-line for maintenance or replacement.

Attention shall be paid with respect to the configuration of disconnects external and internal to the UPS system to enable maintenance of rectifiers, inverters, or static bypass components in a safe manner.

A dedicated input to the static switch that is separate from the rectifier input allows the critical load to further sustain faults that could be associated with the rectifier. In Class F0 and Class F1 applications, a single source of input power for both the rectifier and the static bypass is permitted (see Figure 9-13).

In Class F2 applications, a single source of input power to the rectifiers and to a static bypass is permitted (see Figure 9-14), but best practice is to provide an input path to the static bypass that is discrete from the rectifier input (see Figure 9-16). Momentary-duty equipment is allowed where designs incorporate individual modules into the topology.

Fully-rated static bypass switches with dedicated inputs are recommended for all Class F3 and Class F4 applications and for all paralleled system control cabinets (see Figure 9-16).

If proper breaker coordination has been completed, the input(s) to the rectifier(s) should be selectively protected from a static input breaker failure.

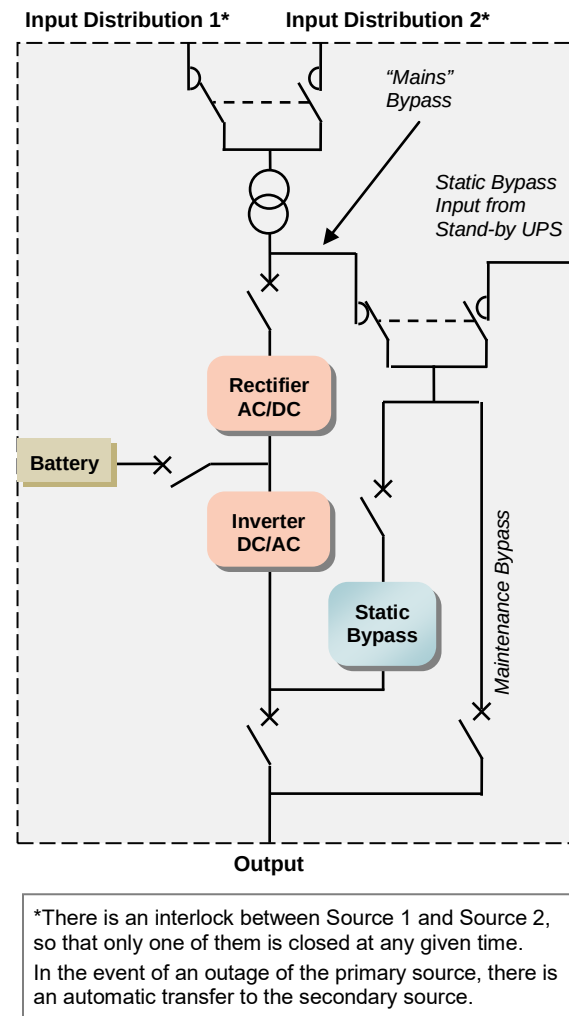


Figure 9-20
Topology Inside an UPS Unit

Table 9-8 Static Bypass Switch Input, By Availability Class

<i>Class</i>	<i>Description and Input source(s)</i>
F0	(UPS optional) Single power module with a single input to both the rectifier and the static switch
F1	Single power module with inputs to both the rectifier and the static bypass switch from the same upstream breaker
F2	Single or multiple power modules; all power module inputs from the same upstream distribution; static bypass switch input from a separate upstream breaker than the power module inputs.
F3	Multiple power modules; all power module inputs from the same source; static bypass switch input from a separate upstream breaker than the power module inputs
F4	Multiple power modules; all power module inputs from the same source; static bypass switch input from a separate upstream breaker than the power module inputs

9.3.9.3 Synchronization

9.3.9.3.1 Introduction

Synchronization can occur in one of two ways for UPS systems:

- Actively based on some form of external control system
- Passively by the management of the static switch inputs to the given modules or via active systems specific to the UPS manufacturer, depending upon the chosen UPS topology

The active systems offer excellent synchronization functionality, especially when the UPS system uses batteries. The passive system is important as vital system transfers are assured to be coordinated when the static inputs are managed and considered in the design. A lack of input or output synchronization could result in a failure of ASTS operation or an out-of-phase transfer, thereby resulting in a dropped load and possible equipment damage.

9.3.9.3.2 Requirements

UPS systems shall be synchronized in one of two ways:

- Line-side (source) synchronization
- Load-side (output) synchronization

In either event, synchronization is vital and shall be required for a high-reliability system at the Class F3 and Class F4 levels. Since Class F0, Class F1, and sometimes Class F2 systems are single module/single plant systems, no external synchronization is required.

When system-level synchronization is not possible, static switching at the loads or critical power buses may be required.

9.3.9.4 UPS Output Switchboards

9.3.9.4.1 Recommendations

Output switchboards directly support the PDU and ASTS systems downstream of the UPS power plants. For Class F1, F2, and F3 systems, UPS outputs should be vertically organized to the UPS output distribution system downstream. Simpler electrical topologies may not have separate UPS output switchboards and critical power distribution switchboards.

For Class F3 systems, the second path may be derived from a non-UPS source. For Class F4 systems, there may be multiple power paths, but these are kept separated until they meet at the critical load.

Section 9.3.14 discusses the UPS power distribution downstream from the UPS output switchboards and how these loads are served by these diverse power paths.

9.3.9.5 Ties and Interconnections

9.3.9.5.1 Introduction

As long as the UPS sources are synchronized and are not overloaded, UPS systems may transfer load between each other. Except on a plant level, the UPS is the foundation of the multicorded system for critical loads. All transfers are done via closed-transition, and the control systems for this type of operation are typically redundant or offer some other form of manual operation in the event that the control system fails.

9.3.9.5.2 Requirements

System ties are common in system-plus-system configurations, and several UPS system manufacturers offer pre-engineered solutions for this design feature. For xN or other types of UPS topologies, the system designer shall engineer a solution for the given UPS module and plant configuration.

9.3.9.5.3 Recommendations

Ties and interconnections should also prevent the propagation of failures and should limit short circuit fault current.

See Section 9.7.2 for monitoring requirements.

9.3.10 UPS Output Distribution

9.3.10.1 Introduction

UPS output distribution switchboards are located immediately downstream of the UPS power plants and extend to the PDU or data processing room levels. One important consideration for these systems is that they do not have to follow the redundancy level or plant counts found in the UPS power plants.

For example, for Class F1 systems, the UPS output distribution switchboards are single units. For Class F2 systems, there may be module redundancy, but there may not be UPS power path redundancy. In both cases, UPS systems would match the total UPS power paths. In a Class F3 system with a single UPS power plant, there are at least two UPS output powered critical distribution switchboards, one on the active path and one on the alternate, or non-UPS, path. For a Class F4 system, there are at least two critical power switchboards, if not more.

A summary of the UPS output distribution switchboard counts and configurations for each Class are shown in Table 9-9.

Table 9-9 Summary of UPS Output Switchboard Counts for Classes

<i>Class</i>	<i>UPS power plants</i>	<i>UPS power paths</i>	<i>UPS output switchboard count</i>
F0	One	One	One
F1	One	One	One
F2	One	One	One
F3	One or more	One or two	Two
F4	Two or more	Two or more	Two or more

9.3.10.2 Recommendations

UPS output distribution switchboards may come in numerous specifications and configurations, all depending on the maintenance and failure mode of the critical loads downstream and UPS systems upstream. The UPS output distribution switchboards may be in any of the following configurations:

- **Stand-alone or double-ended:**
Stand-alone switchboards are typically used for Class F1 and Class F2 applications or for Class F3 and F4 systems where load is not shared among UPS systems in pairs. Double-ended or interconnected switchboards are typically found in systems where the critical load is shared between a pair of systems or UPS power paths where they may be interconnected for inter-UPS output distribution redundancy. The switchboard configuration is most centrally related to the ability to shift load off an individual switchboard for maintenance. Some designs use the UPS paralleling switchgear or the UPS output distribution switchboard as a vehicle for closed transition load transfer and sharing either via chokes or static switching. This switch is located between the output buses and acts as a tie between them. The switch may feed the load directly or just provide lateral relief for maintenance or failure recovery. This concept is illustrated in Figure 9-21.
- **Automatic versus manual controls for source transfer:**
Controls are locally operated. Failure mode response is always automatic (and that might mean doing nothing and letting other system components swing the load around) while maintenance mode response is always manual.
- **Always closed transition to avoid load interruption:**
Since the UPS output distribution switchboards are located downstream of the UPS system, any switching operations need to be closed-transition (make-before-break) to avoid load interruption.

The diversity and configuration of the UPS output distribution switchboards is at the discretion of the system designer and user.

An example of critical power switchboard interconnection and diversity is shown in Figure 9-21.

Figure 9-21 indicates central static switch for a paralleled UPS operation. Note the conditions of use and design application for individual UPS modules and static switches in a paralleled mode of operation noted in this section.

9.3.11 Power Distribution Units (PDUs)

9.3.11.1 Introduction

While most PDUs in North America have transformers, this is not typical in countries where the nominal voltage is already 230/400V. PDUs with an isolation transformer create a separately derived neutral for downstream loads although this may not be necessary for 3-phase loads or for systems in which the load utilization voltage is created at the UPS. PDUs with transformers convert the output voltage of the UPS system to the utilization voltage of the critical loads as needed. Regardless of the application, the PDU always has output branch circuit panelboards or distribution circuit breakers that serve the downstream critical loads or subpanelboards serving downstream critical loads. The overcurrent protective devices are usually circuit breakers although fuses are sometimes used for DC distribution systems.

9.3.11.2 Recommendations

A PDU is usually provided as a fully integrated, factory-tested, and listed product. In addition, the term “PDU” can be applied to a combination of site-connected elements, including a transformer, metering, controls, and power distribution panelboards.

If the PDU has an isolation transformer, its inrush characteristics should be coordinated with the upstream UPS peak load tolerances for normal, failure, and maintenance modes of operation. Low inrush transformers may also be employed depending on the UPS system’s design.

Where PDUs are expected to run close to their rated loads or one or more loads will generate large harmonic currents, a K-factor transformer might be considered. Harmonic currents can be created by the ITE (e.g., switched mode power supplies [SMPS]), but they can also be created by fans or drives that are connected to the PDU critical bus. High harmonic currents, especially those caused by single-phase power supplies in the ITE that create triplen harmonics (odd multiples of the 3rd harmonic, such as 3rd, 9th, 15th, 21st), can cause PDU output voltage distortion and transformer overheating. This heating reduces the efficiency of the transformer and increases the load on cooling equipment. These problems can be exacerbated when the PDU’s transformer is operated close to its rated capacity.

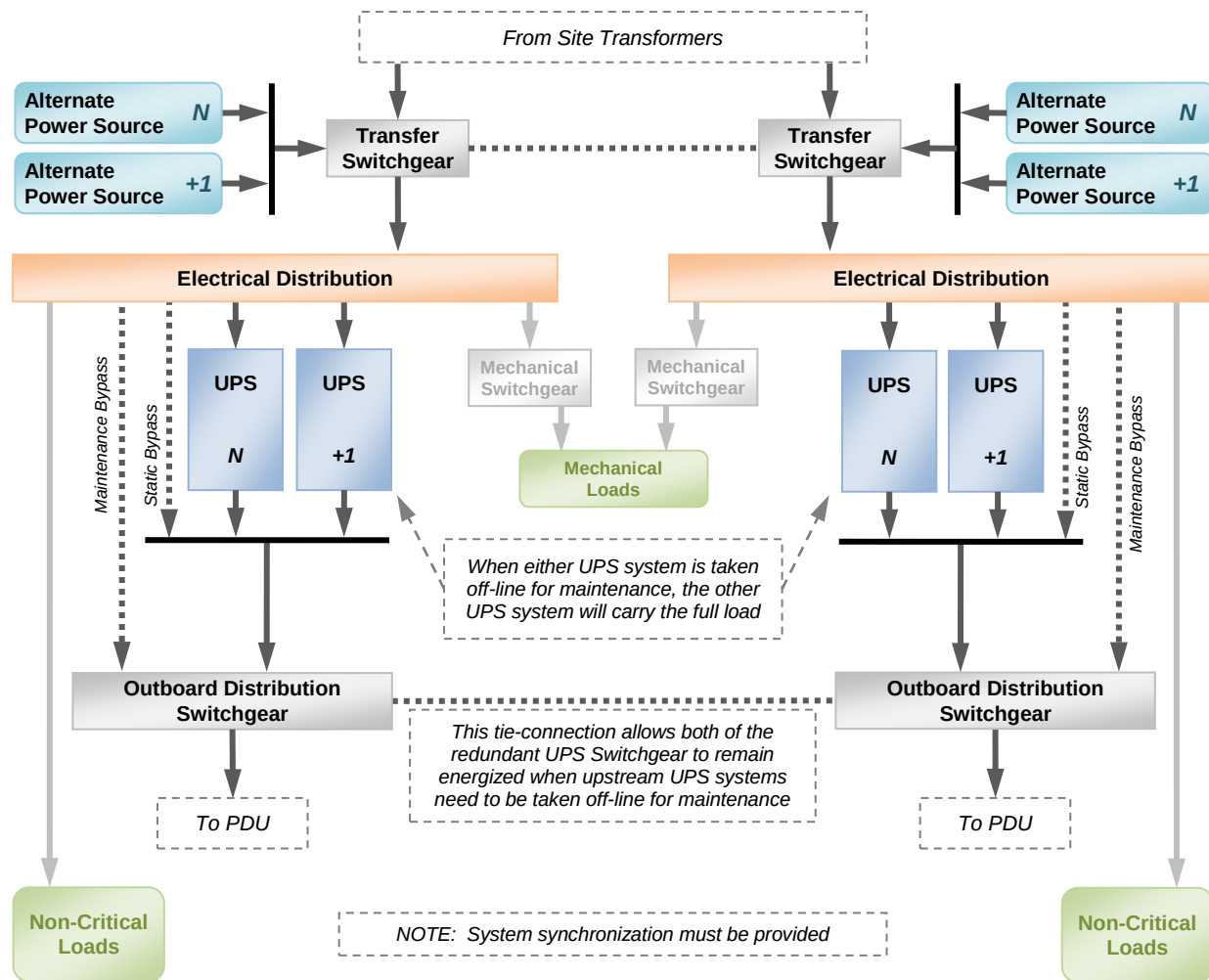


Figure 9-21
An Example of an Approach to UPS Output Switchboard Load Management

Transformers are frequently rated to K-9, but they may also be as high as K-13 to K-20. K-factor rated transformers are larger, more expensive, and less efficient than non-K-rated transformers, thereby increasing both capital and operating expenses, so they should be deployed judiciously. For Class F3 and Class F4 facilities where the transformer seldom operates at greater than 40% of its rated load, K-factor rated transformers may not be necessary as harmonics can be tolerated up to a certain level.

For existing loads it is possible to measure the harmonic content to determine how much, if any, harmonic content must be addressed. For greenfield (new) installations where the load is unknown, it would be advisable to specify the permissible level of harmonic distortion when purchasing the ITE power supplies or other loads, and to operate fans and variable speed drives (VFDs) on separate circuits where feasible.

The PDU may possess the following attributes:

- It may be a stand-alone system or may be coupled with a static switch for the management of single- or poly-corded ITE loads.
- It may have single input or dual input depending on the UPS system topology.
- It may have a harmonic-tolerant (or K-rated) transformer.
- It may have a low inrush transformer to prevent unintended upstream circuit breaker trip.

See Table 9-10 for transformer wirings and output voltages commonly used in data centers.

Table 9-10 Transformer Wirings and Output Voltages Commonly Used in Data Centers

Wiring	3-phase 3-wire ^{1,2}		3 phase 4 wire ³	Autotransformer
				
Output voltages	100V or 200V		400V and 230V 208V and 120V 200V and 115V	400V and 230V 208V 3 phase 4 wire

NOTE 1: These symbols are from IEC 60617

NOTE 2: 3-wire configuration with no neutral wire is popular in some locations to reduce the number of conductors, using delta-open delta transformers to step down to 100V.

NOTE 3: In general, delta configuration reduces harmonic content, but it has difficulty creating grounded neutral.

NOTE 4: There exists options for 6 or 7 wire outputs to provide dual output voltages at a ratio other than 1.732:1 such as 210V/105V_{AC}.

Considerations for selecting a PDU include:

- It should have larger-than-standard wiring gutters for easy circuiting.
- It should have a base plate tall enough for the ready connection of conduit for underfloor cabling applications.
- It should be located where thermographic testing can observe all critical connections, circuit breakers, and transformer cores while operating.
- Consider efficiency ratings at the expected operating loads pursuant to local energy guidelines. Specify no load and loaded losses at 25%, 50%, 75%, 90%, and 100% loads.

PDUs can be grouped together with other PDUs from alternate UPS power output sources such as the A and B systems collocated for matched circuit impedance and direct wiring. However, for higher Classes, it may be desirable to maintain physical separation of all elements in the critical power path as much as possible.

In the case where the UPSs are in a “catcher” configuration, it is possible to achieve concurrent maintainability of the UPSs without using an STS by using an overlap switch at the PDU source to switch between normal and standby UPS, which are both synchronous. This enables uninterrupted transfer of the PDU load between normal and standby UPS modules, improving both availability and operational flexibility.

For a PDU pair using a static switch, the load connections for single-corded and dual-corded devices might appear as illustrated in Figure 9-22. Within a cabinet or rack, an automatic transfer switch (either separate or integrated within a power strip) should be installed for all single-corded loads.

See Sections 9.3.15, 9.7.2, and 9.10 for further information.

9.3.12 Automatic Static Transfer Switches

9.3.12.1 Introduction

Automatic static transfer switches (ASTS) are used in power systems where subcycle, high-speed source switching outside of the ITE is desirable. The operation of ASTSs is similar to that of mechanical ATSS in that the ASTS automatically transfers on loss of preferred source or retransfer on loss of alternative source when preferred source has returned. A majority of ITE comes either single- or dual-corded with some newer systems IT devices requiring multiple-corded loads (some IT devices require 3, 4, 5, or more cords). When this occurs, the ASTS allows for a multiplication of the UPS power distribution paths without the multiplication of the UPS plants.

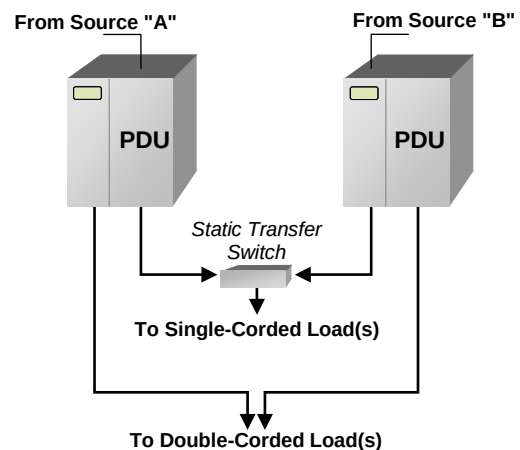


Figure 9-22
PDU Configuration: Single-Corded and Poly-Corded Devices

Other loads vital to the data center's operation include temperature control and building monitoring systems, operation or control room video and control systems, security systems, and single-corded IT systems. At the Class F0, F1, and F2 levels where the UPS power distribution and circuiting systems are single path, static switches are not typically utilized.

9.3.12.2 Recommendations

Since ASTSs represent a single point of failure (because they, like the loads they support, are single output systems), their use needs to be balanced with the overall reliability and failure mode analysis for the critical power distribution system. The ASTS can provide reliable recovery for an unexpected input source loss, but by its nature, it is a complex system that will cause the loss all of the downstream loads if it fails.

Features of the ASTS might include:

- Solid state transfer systems (e.g., silicon control rectifier [SCR]) instead of mechanical contacts seen in ATSSs.
- Dual-input and bypass-able for all loads—some ASTSs have been specified and built as three input systems, but these are typically custom units.
- Rack-mounted or floor-mounted options.
- Control systems that allow for transfer control within a few phase angle degrees.
- Fault-tolerant internal controls and wiring systems if needed.
- Mated to PDUs for numerous transfer and distribution options.

See Figure 9-23 for examples of transformer and distribution system configurations utilizing an ASTS.

See Sections 9.3.15, 9.7.2, and 9.10 for additional details on emergency power off, monitoring, and marking (respectively) as they apply to ASTS.

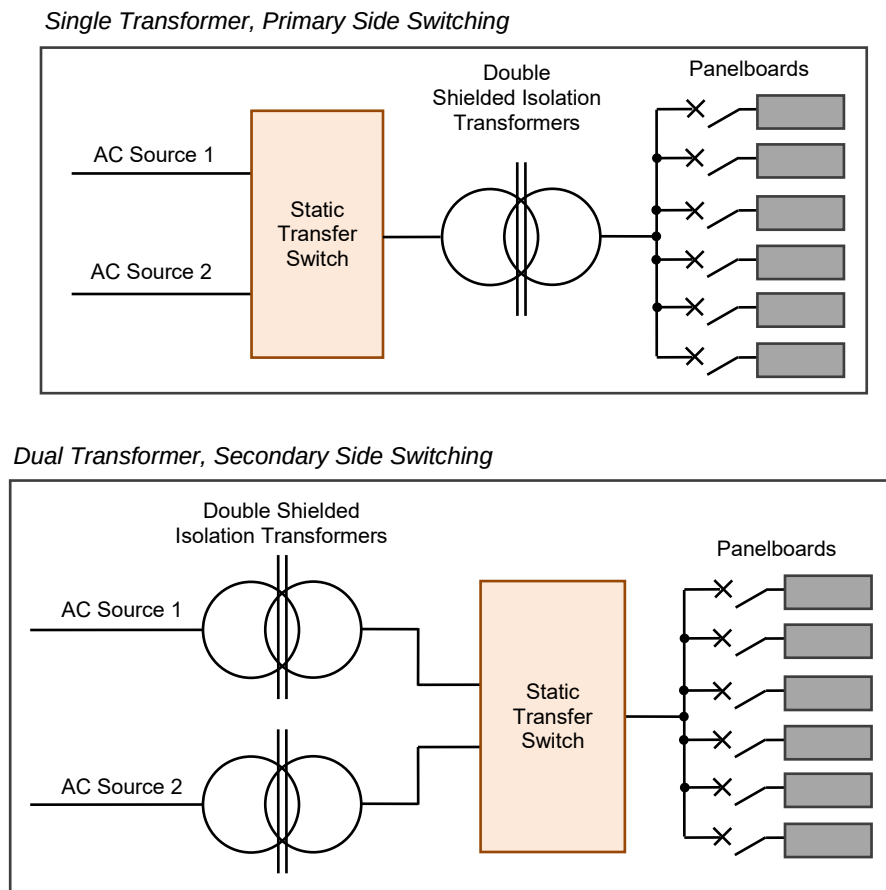


Figure 9-23
Automatic Static Transfer Switches

9.3.13 Direct Current (DC) Power Systems

9.3.13.1 Introduction

DC power systems that serve critical loads are common in two forms:

- The primary power source for access provider and carrier equipment
- As an alternative to AC power in computer rooms because of energy efficiency, design simplification, and ease of paralleling alternative energy sources

DC power distribution systems function within the data center in the same way as the AC systems providing power to a variety of loads. However, DC-based systems can offer additional features that can be attractive to data center designers and operators. It is also possible to mix DC and AC systems in hybrid configurations, for example, providing DC to critical loads and AC to mechanical loads.

DC power system operating voltages are affected by several factors such as:

- Battery technology (e.g., lead-acid varieties, nickel-cadmium, nickel-metal-hydride, lithium-ion varieties, sodium varieties, flow varieties)
- Rectifier output regulation in maintaining constant voltage under dynamic loads
- Voltage drops in DC power conductors—cable sizes and lengths
- Operating voltage limits of various connected loads
- Derating for environmental conditions such as altitude
- Availability of DC-rated components

9.3.13.2 General Requirements

All DC equipment shall be properly and clearly marked according to the applicable electrical or building codes and as required by the appropriate listing agency. DC equipment includes, but is not limited to:

- Cords
- Cables
- Raceways
- Busways
- Power connectors
- Junction boxes
- Batteries
- Generators
- Flywheels
- Circuit breakers
- PDUs
- Rectifiers
- DC-UPS

The design of all DC-powered ITE shall likewise comply with applicable sections of required electrical and building codes and shall be rated, listed, and marked for DC operation at the anticipated voltage range.

Electrical safety clearance rules are applicable to both AC and DC circuits. For DC circuits, the clearance requirements shall generally be the same as those for AC circuits having the same nominal voltage to ground.

9.3.13.3 General Recommendations

Direct current systems should meet the same requirements for availability, reliability, maintenance, and safety as AC power systems. While DC-based critical power systems are an emerging and potentially viable option for mission-critical environments, it is advisable at the present time to work closely with the designers, equipment providers, and electrical contractors who have experience in the direct current applications.

Designers, operators and others involved in DC systems should refer to the appropriate standards such as NFPA 70E, IEEE C2, and others.

NOTE: NFPA 70 E-2012 Article 130 defines DC approach boundaries and, hazard/risk category classifications for DC equipment; Article 340 outlines Safety-Related Work Practices: Power Electronic Equipment.

For installation and maintenance of batteries, IEEE 450 (vented lead-acid batteries), IEEE 1188 (valve-regulated lead-acid batteries), and IEEE 1106 (nickel-cadmium batteries) should be followed.

While DC-based critical power systems are an emerging and potentially viable option for the mission-critical environment, insufficient data exists to offer design guidance in this standard.

Applying DC power system telecommunications utility practices to the nonregulated environment of a data center requires additional considerations. Design considerations should include, but are not limited to:

- Per ATIS 0600336, the highest DC voltage covered by the telephone/telecommunications/ITE industry is 160 V_{DC}. The utilization of higher DC voltages (such as 240 V_{DC} or 380 V_{DC}) is essentially new territory and will require some additional safety and performance investigation. However, established principles are not expected to change.
- Overcurrent protection devices (OCPD) and disconnect devices for DC power systems will need further investigation for higher voltage DC systems. AC-rated devices cannot automatically be used on a DC power system at the same rated voltage and current. The established 2:1 protection coordination scheme for DC fuses is not readily applicable since data centers typically utilize circuit breaker technology.
- Transients for other than 48 V_{DC} systems are not well described.
- Battery disconnect or other DC disconnect usage at voltages above 50 V_{DC} is not well established. Disconnects may or may not be required, depending upon local requirements. 2-pole or even 3-pole disconnects may be required, perhaps at multiple points within a system. Interrupting capacity and withstand ratings may need to be selectively coordinated.
- Conductor sizing regulations for DC are not well established; sizing per AC code requirements may be inappropriate for DC conductors.
- If the rectifier technology is switched mode power supply (SMPS), it may require use of electrical noise control via power line filters (possibly connected to the return or DC equipment ground conductor) and might create additional audible noise from cooling fans.
- Rectifier operation modes at the higher voltages, such as 380 V_{DC}, may need verification for AC input power factor correction, load sharing, paralleling, voltage sensing, and current limitation.
- The DC power distribution topology is historically bus or cabling. Further, there may also be a need for an underfloor topology. Distribution (such as rigid busbar) withstand under extreme fault current conditions (such as a direct short across the batteries [if batteries are used]) will likely vary considerably from that for a telecommunications 48 V_{DC} system.
- Voltage drop is a concern, especially if DC is run for distances longer than a few meters. Guidelines for calculating voltage drop can be found in IEEE 946.
- For metallic battery racks, determine the AHJ requirements for sizing the bonding conductor. 13.3 mm² (6 AWG), which is typically specified for telecommunications applications below 50 V_{DC}, may not be acceptable for higher voltages (e.g., 380 V_{DC}).
- Consult with the AHJ regarding limitations for the location of centralized DC power systems in the computer room.
- Determine the grounding methods required by the ITE. The 380 V_{DC} system might be operated as a positive grounded system (similar to the 48 V_{DC} telecommunications system) as a negative grounded system (similar to the 24 V_{DC} telecommunications system) or as an ungrounded system (similar to higher voltage UPS systems).

9.3.13.4 Voltage Ratings

9.3.13.4.1 Introduction

Direct current nomenclature differs somewhat from alternating current nomenclature in terms of range. In AC terminology, the “nominal voltage” is the voltage at which the ITE is expected to operate under conditions of normal operation. AC equipment has a tolerance range within which it can operate reliably (e.g., +10% / -15% of nominal).

In DC equipment, there is generally assumed to be a battery, so the DC voltage range is usually determined by the needs of the battery. In most cases, a battery is charged (and the ITE operates) at a constant “float voltage” for a high state of readiness. When a battery is required to discharge (i.e., upon loss of mains [utility] power), the voltage declines until it reaches a cut-off voltage. When the battery is recharged, a higher voltage is pumped through the cells until the battery reaches capacity at which time the charger drops the voltage back down to the “float voltage” level. In some cases, an even higher voltage may be applied to “equalize” the cells. The “nominal voltage” is a point somewhere around the middle of the range.

The connected DC load equipment is expected to operate within an entire band range of DC voltages. The industry speaks of “narrow range” and “wide range.” The efficiency of the ITE will vary, depending for which band it is designed. For example, a narrow range system could be 361-399 V_{DC} with nominal midpoint of 380 V_{DC}, whereas a wide range could be 294-380 V_{DC} with a nominal midpoint of 336 V_{DC}.

The industry has adopted the term “high voltage direct current (HVDC)” to distinguish it from the traditional telecom systems which operate below 50 V_{DC}. Data center voltages are generally identified at two voltage levels:

- 240V HVDC—the system provides 240 V_{DC} nominal voltage and 270 V_{DC} floating voltage
 - (nominal = 2 V_{DC} per battery cell x 120 cells)
 - (floating = 2.27 V_{DC} per battery x 120 cells)
- 380V HVDC—the system provides 336 V_{DC} nominal voltage and 380 V_{DC} floating voltage
 - (nominal = 2 V_{DC} per battery cell x 168 cells)
 - (floating = 2.27 V_{DC} per battery x 168 cells)

Thus, the existing HVDC systems should be categorized as:

- 240V wide-band HVDC system (240 V_{DC} nominal/270 V_{DC} float charge)
Primarily designed, deployed and operated in China by telcos and a few Internet companies.
- 380V wide-band HVDC system (336 V_{DC} nominal/380 V_{DC} float charge)
Adopted in North America, Europe, and Japan. Research laboratories, such as Lawrence-Berkeley National Laboratory, and experimental installations (e.g., Duke Energy, NTT) are based on this system.
- Under-400V narrow-band HVDC system
Incorporates all the narrow-band HVDC systems, which provides constant but adjustable output voltage under 400 V_{DC}, and complies with standard ETSI 300 132.

NOTE: By definition in the narrow-band system, there is no “float” voltage, because the DC voltage is regulated.

9.3.13.4.2 Additional Information

DC power distribution systems can be designed with the same topology as comparable AC systems. In the simplest implementation, the DC system can follow the same principles and tier structure as AC data centers. The only departure from the AC design is replacing the AC-based UPS with DC-based power systems and all the downstream AC equipment with the DC rated equipment such as switchgear, PDU, STS, and PSU. In a more sophisticated approach one can design a microgrid type of DC system, which can incorporate a variety of sources (DC and AC with their AC-to-DC conversion) and a variety of loads (DC loads such as DC PSU and DC telecom equipment, DC VFDs driving the HVAC motors for cooling systems as well as DC building lighting).

With regards to arc flash safety, NFPA 70E has provided guidance for arc flash hazards in AC systems for a number of years. In the 2012 version of the standard, guidance on arc flash hazards in DC systems was added.

One has to notice that the different standards define different voltage ranges for the DC systems (e.g., 0-250 V_{DC}, 250 V_{DC} – 600 V_{DC} or < 750 V_{DC} and > 750 V_{DC}). Although there is no consistency between the various standards on voltage ranges for a given voltage selected for a data center (such as 380 V_{DC}), one can easily extract the applicable sections of the other standards related to safety of such a system.

Renewable sources of energy and short term energy storage systems, such as photovoltaic (PV) arrays, fuel cells, microturbines, battery systems, ultracapacitors, and flywheels, are very compatible with the DC systems. With the increasing awareness of sustainability, these sources and energy storage technologies are finding their way into the data centers. Since many of these sources and storage systems are intrinsically DC based or utilize equipment that converts variable AC to DC and then to main frequency AC (50 or 60 Hz), it is only natural that they can be easily adapted to the DC distribution systems by eliminating the last DC to AC conversion. This can improve overall system reliability (fewer components), system efficiency, and control over dispatching energy throughout the entire DC network.

Moving forward, there is interest in using direct current at voltages as high as 600 V_{DC} although 380 V_{DC} nominal is emerging as a global standard (except in China where 240 V_{DC} is being widely deployed). The claimed advantage of DC power over AC power is that fewer power conversions result in higher efficiency and greater reliability although such claims have yet to be verified through wide adoption. Some of the initial attractiveness of DC power systems has been their natural efficiency. In recent years, AC power efficiency has reached or exceeded the levels of DC, making DC less relevant for efficiency. However, there are still persuasive arguments to be made regarding parts reduction and, thereby, improved reliability. Distributed versus centralized rectifier plants will affect the data center design both for power distribution and for grounding and bonding.

9.3.14 Computer Room Equipment Power Distribution

9.3.14.1 Introduction

Unlike upstream UPS plants and critical power distribution, distribution to the critical loads must be exactly mapped to the redundancy of those loads and the cord and circuit diversity that they require.

The upstream systems must be able to deliver the source diversity to the computer room circuiting under normal maintenance and failure modes of operation as prescribed in the Class performance descriptions.

At this level, the electrical system is downstream from the PDU or transformer level, and this system is typically operating at the utilization voltage level for the ITE or critical equipment. This distribution can be present in several forms such as busway or individual circuits.

For high-density loads, a given design may separate the panelboard branch circuit sections of the PDU into cabinets near the critical loads. This system may have either single or dual-inputs and is commonly known as a remote power panel (RPP). RPPs reduce installation labor and reduce the cable and circuit length to the load.

Distribution to the loads may be either overhead or underfloor. Underfloor power distribution is most commonly accomplished using liquidtight flexible metallic conduit, although in some jurisdictions, hard conduit may be required. IEEE 1100 recommends hard steel conduit with an AHJ-approved insulated grounding wire for added safety, performance, and EMI protection. Power distribution should be located under the cold aisle and telecommunications cabling located under the hot aisle to minimize air blockages. Overhead power distribution can frequently eliminate the cost of conduits (with the addition of cable tray or busway) and can have the added benefit of eliminating cables as a cause of underfloor air blockage. Overhead cabling, if used, should be planned to minimize blockage of airflow above the floor. Refer to Section 14.7 for considerations of overhead cable routing.

For future and high-density loads, traditional 20A circuits may not be sufficient for power strips in the IT cabinets, and in some installations, 3-phase power strips with appropriately sized circuit capacity may be required to support the load. To accommodate future power requirements, installation of three-phase cabling at an ampacity of up to 50 or 60 A or at utilization voltages of around 400 V_{AC} is recommended even if such power is not immediately required.

9.3.14.2 Load Connections

9.3.14.2.1 Requirements

Unused or abandoned cables not terminated at equipment or marked for future use shall be removed.

See Sections 9.3.15, 9.7.2, and 9.10 for additional details on emergency power off, monitoring, and marking (respectively) as they apply to load connections.

9.3.14.2.2 Recommendations

Load connection best practices for facilities in the United States are listed below:

- Twist-lock receptacles and plugs for all underfloor or overhead receptacles should be provided. Receptacles on the power strip within a cabinet or rack do not require locking-type receptacles. Some systems use a plug-in busway system installed adjacent to the loads or cabinets. The busway's design should allow new load taps to be installed while the bus is energized without creating any arcing or transients.
- Locking receptacles should be used for connecting the input cords of the power strips and for larger ITE. For in-rack loads using straight-blade cords, anti-pullout tie downs should be used where cords plug into the power strips.

<List continues on next page>

- Power distribution cables originating from different source PDUs, RPPs, electrical phases, taps off the same PDU, or electrical panels should be clearly identified as to their source, phase, and load capacity. If permitted or required by the AHJ, cables from different sources may have different color jackets and connectors.
- Branch circuit overload protection devices should be de-rated by a design factor of 20% (e.g., be at least 25% larger than their connected ITE load) to ensure that circuits are not operating at the edge of their circuit breaker trip rating.
- For equipment and systems that require power feeds from more than one power source to provide availability (typically Class F3 or Class F4), the power cords should be split across two of the cabinet power strips. To provide availability for single-corded equipment and for equipment that utilizes multiple cords but is not power feed-fault tolerant, these items should be plugged into a rack-mounted power strip or receptacle fed by a larger upstream, automatic static transfer switch (ASTS), or some other point-of-use ASTS.
- Equipment with three power cords should have one of the three plugs on a rack-mounted power strip or receptacle fed by a static transfer switch or point-of-use switch. The other two plugs should be plugged into receptacles supported by different PDUs. These other two receptacles should not be on static transfer switches.
- Power cords should be mechanically connected at the point of entry to the rack or piece of ITE. This may be accomplished via the ITE manufacturer's cable tie downs, hook-and-eye straps, cable ties, or similar attachment that allow for the secure attachment of the power cable to the enclosure and would prevent the accidental disconnection or damage of cable. Provide slack loop, as appropriate, in the tie down to allow for some cable movement.
- UPS sources should be paired or grouped together and represented by individual panels or remote power panels for ease and clarity.
- Plugs and rack-mounted power strips should be located where thermographic testing can observe all critical connections and overcurrent protection devices while operating.
- Cable management should be used.
- Disruption to future operations should be minimized by locating distribution equipment to permit expansion and servicing with minimal disruption.
- All power receptacles and junction boxes should be labeled with the PDU/RPP/panel number and circuit breaker number. Each PDU/RPP/panel circuit breaker should be labeled with the name of the cabinet or rack, or the grid coordinates of the equipment that it supports.
- All power receptacles and junction boxes installed under an access floor system should be attached to the access floor or the structural floor per manufacturer's recommendations when required by the AHJ. Receptacles and junction boxes should be mounted on channel to keep raceways and equipment above the sub floor. This attachment may be made mechanically via concrete anchors, brackets attached to the access floor pedestals, or even industrial hook-and-loop NRTL-listed fasteners, which make an excellent, dust-free alternative to drilling in an anchor or adhesives. Additionally, boxes and other electrical devices should be mounted at least 25 mm (1 in) above the sub floor to prevent water intrusion in the event of a leak.
- Every computer room, entrance room, access provider room, and service provider room circuit should be labeled at the receptacle with the PDU or panelboard identifier and circuit breaker number.
- Receptacles on UPS power should be color coded, have a color-coded label, or have a colored dot to indicate the specific upstream UPS power source.
- Supply circuits and interconnecting cables identified for future use should be marked with a tag of sufficient durability to withstand the environment involved.

9.3.14.3 Load Management

9.3.14.3.1 Introduction

Data center load management deals with the physical connection of critical loads to the critical power system in a manner consistent with the normal, failure, and maintenance modes of operation. At this level, it is assumed that the ITE load's internal power supplies will switch between the input sources independent of the critical power system's response to a failure. Knowing this, the data center or critical environment circuiting must agree with the response of the systems serving them. This is known as circuit mapping, and the same thinking that applies to all other parts of the critical power system applies here.

9.3.14.3.2 Requirements

Once equipment has been selected, continuous duty and design safety factors must be prudently applied to the critical power system. Safety factors are explained in more detail in Section 9.5.2. The maximum power required for a given critical power topology is then applied to the combined duty cycles and safety factors, resulting in the practical loading of the system. This practical loading accounts for all normal, failure and maintenance modes of operation of the critical power system.

This calculation varies depending on the Class and UPS topology. Most importantly, a facility operator needs to understand how this factor is applied at the PDU and critical power branch panelboard level in their facility so that they can readily and most efficiently use the critical power they have available.

The formula for rating a critical power system is:

$$\text{System kVA} \times \text{continuous duty factor (if not rated for 100\% duty)} \times \text{design safety factor} \times \text{system power factor} = \text{usable kW of critical power} \quad (9-1)$$

The power factor is the ratio of the real power (kW) used to do the work and the apparent power (kVA) used to supply the circuit. This difference can come from a phase delay between the current and the voltage, harmonics, or distorted current waveforms. An ideal power factor is equal to 1, and anything lower means that the electrical infrastructure needs to be oversized to supply the load. Furthermore, although this difference of power is not actually consumed by the equipment, it is possible for the service provider to invoice it or apply penalties according to the power factor value. Therefore, the objective is to maintain the power factor closest possible to 1. Some methods that can be used are:

- Use equipment that is less inductive. The ITE is constantly improving to be closer to 1.
- Use a UPS with power factor 1.
- Use a power factor correction device, also called capacitor bank, located between the UPS and the substation. It can be fixed or automatically adjusting and can include monitoring.

9.3.14.3.3 Recommendations

Power distribution design should have sufficient flexibility and scalability to allow the load to increase or decrease in any cabinet, rack, or ITE zone within acceptable design limits. If the total anticipated data processing load has a capacity criteria of N, the multipliers for each subsystem within the electrical distribution system (as shown in Table 9-11) will provide sufficient capacity to meet normal equipment layout diversity and scalability, thereby preventing the creation of areas where the power available is insufficient to support the connected load.

Redundancy reduces the load on any given device, with a corresponding impact on efficiency and operating cost. Equipment selection should consider operating cost at the anticipated load levels in addition to capital costs and footprint.

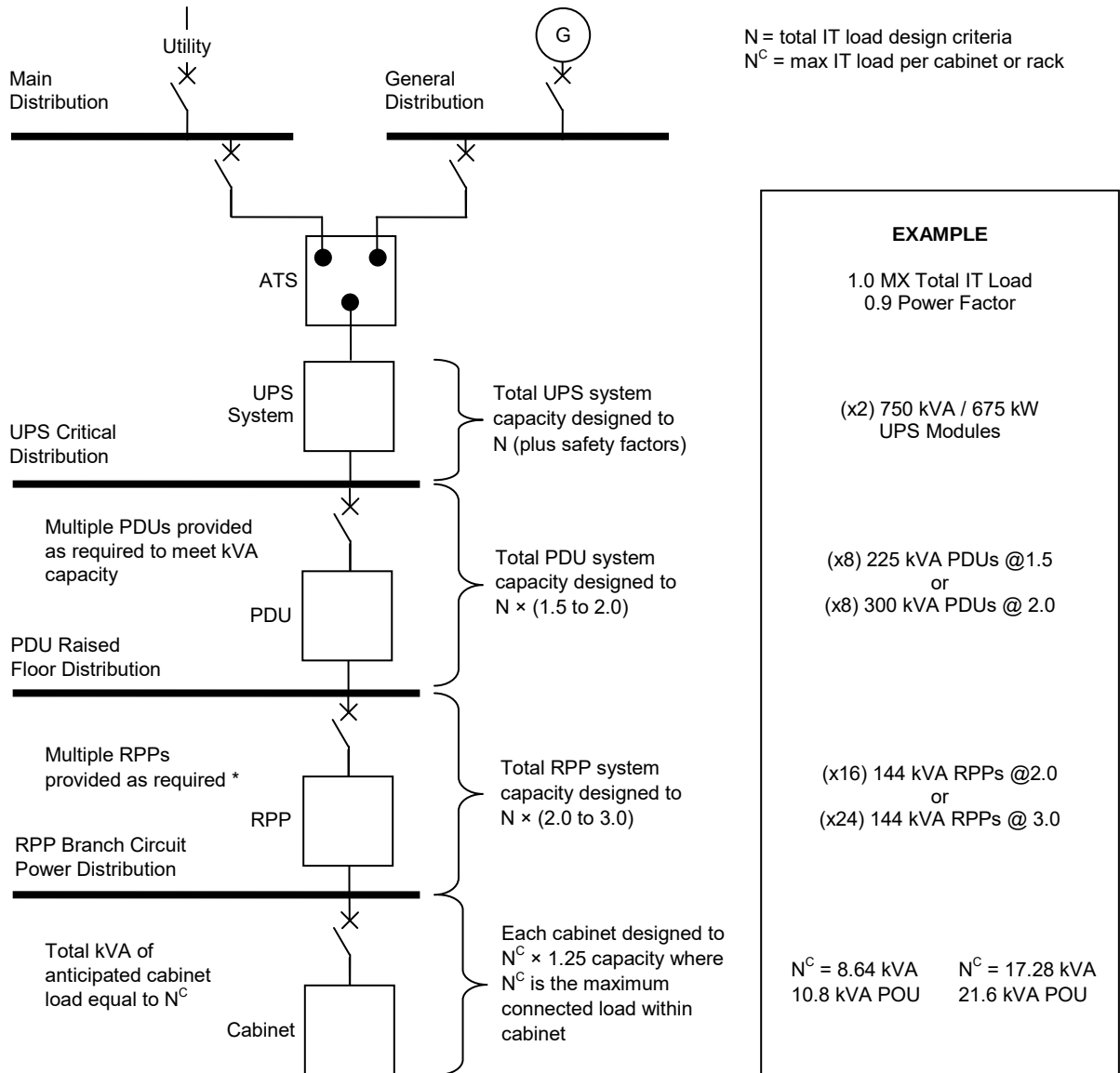
Figure 9-24 shows a single path electrical system to represent system capacities at various stages of the electrical distribution system.

Table 9-11 Multipliers for Electrical Distribution System Components

<i>Distribution System Component</i>	<i>Multiplier (N = ITE load design criteria without safety factors)</i>
UPS and UPS critical distribution	N (plus safety factors)
Power Distribution Units (PDU)	N × 1.5 to 2.0
Remote power panels (RPP) or overhead power plug busway	N × 2.0 to 3.0
Power strips (POU)	N ^C × 1.25

Electrical Block Diagram

Diagram shows single path electrical system to represent system capacities at various stages in the electrical distribution system



* Quantity of RPPs is not only dependent on the total IT load "N" but also the:

- Layout of the IT equipment, coordinate with number of cabinet rows or equipment zones.
- Capacity of RPPs shall be sized to accommodate total N^C of all IT hardware within rows or zone covered by RPP.
- Number of pole positions required to support quantity of circuits required for IT hardware within rows or zone covered by RPP, pole positions (min.) = $2 \times$ circuits required.

Figure 9-24
System Capacities at Various Stages of the Electrical Distribution System

9.3.14.4 Circuiting Protocols

9.3.14.4.1 Introduction

One of the most effective methods for preventing system overloading is the management of ITE loads in the critical environment. The management of the ITE loads must be considered for both the normal mode of operation and for maintenance modes of operation. While it may be difficult to overload a PDU or UPS system, improper cord management may lead to a lack of adequate circuit diversity for the ITE loads. As a result, the failure mode response of the ITE loads may be compromised.

To graphically represent how Class characteristics are manifested in the data center's circuiting environment, each system offers different options. For Figure 9-25 through Figure 9-31, each of the individual power circuits within the multi-system architectures are sized to support the ITE power demand.

9.3.14.4.2 Circuit Mapping

There is no redundancy in the critical power system's pathways until Class F3 is realized. The model for the Class F0 and F1 critical power systems would be as shown in Figure 9-25.

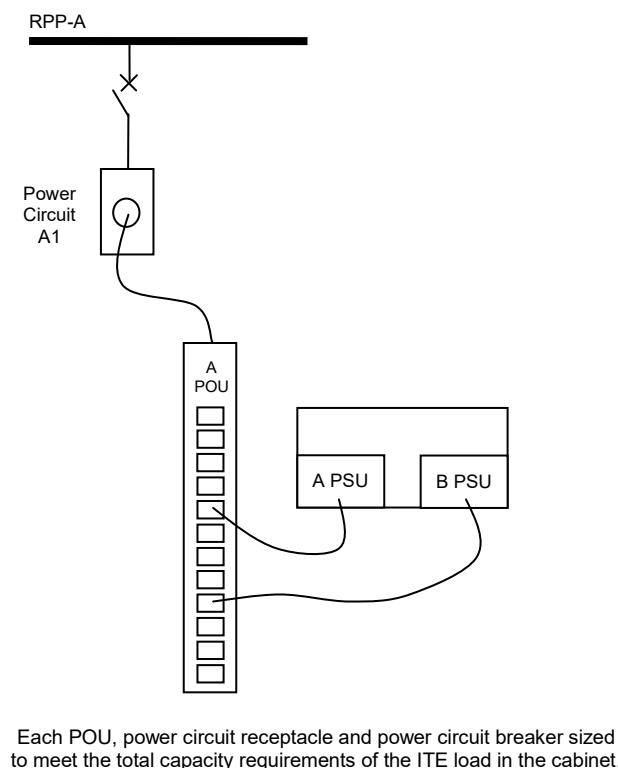
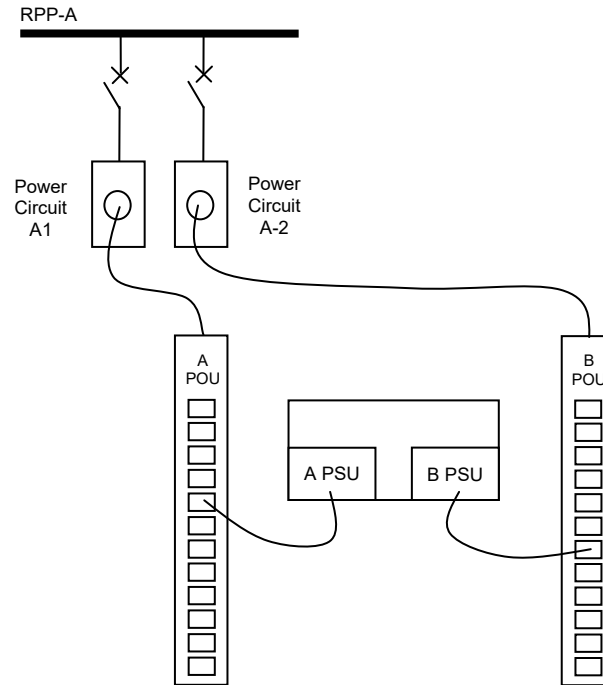


Figure 9-25
Class F0 and F1 Circuit Mapping

For Class F2, although there is no redundancy in the critical power backup generation, UPS system, or system's pathways, it is recommended that multiple power strips (POU) be provided within each ITE cabinet. Each POU would be fed from separate dedicated upstream breakers. The power circuits for a POU pair within a cabinet will often be fed from a common upstream RPP or PDU for a Class F2 electrical distribution. The model for the Class F2 critical power systems would be as shown in Figure 9-26.



Each POU, power circuit receptacle and power circuit breaker sized to meet the total capacity requirements of the ITE load in the cabinet.

Figure 9-26
Class F2 Circuit Mapping

With the diversity in the critical power paths in the Class F3 and Class F4 systems, the complexity of the circuiting systems in the data center increases. The key point to the higher Classes is that the circuits that serve the ITE must be derived from separate sources, and the power distribution downstream from the UPS must be concurrently maintainable for Class F3 and Fault Tolerant for Class F4.

There is a misconception within the data center industry that redundant power supplies have been implemented within critical server, storage, and network devices to enable concurrent maintainability of the power distribution supporting the devices. This was not the initial intent for redundant power supplies. The redundant power supplies have been provided because the power source and the power supplies represent a component or system that has higher failure rates, and in order for the IT hardware manufacturers to ensure high availability of the systems, redundant power supplies were implemented. It may be acceptable to a data center owner to use the redundant power supplies to assist in facilitating concurrent maintainability; however, the risks with this approach must be understood by the IT team.

When power on one leg of dual power supplies is interrupted and then returns after some period of time, the failure rate of power supplies could be as high as 5%. Empirical data suggests that the failure could go undetected until power on the surviving leg is interrupted and the ITE load is lost, but the probability of such ITE failure is less than 1%; ITE on other circuits will be unaffected.

If the data center server architecture is one where there are hundreds or thousands of servers for both capacity and redundancy supporting a single function and the loss of up to 5% at any time would not be considered business disruptive, then using the dual power supplies within the ITE to support concurrent maintainability of the power distribution would be a reasonable approach. However, for data centers where a business critical application is supported by high availability IT hardware clustered pairs or where there is a single large frame server in the primary data center supporting a critical function, a failure rate of 5% can represent a significant risk. In this case, attention to providing multiple redundant power circuits from the RPP, in addition to providing closed-transition tie breakers between redundant UPS output distribution switchgear to support each ITE cabinet, is recommended for Class F3 and F4 data centers.

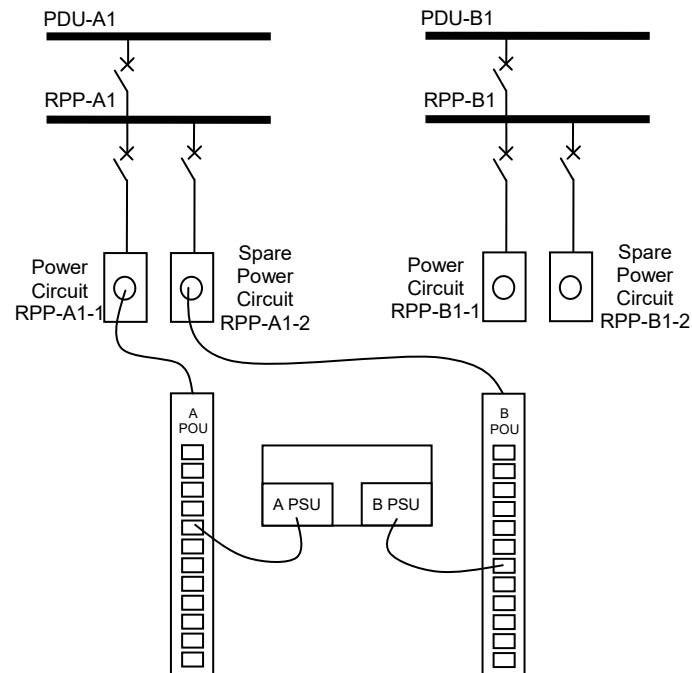
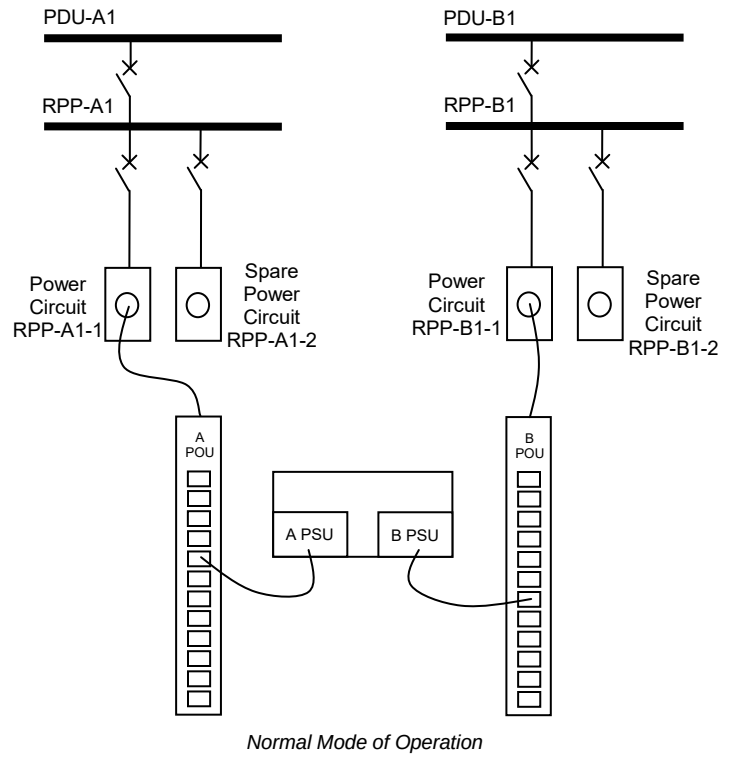
For Class F3, the power distribution between the UPS and the ITE shall be concurrently maintainable. Concurrent maintainability can be achieved through manual operational processes with multiple circuits or automated systems through the use of multiple static transfer switches. If there is significant coordination between the data center's facility and IT operations teams, then concurrent maintainability can also be achieved by moving the application from one virtual server to another. The critical application on the power circuit that requires maintenance can be moved to another virtual server within the data center whose physical server is connected to an alternate upstream PDU or RPP.

A method of providing concurrent maintainability through manual operational processes is to have each cabinet provided with two power circuits and receptacles from each of the redundant power paths. This would enable, for example if the "A" power path required maintenance, the operations team to manually disconnect the "A" POU within each cabinet and connect it to the spare "B" power path. It would likely be impractical to use this practice to maintain one side of the power distribution (where closed-transition tie breakers do not exist in the distribution downstream from the UPS) for a large data center, but it may be more applicable for mid- to small-size data centers or for maintenance of individual PDU or RPP within the computer room. The benefit this operational process offers is that if a power supply fails, then the high availability clustered pair should not be impacted (the clustered pairs should never be located within the same cabinet). The failed power supply can be replaced prior to proceeding with the remaining cabinets. If overhead power distribution buses with plug-in receptacle units are used instead of RPPs, the design is simplified. With an overhead power bus, there is no need to pull extra circuits; only spare plug-in receptacle units are required. If the "A" overhead power bus required maintenance, the spare plug-in receptacle unit would be installed in the "B" overhead power bus.

A method of providing concurrent maintainability through automated systems is to provide two POUs with an integrated STS within each cabinet. Each POU would be connected to both "A" and "B" power paths with one STS set to "A" as the primary source and the other set to "B" as the primary source. This method allows the facilities team to maintain either power path without the ITE seeing a disruption to either of the redundant power supplies.

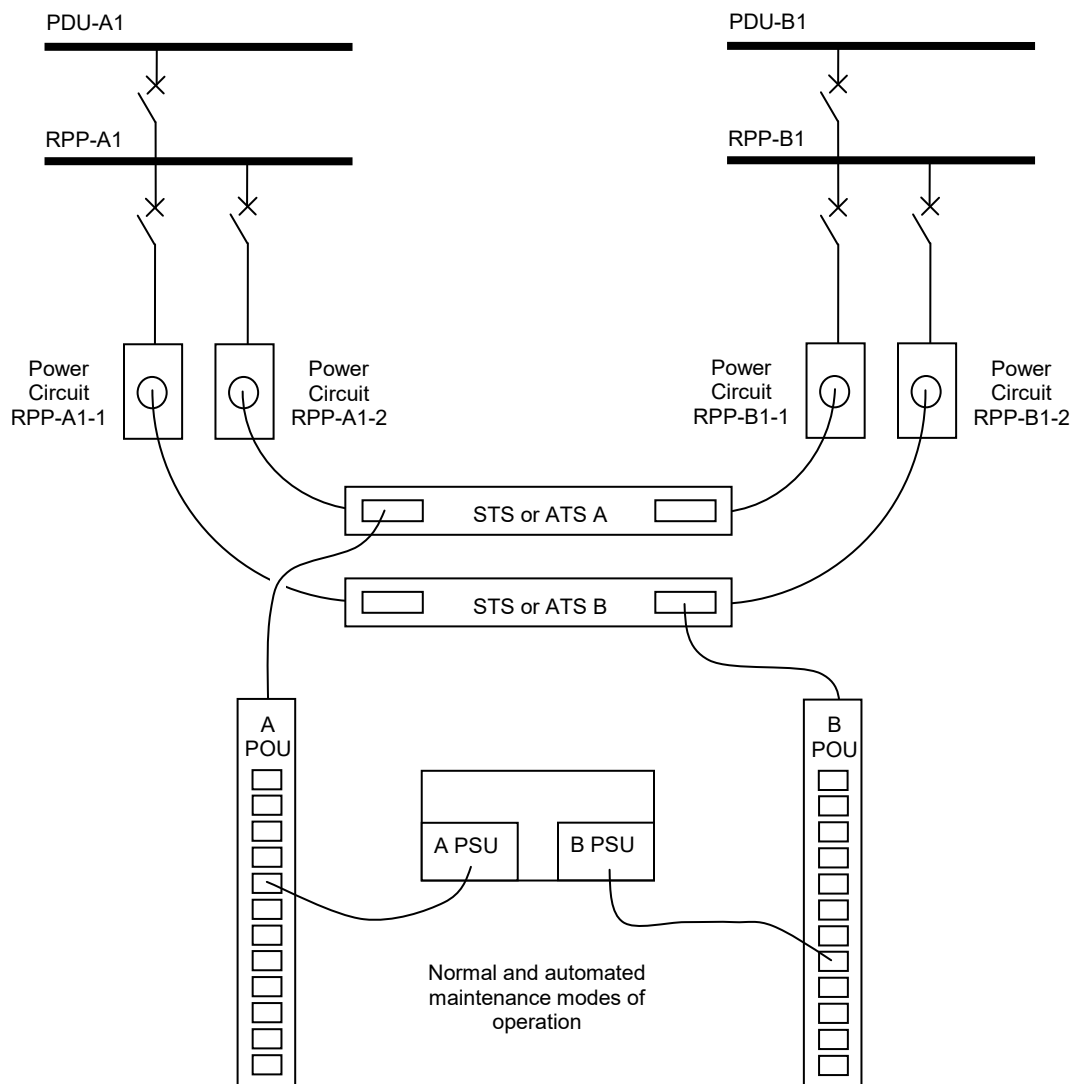
CAUTION: The MTBF data for the STS or ATS components should be provided by the manufacturer and analyzed by the designer prior to the use of rack mounted STS or ATS components in order to provide concurrent maintainability between the UPS outputs and the POU within the cabinet. Inadvertent and non-predictable failures of rack-mounted STS and ATS components have resulted in unplanned outages. When using this circuit mapping topology, it is recommended that the STS or ATS have a defined replacement cycle, which could be every 3 years or less depending on the MTBF.

Figure 9-27 shows a normal mode and manual operations maintenance mode of operation for circuiting a Class F3 critical power systems, whereas Figure 9-28 shows the circuiting for normal and automated operation maintenance modes.



Each POU, power circuit receptacle, and power circuit breaker sized to meet the total capacity requirements of the ITE load in the cabinet.

Figure 9-27
Class F3 Circuit Mapping (Manual Operations)



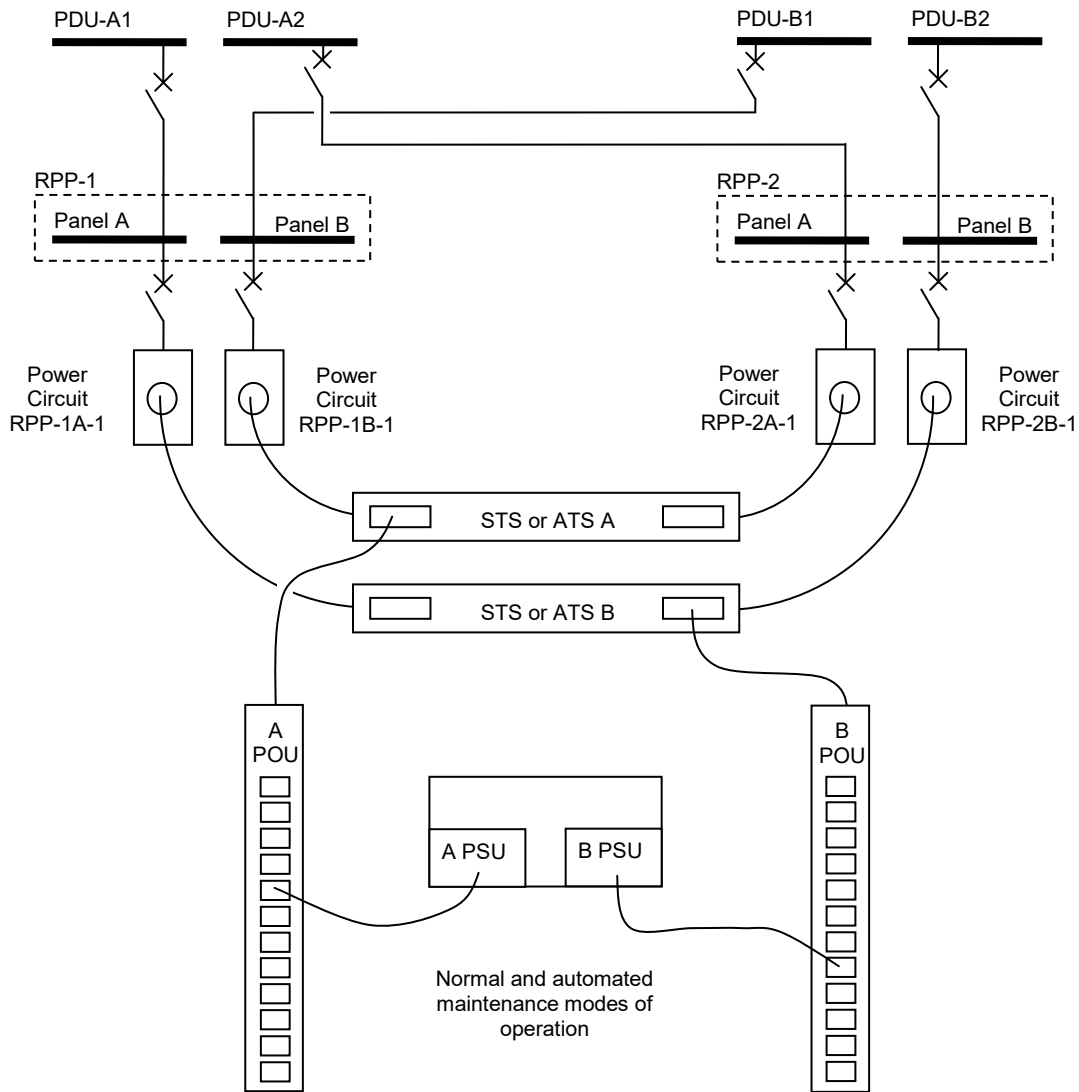
Each POU, STS, ATS, power circuit receptacle, and power circuit breaker sized to meet the total capacity requirements of the ITE load in the cabinet.
STS or ATS with transfer times below PSU tolerances.

Figure 9-28
Class F3 Circuit Mapping (Automated Operations)

For Class F4, it is not possible to achieve concurrent maintainability plus fault tolerance at the ITE level when the ITE contains dual power supplies (or any N+1 power supply configuration). Only if all the ITE is provided with N+2 power supplies, then the power distribution consists of an "A," "B," and "C" redundant power plants all sized to "N" and with power circuits from each power plant connected to the N+2 power supplies is concurrent maintainability and fault tolerance achievable for ITE. This type of ITE power supply configuration and power distribution topology has not typically been implemented. However, Class F4 fault tolerance capabilities can be provided for the power distribution up to the ITE cabinet, ensuring that power distribution component redundancy is provided even when either an "A" or "B" upstream component or system is off-line for maintenance.

CAUTION: The MTBF data for the STS or ATS components should be provided by the manufacturer and analyzed by the designer prior to the use of rack mounted STS or ATS components in order to provide concurrent maintainability and fault tolerance between the UPS outputs and the POU within the cabinet. Inadvertent and non-predictable failures of rack mounted STS and ATS components have resulted in unplanned outages. When using this circuit mapping topology, it is recommended that the STS or ATS have a defined replacement cycle, which could be every 3 years or less, depending on the MTBF.

Figure 9-29 shows a method for circuiting a Class F4 data center's critical power systems.



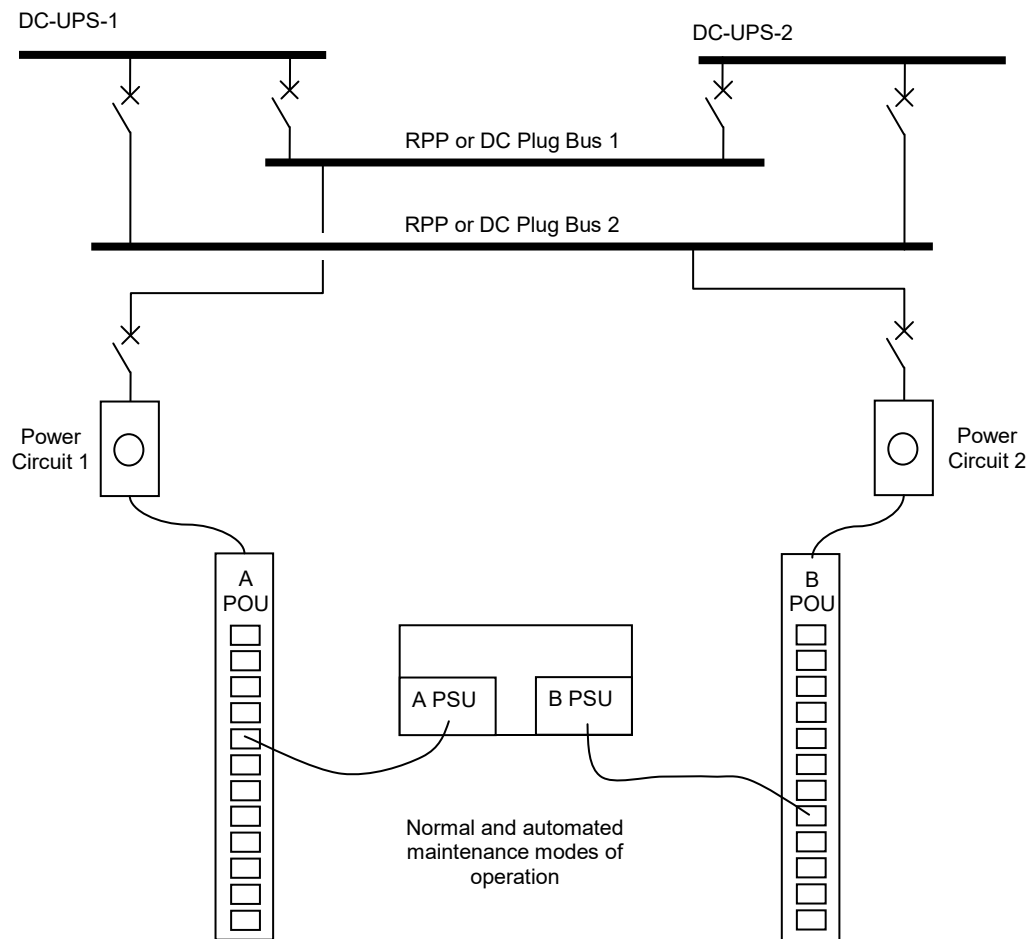
Each POU, STS, ATS, power circuit receptacle, and power circuit breaker sized to meet the total capacity requirements of the ITE load in the cabinet. STS or ATS with transfer times below PSU tolerances.

Figure 9-29
Class F4 Circuit Mapping

The figures showing Class F3 and F4 represent one method available to implement the required level of redundancy. PDU and RPP manufacturers have options that enable other means to achieve the required level of redundancy, ensuring concurrent maintainability to the cabinet for Class F3 or fault tolerance to the cabinet for Class F4.

The implementation of a 50 to 600 V_{DC} power distribution from the output of the UPS can significantly simplify the concurrent maintainability and fault tolerance of the power distribution and circuit mapping from the UPS to the ITE. A Class F3 or F4 electrical distribution would consist of redundant double-ended overhead bus with each bus connected to both the "A" and "B" UPS system. This would enable the maintenance of any PDU or power circuit between the UPS and the ITE while maintaining fault tolerance on the circuits supporting the ITE. This is a significant benefit that 50 to 600 V_{DC} computer room power distribution offers.

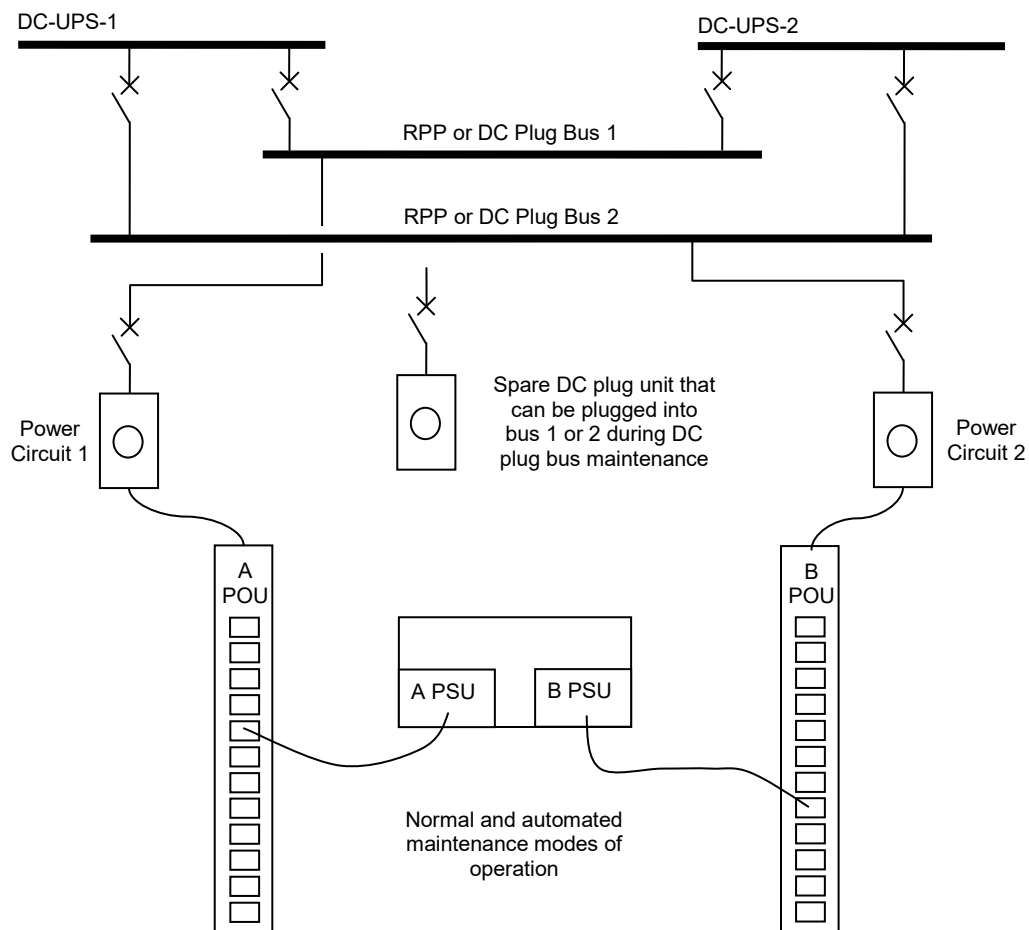
Figure 9-30 shows a method for circuiting a Class F3 50 to 600 V_{DC} critical power system.



Each POU, power circuit receptacle, and power circuit breaker sized to meet the total capacity requirements of the ITE load in the cabinet.

Figure 9-30
Class F3 50 to 600 V_{DC} Circuit Mapping

Figure 9-31 shows a method for circuiting a Class F4 50 to 600 V_{DC} critical power system.



Each POU, power circuit receptacle, and power circuit breaker sized to meet the total capacity requirements of the ITE load in the cabinet.

Figure 9-31
Class F4 50 to 600 V_{DC} Circuit Mapping

9.3.14.4.3 Power Cord Mapping

In addition to circuit mapping, it is important that the IT team understand how to implement power cord mapping based on the ITE being implemented. There are several power cord and redundant power supply configurations provided by ITE manufacturers, such as:

- 2 power supplies, 1 to 3 cords each power supply, N+1 power supply configuration
- 3 power supplies, 1 to 3 cords each power supply, 2 power supplies in 2N configuration plus 1 non-redundant power supply configuration
- 3 power supplies, 1 to 3 cords each power supply, N+1 power supply configuration
- 4 power supplies, 1 to 3 cords each power supply, N+1 power supply configuration
- 4 power supplies, 1 to 3 cords each power supply, 2N power supply configuration
- 5 power supplies, 1 to 3 cords each power supply, 4 power supplies in 2N configuration plus 1 non-redundant power supply configuration
- 5 power supplies, 1 to 3 cords each power supply, N+1 power supply configuration
- 7 power supplies, 1 to 3 cords each power supply, 6 power supplies in 2N configuration plus 1 non-redundant power supply configuration
- 7 power supplies, 1 to 3 cords each power supply, N+1 power supply configuration
- 9 power supplies, 1 to 3 cords each power supply, 8 power supplies in 2N configuration plus 1 non-redundant power supply configuration
- 9 power supplies, 1 to 3 cords each power supply, N+1 power supply configuration

It is critical to fully understand how the power connections of the ITE with 3 or more power supplies have been configured within the ITE. If the power supplies are configured in a 2N+1 configuration, it is vital that it is specifically known which power supply is the "+1" non-redundant power supply and that it is connected to an STS with dual inputs. If the power supplies are configured in an N+1 configuration, then any one of the power supplies can be connected to an STS with dual inputs.

When power supply units have multiple input power connections, it is also important that the IT designer fully understand how the inputs are configured within each PSU and how they respond to all the failure modes. Some ITE have options to reconfigure how the input cords and power supply units are configured. It may be that all input cords to a PSU should be grouped to the same upstream distribution, or it may be required that the inputs to each PSU must be connected to separate upstream distributions in order for all the power supply units to perform as intended. As indicated, the IT designer must fully understand how multiple PSU inputs and multiple PSUs are configured for each ITE, and the network or system administrators must also fully understand the configuration before any changes are implemented within the ITE to alter the configuration.

Improper implementation of the power cord or power supply configuration with the redundant upstream power distribution can result in unplanned downtime because of human error, even if both the ITE and the power distribution have been designed as Class F3 or F4 systems.

9.3.15 Emergency Power Off (EPO) Systems

9.3.15.1 Introduction

A means of disconnecting the electrical supply, more commonly known as emergency power off (EPO), while not mandated by standards, is sometimes required by local codes. An EPO presents the greatest risk to electrical system availability in the data center as an EPO activation can be intentional, caused by sabotage, or accidental, via physical contact, mechanical failure, and human error during maintenance (such as the manipulation of the EPO system's link to the fire suppression system).

Organization of an EPO system is illustrated in Figure 9-32.

9.3.15.2 Requirements

Local codes or insurance carriers often require EPO for the safety of firefighters, but they may allow some exceptions (such as when "orderly shutdown" is necessary). Additionally, some jurisdictions or codes may allow the EPO for the data center to be eliminated based on 24/7 occupancy of the facility or other considerations.

When a single point EPO for the data center or larger portion of the building is required and implemented, EPO shall be supervised on a 24/7 basis.

NOTE: A single point EPO is typically an individual project requirement, negotiated at the time of the project's development.

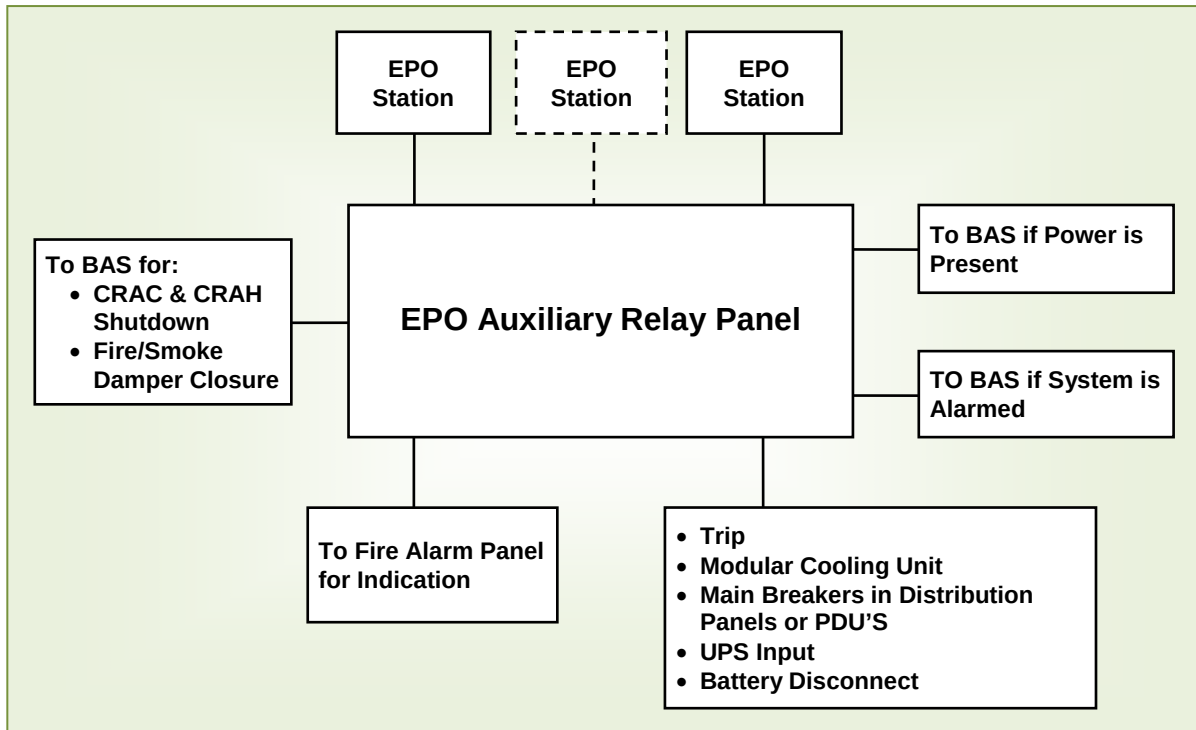


Figure 9-32
EPO System

9.3.15.3 Recommendations

When not required by code, the owner must carefully balance the needs of business continuity with personnel and building safety. When an EPO system is to be installed, a number of features can be included to make it more reliable, including:

- Delay to EPO activation after button push
- EPO override switch (keyed or non-keyed)
- EPO activation countdown timer
- Multiple stage systems

NOTE: EPO systems used in data centers should be three-state systems, with *off*, *test*, and *armed* modes of operations.

- EPO activation stations requiring multiple steps to operate them such as lift-hold-and-pull or the simultaneous operation of two buttons (when not prohibited by ADA and similar accessibility regulations).
- EPO activation stations that include a pre-alarm function, in which an audible and visual alarm is activated when the EPO button cover is lifted. This allows someone who has accidentally lifted a cover to know that there is a danger of activating the EPO system.
- EPO activations that allow a time delay, deactivation of a smaller areas of the data center, or centralized as part of an integrated electrical system.

NOTE: All of these techniques should be reviewed and approved by the local jurisdiction prior to implementation.

- Multiple disconnecting means to de-energize ITE and cooling equipment.

Decisions during installation can also affect reliability. Recommendations that should be followed include:

- Security cameras should be installed at EPO stations so that the face of the operator of the EPO can be clearly seen.
- EPO systems should be capable of being isolated from the fire alarm system so that when the fire alarm system is undergoing routine maintenance, the EPO is not accidentally activated.
- Do not specify or disconnect onboard, device-specific EPO buttons, if present, from UPS modules, UPS control cabinets, PDUs, static switches, and any other factory-installed EPO button. If the EPOs cannot be safely removed, the covers should be tied down to prevent accidental activation. These EPOs are not required if the room they reside in has one since they disconnect only one system or device as opposed to all of the room's equipment.
- Activation of an EPO circuit should also remove power to dedicated HVAC systems serving the room and should cause all required fire or smoke dampers to close unless a hazard/risk assessment determines, and the AHJ agrees, that cessation of air movement would pose a greater hazard than continuous ventilation.
- The disconnecting means may be permitted to be located in a secure area outside of the computer room, but this should be reviewed and approved by the local jurisdiction prior to implementation. Consideration should also be given to security risks if the EPO is not in a controlled access space.

Additionally, unless required by code or the local jurisdiction, EPO systems should not be installed:

- In UPS, chiller, and battery rooms
- Near light switches, phones, or any other device that is routinely touched

9.4 Mechanical Equipment Support

9.4.1 Introduction

Mechanical systems are as vital in the data center as the UPS systems that serve the ITE. The ability to have little or no interruption to the cooling services while maintaining temperature and humidity within a relatively narrow band is vital for the operation of most high-performance computing systems.

There have been several instances of thermal runaway where the heating of the data center could not be stunted in time to prevent the ITE from shutting down on a high temperature condition.

Some computing systems consume so much power and operate at such a high-power density (as viewed in W/m^2 , W/ft^2 , kW/cabinet , or kW/floor tile) that an interruption of cooling medium for only one minute can result in ITE shutting down. In this light, ITE requires uninterruptible power and nearly uninterruptible cooling.

There are two considerations for the electrical system when it supports the mechanical system—the restart of the cooling system (viewed in its entirety from the cooling plant to the ventilation systems) and the diversity of the electrical paths to the mechanical systems that matches the redundancy of the given mechanical components being served.

In traditional chiller plants (not including slaved DX units to a given air handler), the compressor restart time for the chiller can lead to thermal runaway in the data center during a power failure. This is caused by the ITE loads still operating under UPS power while the chillers, powered by the generator system, undergo a complete and protracted restart cycle following a power interruption.

Battery run time for UPS power systems that are supporting continuous cooling system needs to be coordinated with generator start and transfer time. Similarly, critical house and control systems need to consider any reboot or transfer time ahead of any mechanical equipment restarting.

While the restart control sequence is the purview of the mechanical designer, careful consideration needs to be paid to the following as soon as possible after an outage or retransfer from generator to normal power:

- Keeping chilled water moving in the system
- Keeping the ventilation systems operating
- Reestablishing the cooling plant (regardless of its design).

Generally speaking, a Class F4 mechanical system does not have the same topology as a Class F4 electrical system. Since the Class F4 mechanical system must meet the performance definitions defined for Class F4, the electrical system that supports the mechanical system must map to the normal, failure, and maintenance modes of operation for the mechanical system.

In many ways, the circuiting of the mechanical system is similar to circuiting of multicorded equipment loads in the computer rooms; multiple power paths must be used to ensure that a given piece of equipment survives a failure or is still on line during maintenance. Since Class F1 and Class F2 systems do not offer load supply redundancy, these Classes are not offered as solutions. The circuiting pathway for support of mechanical loads for a Class F3 facility is illustrated in Figure 9-33.

An example of a power distribution system supporting a Class F4 mechanical system is illustrated in Figure 9-34.

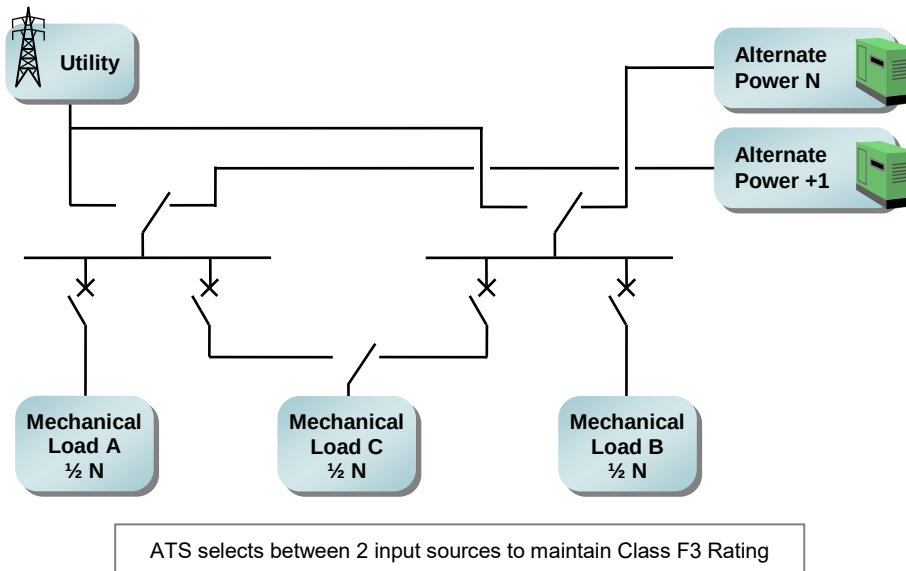


Figure 9-33
Sample Power Circuits For a Class F3 Mechanical System

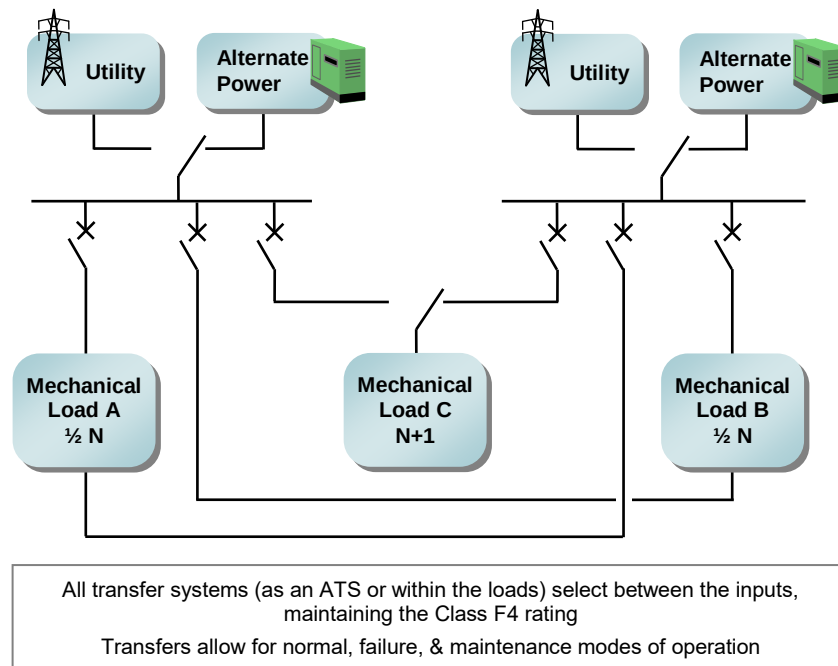


Figure 9-34
Sample Power Circuits For a Class F4 Mechanical System

9.4.2 Requirements

Temperature controls shall to be maintained during normal, maintenance and failure modes of operations. Where redundant temperature and cooling plant controls are provided, redundant circuits shall be provided commensurate with the diversity of the control system.

Cooling water pumps may require uninterrupted power. If the decision is made to support motors and pumps without interruption, they shall have a dedicated UPS suitable for the high inrush currents characteristic of such loads. Motors and pumps shall not share the same bus as ITE loads. (See Sections 9.1.6.5 and 9.1.6.6).

9.4.3 Recommendations

9.4.3.1 General Considerations

Having mechanical system controls on UPS power may provide faster cooling system restart times; however, this would need to be verified with the mechanical system vendor as it can be dependent on the manufacturer/model of system implemented. If the chiller is on unprotected power but the chiller controls are backed by UPS, upon loss of utility power, the chiller controls might lock out the chiller and remain in failed state. This constraint may not be factory or field adjustable.

Chiller and cooling systems often require substantial restart time, and these systems will take some time to return to full operation. This demands a few considerations:

- While the cooling systems are restarting, the UPS systems are still providing power to the load. Heat generated by the ITE loads operating on that UPS power will build in the data center spaces. Cooling plant restart times are often much longer than the time it may take for heat to rise sufficiently in the room to a point where ITE will shut down.
- The diversity of the electrical systems serving the mechanical plant must address maintenance and failure modes of operation to ensure that the cooling system restart time does not cause ITE loads to fail because of overheating.
- Substantial cooling water may exist in the cooling water piping system to help bridge the time or capacity gap for the cooling plant restart. In this light, keep cooling and condenser water pump running at all times.
- Some heat transfer may take place by simple ventilation, so keeping the fan system running can mitigate some of the heat rise in the room.
- For cooling plant restart, the following sequence of load additions to active service are recommended (all loads on alternate power):
 - Ventilation
 - Pumps
 - Chillers and cooling plant
- For higher power densities, there may be only a couple of minutes or dozens of seconds before the room heat “runs away” to a point where, even if cooling is restored, ITE may drop out or be damaged because of temperature. In this case, some of the mechanical support loads must be maintained on a 24/7 basis and may require UPS power in support of the IT mission. For high-density loads, some pumps and fans will require power from a dedicated UPS.
- Prudent design calls for the ability, first, to determine the rate of heat gain in the data center versus the restart time in failure or maintenance modes of operation and, second, to ensure that the electrical system offers sufficient capacity and diversity to prevent thermal run away in the facility.
- For fast chiller restart the chiller controls (but not the pumps) should be on UPS.

9.4.3.2 Chillers and Central Cooling Plant

Chiller and cooling plants have particular challenges to overcome for high-availability applications. Chillers, towers, and pumps tend to be single input type of machines with only a single feeder serving them. For open-circuit cooling systems utilizing cooling towers, chillers are sometimes paired with a cooling tower and pumps while in other cases, they work independently from each other. Whichever the case, the chiller input power must be coordinated with the mechanical plant’s chiller redundancy scheme. For some high-availability sites, heat exchangers and thermal storage systems are employed and must be considered in the circuiting of the cooling plant.

In all events, the pumping and other supporting systems, such as controls, must also be energized and maintained during normal, maintenance and failure modes of operation. Dual input to the chillers, cooling towers, and associated cooling equipment via automatic or manual transfer systems may be required.

For high-density computing environments, it is essential that some form of cooling be maintained during the generator start and mechanical cooling plant restart cycles. Some form of cooling equipment may have to be placed on UPS power in order to maintain temperature and humidity control in the data center.

9.4.3.3 Pumps

Pumping systems for data centers come in numerous forms—chilled water primary and secondary, condenser water, make up water, well water, and booster pumps. Most of these systems are configured as parallel redundant systems, operating on an $N + x$ basis (where x can be an integer or a percentage, depending upon the design criteria). Occasionally, a $2N$ system might be seen as well. Pumping systems typically operate much like paralleled generators or UPS modules might, sometimes equally sharing the load and sometimes not, depending on the drive and control configuration. Therefore, each pump for a given system needs to be powered independently of its partners. The circuit mapping also needs to follow the Class requirements and maintenance and failure modes for the equipment.

For high-density computing environments, it is essential that water flow be maintained, possibly requiring that some water flow systems be placed on dedicated UPS power.

9.4.3.4 Air Handling Systems

Air handling systems typically possess a higher degree of diversity than any other mechanical load in the data center. For example, 10 air handlers might be required for the load, and 13 are installed. This can be due to air distribution, the designer's preference, or the room's physical organization or dimensions. Serving that from two or three mechanical load buses poses a challenge without the use of manual or automatic transfer systems for individual or groups of air handlers. Similar to chillers and pumps, the air handler diversity and the $N + x$ basis (where x can be an integer factor or a percentage factor depending upon the design criteria) must be known. Then the electrical system circuiting should be overlaid to support them.

For high-density computing environments, it is essential that air circulation be maintained, possibly requiring that some air handling systems be placed on UPS power.

9.4.3.5 Humidification

Humidification can occur either locally or centrally in a data center, depending on the mechanical designer's technique. If the humidity control is local to the air handler, the power for the humidity system may be integral to the air handler. Note that humidification and dehumidification can be very energy intensive, which means that each unit having its own control can be very wasteful. Additionally, there is the potential for units to "fight" each other (i.e., one unit is adding humidity which triggers another unit to reduce humidity), which is extremely wasteful. Thus, current best practice is to have a more centralized control of humidity either at a room, module, or entire data center level. The air handler's circuiting will accommodate it pursuant to the Class' requirements. If the humidification is not powered by the air handler, a separate circuit for the humidifier is needed and the same set of circuiting requirements for the given Class. The same can be said for humidification or dehumidification systems that are independent of the air handlers that are mounted either in the data center itself or in the air supply ductwork.

9.5 Uninterruptible Power Supply (UPS) Systems

9.5.1 Introduction

NOTE: UPS systems are also discussed in Section 9.3.9 as part of the distribution system.

Using an analogy in which the electrical distribution system can be considered the arteries of the critical power system, the UPS systems are the heart—the nexus of power conversion and continuity. While there are several methods and designs for achieving a topology that will meet a given Class goal, the sizing and considerations of the UPS power plant itself has several common issues. This section will address the varying technologies, design applications, and other considerations for the UPS plant. These include:

- Sizing and application
- Technology
- Paralleling and controls
- Batteries and stored energy systems.

Appropriate selection of the UPS topology depends on the criticality of the applications supported by the data center. It is acknowledged that every business demands different levels of criticality and that the topology chosen has substantial impact on cost, space, complexity of operation, cost of operation, and expected lifespan.

9.5.2 Sizing and Application

9.5.2.1 Application

UPS and critical power system applications are focused on delivering quality power, whether originating from an electric utility or from internal energy storage, on an assured, 24/7 basis. While there are several issues related to loading and topology, the primary concern of UPS system design for Class F3 and F4 systems is the maintenance of critical power services while accommodating known failures or allowing for safe and logical preventive maintenance. There are several points to consider when selecting equipment or employing UPS systems and critical power components into a cohesive critical power system.

Similarly, system bypasses, whether they be static or external/maintenance, must offer a safe and clear method for rolling load on and off the UPS module or system. System designs should be arranged so that a failure in a single module or system is not allowed to propagate to adjacent or paralleled systems. Failure compartmentalization should also be used for other portions of the critical power system.

The main design and application considerations for UPS and critical power systems are:

- Automatic, single-step response to a failure
- Failures limited to the system that failed
- UPS power plant maps correctly to the critical power distribution system
- Stored energy system able to carry the critical load during all input power failures

9.5.2.1.1 Automatic, Single-Step Response to a Failure

System failures should be automatically corrected without risking the load. Failure response should allow the UPS system to settle into a steady state as expeditiously as possible. The response to a fault may transfer the load from the UPS module or system to another UPS system or to an unconditioned bypass source. Regardless, the UPS system has its highest chance of maintaining the critical power load's continuity with a single transfer or operation, also known as the "one step save." If the UPS system requires several steps to arrive at a revised steady state, it may fail in the transition process, resulting in a critical power load loss.

Failures should be limited to the system or portion of the critical power chain that experienced the failure. For example, a failure of a single module in a multiple module, paralleled system should limit the failure to the module that failed. In the case of a distributed system, the interconnection of the systems should not allow a failure to cause a failure in the supporting systems. This only speaks for system changes of state and not the normal, customary, and predicated load transfer to the other UPS systems that are expected based on the Class or system constitution.

There is a word of caution for some of the UPS plant designs that seek to establish a "ring" bus to share redundancy for multiple UPS power plant outputs or in the distribution system. Power quality, especially switching transients, resonance, or "ringing," need to be carefully examined to ensure that the UPS waveform is not corrupted by the failure mode operation of any portion of the system.

9.5.2.1.2 UPS Power Plant Maps Correctly to the Critical Power Distribution System

There are several instances when the N count of the UPS systems may not agree with the N count of distinct critical power distribution channels downstream of the UPS plants. ITE loads are typically dual-corded with many systems being more-than-two-corded. This brings up the phenomenon where the UPS plants' pathways do not directly map to the number of pathways of the downstream power distribution system. An easy plant-to-distribution map is a 2N system with a PDU capacity matching the UPS system (not considering the idiosyncrasies of the individual PDU setups).

For distributed systems, the failure modes of the individual critical power circuits need to be mapped upstream to the PDUs, then the PDUs need to be mapped against the critical power distribution systems or switchboards, and then the critical power distribution switchboards need to be compared against the UPS plants to which they are connected. While this is a straight forward exercise for normal operations, the failure and maintenance modes of operations need to be examined for loading and change of state operations as well to ensure that the critical power is maintained at all times under all modes of operations.

9.5.2.1.3 Stored Energy System Able to Carry the Critical Load During All Input Power Failures

Since an alternate source of power is an integral part of the data center's design, a utility power failure should result in the generator starting and the facility being transferred to the generator or that alternate source of power. The ability to carry vital ITE loads and critical support loads during the power resumption on the generator or maintaining services during the retransfer from generator to utility is necessary for any data center design.

With the advent of the high-density computing environment, the maintenance of cooling systems and the room environment is as vital to maintaining the IT processes as the UPS systems' stored energy systems.

The stored energy systems for the UPS modules and systems will be discussed in detail in Section 9.5.5. Every UPS power system must have some form of stored energy to bridge the transfer to the alternate source of power and the retransfer to utility and normal operating conditions or for any situation where the input power falls outside of the system's tolerances. For single corded loads, subcycle static transfer switches may be employed where the ITE loads themselves do not offer redundancy. In many cases, the ITE loads themselves will arbitrate which power input is most appropriate for its use.

For certain computing environments, UPS power may be derived from batteries, flywheels, or another stored energy system that provides the ability for a power or cooling system to maintain or restart loads before an impact to the computing environment. In some cases, this might mean that the chilled water pumping systems or chiller water storage system must be on UPS power. In other cases, the ventilation system must be maintained on the UPS power system.

In any event, these collateral, nontechnology loads must be added to the ITE loads to arrive at the proper UPS plant size for the facility.

9.5.2.2 System Sizing

System sizing is linked to the Class, system design, and topology chosen by the designer. The UPS system design should be based on kilowatts (kW) with consideration given to kilovolt-amperes (kVA) and the resulting power factor. The system kW must consider derating factors such as:

- Altitude
- Run time at a given load level
- Operating temperature of the electrical room or the location of the systems and equipment

The critical power system sizing is based on fully meeting the critical power load with the fewest modules or pathways available during maintenance or failure modes of operation (fairly assuming that the normal mode of operation always has more systems or pathways than failure or maintenance modes of operation).

The UPS power system capacity is always determined at the output of the UPS system. PDU or transformer losses related to generating ITE utilization voltage are to be considered part of the ITE load and are not to be included in the power capacity calculations. This method considers all UPS module and system losses but it does not penalize critical power distribution systems that may not employ PDUs or transformers or any further voltage conversion below the UPS systems. When determining power density (rendered in W/area), the output kW rating of the UPS power system is to be utilized for the calculation.

9.5.2.2.1 Loading Levels

As for many power systems, there is a fine balance between an overloaded and an under loaded electrical system. While the issues of overloading are clear (e.g., heating, breaker tripping, and reduction of Class), under loading may lead to system instability or, for some older systems, an inability to operate.

While this is not a big issue for a single module system, this can be a huge issue for large-scale paralleled or distributed-redundant systems where load is being shared equally among several, equal components. Loading levels must be considered for normal, maintenance and failure modes of operation. The fact is that for higher Class rated systems, there are often many systems sharing a modest critical power load sometime during the lifespan of the facility.

Overloading factors are noted below in the next section, and it is recommended that a given UPS system be operated at no less than 20% and no more than the safety factor discussed below under normal, maintenance and failure modes of operation.

Critical power system loading is load growth versus the Class. For example, a Class F4 system, when it passes a certain loading level, may revert to a Class F3 level. This occurs because power modules that were formerly used for redundancy may now be required for capacity (i.e., to serve a larger critical power load).

9.5.2.2.2 Safety Factors

It is impractical to load any electrical system to its full capacity. While some manufacturers have purported or proven 100% system rating and a resulting 0% safety factor when weighed against the critical power load kW rating, best practice is to always apply a safety factor in system design. This addresses unanticipated load fluctuations, inrush currents, and code-required continuous-duty system ratings.

A load factor of 90% is recommended with a 95% maximum, leaving a design of 10% to 5% safety factor. This does not include the continuous-duty rating demanded by the applicable code (e.g., *NEC*). For most designs, the code-mandated safety factor required for continuous load could also be used as the design safety factor.

9.5.2.2.3 Maximum Critical Power Load

The UPS plant and systems must be designed to accommodate the maximum critical load that the facility is expected to require during its useful life. These loads include ITE loads, critical cooling systems, and other supporting systems. This maximum critical power load must be supported by the utility and alternate/generator power plants as well.

9.5.2.2.4 Scalability

Modular system architecture may allow for a phased installation of UPS components. The initial, interim, and final system configuration must anticipate the maximum capacity. The design must offer a system count that logically addresses system loads at any time during the system lifespan while offering an individual module size that is neither too large nor too small to achieve the Class specified for the system.

The key point in system sizing and application is that the system design and configuration must address both the normal mode as well as failure and maintenance modes of operation. The resulting system capacity must be sufficient to support the load that is present at any point in the system's life during all modes of operation.

9.5.3 Technologies

9.5.3.1 Technology Considerations

For UPS systems, several criteria must be met regardless of manufacturer, system organization, or type of UPS system technology being employed. UPS systems may consist of individual UPS modules, individual UPS systems, or a group of several paralleled modules. However, the recommendations for the performance of these systems regarding maintenance, failure and normal mode responses are similar:

- The UPS technology should compartmentalize failures so as not to allow failures to spread to other modules or systems.
- Each module should be provided with a means of individual isolation without affecting the integrity of operation, overall redundancy, or Class.
- Each system should be capable of both automatic and manually-initiated bypass and should be provided with external means to bypass the system to avoid interruption of power in the event of system failure or maintenance.
- Modules and systems should possess an ability to be isolated from the critical loads and inputs. This allows the module or system to be fully isolated from power and control input for safety, maintenance, or replacement of the UPS module or system.
- The UPS system always possesses some form of stored energy system using batteries, mechanical stored energy systems, such as flywheels, or clutch-based systems for momentary ride-through of the critical load.

9.5.3.2 UPS Operating Modes

IEC 62040-3 identifies 3 basic modes of UPS operation, listed in ascending order of reliability:

- Voltage and frequency dependent (VFD)

The UPS AC output voltage and frequency are identical to the input voltage and frequency from the AC source. This type of architecture is typical of a static "off-line" or "standby" UPS. During normal operation, the system is idle and the load is run directly from the primary (e.g., utility) power source. When an overvoltage, an undervoltage, or an outage occurs, the system detects the condition and switches to on-line (double conversion) operation. VFD systems are typically the most efficient and least expensive, but they must rely on the ITE loads' internal power supplies to keep operating long enough for the UPS to sense and respond to the outage. Most ITE power supply units (PSUs) have only about 10 ms of hold-up time.

<List continues on next page>

- Voltage independent (VI)

The UPS provides a stable output voltage to the load(s), but its frequency is identical to the input AC source. This type of architecture is typical of a rotary UPS with a synchronous motor generator, or a static standby UPS with some form of voltage regulation on the bypass line. This architecture may be attractive to applications in which the load PSUs can tolerate a wide range of frequency variation. Clock functions cannot be synchronized to frequency.

- Voltage/frequency independent (VFI)

The UPS is able to provide stable voltage and stable frequency to the connected loads independently of the input AC source. In static UPS systems, this is referred to as a “double conversion” or “on-line” UPS and has historically been the dominant UPS architecture in data centers.

Today’s UPS systems can have multiple modes of operation, thereby allowing the owner to determine which mode of operation is appropriate based upon considerations such as the criticality of the mission and the desired operating efficiency. These modes, which may be manually or automatically selected, can include (but are not limited to):

- Full on-line operation (VFI) —voltage and frequency are always regulated without any interruption
- Partial Standby operation (VI) —with some power conditioning such as transient suppression or voltage regulation
- Off-line operation (VFD) —voltage and frequency are regulated only after a brief interruption of power
- Automatic bypass operation (VFD) —load is transferred automatically to utility or secondary source because of detection of a fault condition
- Manual bypass operation (VFD) —load is transferred manually to utility or secondary source for service

Because of the desire for data centers to maximize their power utilization effectiveness (PUE) or efficiency, facility scale UPS systems can offer what is commonly referred to as “eco mode” operation, meaning that the UPS can gain one or two points of efficiency by operating in less than full VFI mode. This may be attractive for Class F1 or Class F2 operation or for Class F3 in which the primary side is in full VFI operation and the secondary side is in VI or VFD operation.

9.5.3.3 UPS System Types

9.5.3.3.1 Introduction

UPS systems use numerous technologies and configurations to support critical loads.

While the technology is important, designers fashion all forms of critical power systems from many types of UPS technologies, thereby meeting the needs of their clients and the attendant critical load. For this section, technology is less important than how that technology is employed to address the normal, maintenance and failure modes of operation.

- **9.5.3.3.2 Static UPS Systems**

A static UPS system uses transistors or other types of power electronics to convert incoming AC power to DC power, stores the DC power, and when the stored power is needed, a second power electronics string converts the DC power back to AC and is supplied.

NOTE: This process is known as double-conversion and is voltage and frequency independent. Some static UPS use the same fundamental AC output, but they use delta-conversion technology for the DC-AC conversion. This difference removes the independence of frequency.

DC power may be stored using traditional chemical batteries or inertial stored energy systems such as high- or low-speed flywheels, compressed air, or other technology.

There are two primary types of static UPS. The conventional type is a single unit with fixed power that can be connected in parallel to provide higher power or redundancy. The modular type is a chassis with control board(s) that can accept multiple power modules inside.

They key advantages of the conventional are:

- Generally larger capacity
- Fewer components, generally meaning lower mean-time-to-failure

The key advantages of the modular type are:

- Smaller modules allowing smaller granularity and optimized load
- Easier module replacement, sometimes hot-swap, allowing greatly improved mean-time-to-repair

Static UPS power modules offer two types of configurations when addressing magnetic isolation, transformer-type and transformer-less. Transformer-less UPS modules can offer better efficiency while on inverter in that the isolation or autotransformer losses are not present as there simply is no transformer present. AC and DC internal bus fault response, internal module power electronics design, downstream critical load fault isolation and system efficiency are some of the considerations when considering the UPS power module specification. There is a sufficient installed base of transformer-less UPS power modules to consider this design an accepted technology.

9.5.3.3.3 Rotary UPS Systems

In rotary UPS power modules, the input to output power conversion is mechanical and accomplished via a synchronous machine. They differ from static UPS power modules in that static modules convert power electrically. Some rotary modules do possess complimentary power electronics similar to static UPS systems, and the discriminating factor in this design is that the primary conversion from AC-AC power is via a rotating motor, not transistorized power electronics. The stored energy system attendant to a rotary UPS would be any and all of the technologies and system types prevalent in a static UPS module.

9.5.3.3.4 Hybrid UPS Systems

Hybrid UPS power systems combine three components:

- Backup power generation source, typically a diesel engine
- The component that reproduces the ITE critical power output waveform, either a rotating machine (rotary UPS) or static component (static UPS) that reproduces the waveform using solid state components
- A stored energy source, either a chemical energy storage device (batteries) or kinetic inertial storage device (flywheel)

A hybrid UPS combines any two or all three components into one packaged solution from a single vendor. The other traditional UPS systems are designed solutions that are field installed, combining the three components using solutions from two or more vendors. A majority of hybrid UPS power systems use kinetic stored energy systems, though designs may also use batteries.

Some hybrid systems may also include an electrically- or mechanically-coupled generator system. Mechanically-coupled systems share a common shaft between the alternator and the generator. The stored energy system would bridge the time between a power outage and the generator assuming the load. This ride-through component would be provided by a manufacturer-specific design. Electrically-coupled generators would not be mechanically-connected to the UPS power system, but they possess controls that are completely integrated to and included with the UPS and continuous power system.

There are three defining factors for a hybrid UPS power system:

- These systems are designed, manufactured and operated as a single system where rotary and static UPS systems are assembled and integrated in the field from the products of several manufacturers.
- Components may not be readily swapped or replaced with another OEM source.
- The control system is specific to the manufacturer and subsumes the power conversion, stored energy, and power generation systems into one, manufacturer-integrated system.

9.5.3.4 Direct Current UPS Systems

Direct current power systems eliminate the output power inverter to achieve improved efficiency and reliability. DC systems supply power to the critical load at voltages appropriate to the load requirements (for example 48 V_{DC}, 240 V_{DC}, or 380 V_{DC}). The output voltage will vary within the high and low voltage range of the batteries and is specific to the tolerance of the systems being supplied. System topologies can range from centralized DC power plants to point-of-use systems. Because there is no possibility of bypass, DC systems require redundancy to achieve the same or better availability of comparable AC systems.

9.5.4 Paralleling and Controls

Paralleling and controls should follow the rules set forth in Section 9.7, which calls for local operation and automatic response to failures. While bypasses may be rated for momentary duty for some UPS systems, Class F3 and Class F4 systems have a continuous-duty rated bypass. Controls should present a clear and concise message and exact system presentation to the operator, denoting the power flow, metering levels of all electrical values, summary functions, and alarms. This is traditionally done via some form of graphical user interface (GUI), each unique to the given system manufacturer.

For paralleled systems with a single control, all available power modules should share load equally under normal operating conditions and under failure and maintenance modes of operation. For physically paralleled systems where the outputs are connected directly and physically to a single collector bus, the controls are traditional and are built into the PLC or control logic of the UPS system's control cabinet.

The challenge resides in a virtually paralleled system such as the xN Distributed Redundant Class F4 system. In this case, there is no centralized load balancing and control like the system control cabinet of the physically paralleled system. For the xN system and those like it, the control system is actually the sequence of operations for the system. In summary, the virtually paralleled system's controls are based on how the individual UPS systems respond to external changes in the other systems.

9.5.5 Batteries and Stored Energy Systems

9.5.5.1 Introduction

Batteries, flywheels, thermal, compressed gas, and induction clutch systems are all examples of viable stored energy sources for UPS systems. The critical points are:

- A stored energy system must be appropriately matched and engineered to the UPS power system it serves.
- A stored energy system must carry the critical load until the input source is restored and the UPS system returns to its particular form of AC power input.

Although a generator or alternate source of power must be present to apply a Class F1 or greater classification, the stored energy system may vary in its capacity, known as the watt-hour rating. The watt-hour rating is related to the stored energy technology used and the amount of backup time required by the system's design.

9.5.5.2 Applications

9.5.5.2.1 Risk Analysis

A well-constructed risk analysis (see Appendix B) will be crucial in the determination of a data center Class, which, in turn, will drive decisions on specifications for an energy storage solution. The probability of power interruption factored against the criticality of the load will influence the type, duration, and investment in energy storage.

9.5.5.2.2 Common Versus Distributed Energy Storage Systems

While using a common energy storage system to serve several UPS modules can reduce the installation cost, this introduces a single point of failure and reduces overall reliability. Thus, a common energy storage system is strongly discouraged and should not be used for higher Classes.

For distributed energy storage, individual battery strings should be provided for each power module. Multiple battery strings may be provided for each power module for additional capacity or redundancy.

9.5.5.2.3 Runtime and Overall Capacity

If the only requirement was to ride through a transfer from one AC input source to another (e.g., between a generator and a utility), only a few seconds of stored energy would be required. However, one must weigh the possibility of failure or unavailability of the transfer mechanism or the alternate power source. For example, if the standby generator failed to start, would it be feasible for the stored energy source to support the loads until they could be gracefully shut down or to transfer data to a hot site? If so, one must calculate the time required to respond and accomplish the necessary activity.

Some mechanical and hybrid systems are quite effective at riding through the few seconds required to bring the alternate power source on line. For longer ride through times, the more common approach has been to use a chemical energy storage device such as a battery or a hybrid chemical/mechanical system. Some chemical technologies are comparatively unstable at the low end of watt-hour requirements, so the technology itself can dictate a longer backup time. For example, lead-acid batteries are rarely recommended to be sized for less than five minutes. As most chemical energy storage devices lose capacity as they age, one should size the battery ride-through time based on the nominal capacity at the predicted end-of-life. Other sizing considerations can include derating batteries and cables for extreme temperatures and DC voltage drop over cable runs between the battery and the UPS.

While a specific minimum backup time is not stated in this section, a system capacity of 5 minutes is a safe minimum rating for most applications. Some facilities, such as access provider central offices, primarily use DC power systems and have several hours of storage capacity. Attention should be paid to paralleled systems or redundant module systems where the battery strings of the “greater than N systems” offer greater run time than the sum of the rating of the individual modules. For example, a four module, N+1 paralleled UPS system with individual 15 minutes batteries can yield a battery backup time well above 15 minutes as long as all battery strings are connected (e.g., not taken out of service for preventive or remedial maintenance).

9.5.5.3 Choice of Stored Energy Technology

The choice of stored energy technology will significantly influence the design, construction, and operation of the data center. Most UPS systems can only work with one energy storage technology, so the energy storage decision can greatly influence the type of UPS system that is selected. The following paragraphs summarize a few of the factors that must be considered.

9.5.5.3.1 Physical, Regulatory, and Environmental Considerations

The following are considerations for the deployment of battery systems:

- Hazardous materials—does the solution include materials that could be hazardous to operators and technicians and under what conditions?
- Hazard class—does the solution create a condition that will require special construction and occupancy requirements (such as special room or container construction), and can it be collocated with other equipment?
- Hazardous conditions—what conditions can lead to heightened safety concerns (such as off-gassing during overcharge or destruction due to vibration)?
- Disposal and recycling requirements—does the solution require recycling or return to manufacturer at end-of-life and are recycling plants available?
- Space construction—does the solution require special room construction (e.g., fire resistance, restricted access); can it be installed inside or outside; how much space will it take up; what is the footprint; can the floor support the weight?
- Ventilation and exhaust—does the solution require special ventilation or air conditioning?
- Gas detectors—does the solution require gas detectors to prevent build-up of toxic or flammable gasses under any operating conditions; who is responsible for installation, maintenance and calibration?

NOTE: Hydrogen detectors are sometimes considered for lead-acid batteries, but because of a high false-positive alarm rate and frequent recalibration their use is discouraged.

- Spill containment—does the solution include hazardous liquids that would require containment in the event of a container breach?
- Safety equipment and materials—is special personnel protective equipment (PPE) required for personnel near the energy storage device; are eyewash stations required; is it necessary to keep chemicals in the space to render harmless any chemicals that might be released from the solutions; who can use them; what are the qualifications to become certified?
- Floor drains—does the solution require floor drains to redirect any hazardous liquid or fuel?
- Temperature and humidity controls—does the solution require a narrow temperature and humidity environment? What are the penalties for operating outside the thresholds?
- Fire protection—does the solution introduce unique fire protection requirements (such as water-reactive materials)?
- Code requirements—are there local code requirements (e.g., fire, mechanical, electrical) that impose special requirements?
- Audible noise and vibration—does the solution create noise or vibration that could be harmful or annoying to operators or occupants?

9.5.5.3.2 Performance Considerations

These are the performance considerations when selecting battery systems:

- Cycling ability—how many times can the solution be discharged and recharged before it must be replaced; what is the significance of shallow (short-duration) and deep (long-duration) discharges?
- Recharge characteristics—following a discharge, how long does it take to recover to full rated capacity; does the recharge affect other systems (such as draw high current or create excess heat)?
- Life expectancy—how long can the solution be expected to be used before it must be replaced under the expected operating conditions; what is the warranted life, and what is the depreciation rate?
- Maintainability—who can maintain the solution (e.g., can the owner perform routine and emergency maintenance, or does it require certified technicians); how often is remedial maintenance required; can the solution be monitored remotely?
- Demonstrated reliability—does the solution have a proven performance record?
- Availability—is the solution available from more than one supplier; are repair parts readily available?
- Lifecycle cost—over a defined life expectancy for a data center (e.g., 20 years), what will be the projected cost of installing, operating, maintaining, replacing, removing, and recycling the solution?

9.5.5.4 Chemical Energy Storage Options

9.5.5.4.1 Lead-acid Batteries

Although many stored energy technologies exist, the great majority of UPS systems rely on some form of batteries. Lead-acid batteries are unquestionably the most common energy storage solution, even though other batteries are available that can provide higher power density, lighter weight, or other benefits. They get the name because the active material of the positive electrode is lead dioxide; the active material of the negative electrode is lead; and the electrolyte is dilute sulfuric acid. Lead-acid batteries generally come in two types—vented and valve regulated—although there can be significant variations in materials, construction, and suitability for any given application.

A lead-acid battery is considered to have reached the end of its life when it cannot deliver more than 80% of its rated capacity. Other chemical battery technologies allow for adequate operation with lower capacities. Temperature affects the life span or capacity of a battery string (optimum is around 20 to 25 °C [68 to 77 °F]), with long-term excursions above or below the rated design temperature significantly affecting the battery string's capabilities. Generally, the life of a lead-acid battery is cut in half for every 8 to 10 °C (14 to 18 °F) rise in continuous operating temperature above rated optimal temperature. Lower operating temperatures will cause a lead-acid battery to deliver less than its rated watt-hour capacity and thus give reduced backup time but can have a positive effect on battery life. The opposite happens at high temperatures; backup time is increased, but life expectancy is decreased as temperatures rise.

It is also the nature of a lead-acid battery to take a large dip in voltage when it is first discharged, after which it recovers to or near its normal float voltage. This phenomenon is called *coup de fouet* and can cause some systems to shut down if the DC voltage drops below a threshold. For this reason, lead-acid batteries are rarely rated for operation below 1 to 5 minutes.

Lead-acid batteries should be recycled. Recycling centers are readily available in most countries.

A note of caution about AHJ requirements and code enforcement: some battery regulations are based on the volume of the electrolyte (which is mostly water) in a liquid-filled battery, while some others are based on the actual hazardous material (such as sulfuric acid in a lead-acid battery or potassium hydroxide in a nickel-cadmium battery). The electrolyte volume triggers various storage, installation, ventilation, and reporting requirements for the stationary battery system:

- Vented (flooded) lead-acid (VLA) batteries—so called because the byproducts of electrolysis, hydrogen and oxygen, continuously escape into the atmosphere through vents. VLA batteries are also called flooded because the plates are immersed in free-flowing liquid electrolyte. These types of batteries are further defined by the types of alloys used in their grids such as lead-calcium, lead-antimony, lead-tin, and many others. Because they continuously vent flammable gas, VLA batteries require dedicated rooms with spill containment, dedicated ventilation, and exhaust. VLA batteries require regular maintenance and water replenishment. Because they are liquid-filled, VLA batteries are always installed upright, usually on open racks, and require spill containment. Because of potential exposure to high energy and hazardous chemicals, they must be installed in spaces with controlled access.
- Valve-regulated lead-acid (VRLA) batteries—derive their name from valves that prevent gas from escaping except when internal pressure builds too high. VRLA batteries recombine hydrogen and oxygen back into water. Their electrolyte is immobilized, either by a gelling agent (gel), which is popular in Europe, or by absorbed glass mats, which is more common in North America and the rest of the world. Many VRLA batteries can be installed sideways and can be stacked, creating a greater power density. Because VRLA batteries take up less space, require less maintenance, require no spill containment, and are sealed under normal operating conditions, they are often preferred, despite a shorter life span (hence more frequent replacement and higher life cycle cost) compared to VLA batteries. Cabinet-mounted VRLA batteries are often used inside computer rooms.

9.5.5.4.2 Nickel-Cadmium (Ni-Cd) Batteries

Ni-Cd batteries are usually “flooded” batteries that vent gas in much the same way as lead-acid batteries do. The active material of the positive electrode is nickel oxyhydroxide, the active material of the negative electrode is cadmium, and the electrolyte is dilute potassium hydroxide.

Because they continuously vent flammable gas, Ni-Cd batteries require dedicated rooms with spill containment, dedicated ventilation, and exhaust. Ni-Cd batteries require regular maintenance and water replenishment. Note that the electrolyte of a Ni-Cd battery is highly alkaline, so safety precautions differ from lead-acid batteries.

Primarily because of their comparatively high price, Ni-Cd batteries are uncommon in UPS applications except where extremes of temperatures or frequent discharges are expected. Ni-Cd batteries are popular as starting batteries for generator systems.

Because they are liquid-filled, Ni-Cd batteries are always installed upright, usually on open racks, and require spill containment. Because of potential exposure to high energy and hazardous chemicals, they must be installed in spaces with controlled access.

Ni-Cd batteries should be recycled. Because of the cadmium content, recycling centers may not be readily available in all countries.

9.5.5.4.3 Monitoring

Like every component of the data center electrical system, the battery systems should be monitored. Most UPS modules have built-in, proprietary monitoring that indicates string voltage, run time, and other basic battery monitoring functions. Battery monitoring is required for Class F2 and higher. Monitoring is required for the individual modules, for paralleled systems, and the entire set of battery strings. However, UPS-based battery monitoring systems may not be capable of detecting individual battery cell failure, which can greatly affect runtime and reliability of an entire battery system.

For Class F3 and Class F4 systems with lead-acid batteries, strong consideration should be given to a battery monitoring system capable of recording and trending individual battery ohmic values. A stand-alone battery monitoring system, capable of monitoring the ohmic values of each individual battery cell or container as well as predicting and alarming an impending battery failure, provides much greater detail on the actual battery status. Such systems are most effective when comparing a data point against an established base line, which requires comprehensive record keeping and trend analysis. These systems are recommended for Class F3 and F4 systems. Systems capable of providing cell charge equalization and charge management are desirable for Class F3 and Class F4 systems.

9.5.5.4.4 Mechanical Energy Storage Options

- Flywheel—flywheels have been around for many years to ride through short duration sags or interruptions (subsecond to many seconds). Advances in composite materials have allowed some systems to achieve minutes of ride-through. However, price and complexity of controls have limited their widespread adoption. Flywheels are almost immune to heat, but they can be affected by seismic activity.
- Flywheel/battery hybrid—for some hybrid UPS systems, very specific systems are provided and coupled with a power conditioning system (typically a mechanically-isolated synchronous machine with a variety of input and output filtering) with a generator system and some form of bridging system that allows for an expedited generator start and load assumption. These clearly and fully satisfy the need for the stored energy system to carry the critical load until the failed utility input is replaced by the generator or some other planned input. In this case, the UPS is a systems-based solution that meets the requirements of the critical load.

Other variations allow the mechanical inertia to sustain conditioned power to the load for short duration (subsecond) disturbances, but they will switch to battery backup for longer power interruptions. The battery sustains the load until the primary or alternate source of AC input power is available or until all useful energy is removed from the battery.

- Induction coupling—This type of batteryless UPS marries a generator and a prime mover (usually a diesel engine) into a single system via an induction coupling system. The prime mover sits idle until the main input power is interrupted. An inner rotor of the induction coupling stores sufficient energy to bridge the prime mover start time. The generator provides electrical power to the load during an outage. In normal mode, the generator acts as dynamic filter and provides power factor correction.

9.5.5.4.5 Emerging Energy Storage Technology Options

The following technologies collectively represent less than 10% of the installed base at the time of publication, but they are expected to increase market share in the coming years:

- Stationary lithium ion batteries—Primarily known for their versatility, high-energy density, excellent cycling capabilities, and light weight in small, portable applications, lithium ion batteries are starting to penetrate the stationary battery market. There are many variations of lithium batteries with some performing better than others in high-rate UPS applications.
- Stationary lithium polymer batteries—These batteries are known for their flexibility in form factor and shape as well as their versatility, high-energy density, and light weight in small, portable applications. Lithium metal polymer batteries showed promise for high temperature environments, but because of quality control and safety reasons, they have been withdrawn from the market.
- Stationary nickel-metal hydride batteries—Although they are not as small and light as Li-Ion batteries, they still have many advantages over lead-acid batteries, specifically in size and weight, and appear to perform better than Li-Ion batteries in UPS applications, especially for applications with constantly changing loads.
- Supercapacitors—A supercapacitor or ultracapacitor is an electrochemical capacitor that has an unusually high-energy density when compared with common capacitors. They are of particular interest in UPS applications as a supplement to batteries. They are able to ride through thousands of short duration power sags or interruptions (subcycle to a few seconds) without forcing the UPS to exercise the battery and can be rapidly recharged. At the present time, supercapacitors are not seen as a practical replacement for most battery systems.
- Fuel cells—Fuel cells are gaining more interest as a replacement for standby and emergency generators because they are quiet and efficient, have no byproducts harmful to the environment, and can be put in places where a generator cannot. Because fuel cells cannot supply energy instantly upon demand, they still require a battery or supercapacitor system to bridge the time period required for the fuel cell to ramp up to full capacity.
- Compressed air storage (CAS)—CAS systems use compressed air as the energy storage medium. CAS systems have limited applications and have more mechanical components than many other energy storage technologies.

9.5.5.5 References

For full details on battery systems, the reader is directed to the IEEE standards, recommended practices, and guidelines as in listed in Table 9-12.

Table 9-12 Battery Standards Cross-Reference Table (IEEE Standard Number)

	<i>Lead-acid batteries</i>		<i>Nickel cadmium (Ni-Cd)</i>	
	<i>Vented (flooded)</i>	<i>VRLA</i>	<i>Normal use</i>	<i>Photovoltaic (PV)</i>
Selection/sizing	IEEE 485	IEEE 1189	IEEE 1115	IEEE 1013
Installation	IEEE 484	IEEE 1187	IEEE 1106	IEEE 1145
Maintenance/testing	IEEE 450	IEEE 1188	IEEE 1106	
	<i>UPS</i>	<i>Monitoring</i>	<i>Spill Control</i>	<i>Ventilation</i>
Special interest	IEEE 1184	IEEE 1491	IEEE 1578	IEEE 1635

9.6 Standby and Emergency Power Systems

9.6.1 Sizing and Application

9.6.1.1 Introduction

Standby power systems are intended to support the data center in the event of a loss of primary power lasting longer than the capacity of the UPS battery (e.g., utility outage lasting for hours or days). Interest in fuel cells and other sources of on-site generation is growing, but the penetration of such emerging technologies into the IT space is still only a small percentage. The overwhelming preference is for generator systems, usually diesel, but turbine and gasoline-powered systems are also in use, especially in smaller data centers. For purposes of this document, assume that the standby power source is a diesel generator system.

The generator plant is a site-controlled power system that offers a stable, reliable power supply during critical maintenance operations and in the absence of utility power. For some installations, a campus-based power plant or some other legitimate, alternate power source can satisfactorily substitute for a generator plant.

The rating of a generator or the entire generator system requires consideration of the harmonic content and power quality of the load itself as well as starting and transfer requirements of the IT, mechanical, and noncritical loads. When addressing starting current, the maximum droop typically seen is 15%. It is not suggested that this large a droop be allowed, as with voltage drops of this magnitude, running systems can drop out unexpectedly. Conversely, lightly loaded generators operate poorly, tend to wet-stack (the buildup of particulate on the fuel injection, valves and exhaust system because of lower operating temperatures of the engine) and eventually operate at a lower capacity.

For 50 Hz systems, generators operate at lower revolutions per minute than those found in the US with 60 Hz systems. Resultantly, 50 Hz generation systems have a lower kW step loading tolerances when compared to equivalent designs rendered in 60 Hz. Care needs to be exercised when loading 50 Hz generator systems as the same step loading considerations for 60 Hz systems cannot be accomplished in identical 50 Hz systems. 50 Hz voltage droops will be larger in amplitude and longer in duration to recover to steady state voltage under the same load condition of 60 Hz systems. For US-based 60 Hz designs being duplicated overseas, output kW ratings do not match the 50 Hz engine-generator systems. Verify output kW for the generator set, with air quality derating factors considered, before final system selection and sizing all 50 Hz designs.

9.6.1.2 Requirements

Generators supplying the entire load of a data center that is identified as an emergency system as defined in the AHJ electrical codes and in prevailing standards such as *NEC* Article 700 shall be equipped with separate ATSS. The emergency system loads shall be separated from the rest of the data center loads with their own ATSS.

Most jurisdictions have substantial planning and operating requirements for stationary generator plants. These requirements include noise abatement, pollution allowance and abatement, fuel storage, operating hour limitations, structural attachment, fire suppression, and operating permits. Check with the local jurisdiction during the planning phase of the data center project in order to ascertain the precise requirements for the undertaking and to determine who is responsible for reviewing and approving the installation.

9.6.1.3 Recommendations

The following conditions should be considered when sizing individual generators and when using paralleled systems:

- Transfer scheme—closed or open transition
- Standby, continuous, or prime engine run time duty
- Harmonic content of the load
- Allowable voltage sag or droop for the mechanical and lighting systems
- Generator system topology and unit count—how many units are required for the load, maintenance rotation, and redundancy
- Inrush and motor starting loads on the initial outage as well as when loads are being brought back on manually after maintenance
- Operating humidity and temperature, based on ASHRAE or local equivalent, extreme temperature for the area of operation
- Altitude of the site
- Engine derating required by pollution abatement systems
- Pollution abatement—air quality, location in relation to building ventilation
- Noise abatement
- Expected run time for the system
- Minimum and maximum load levels and the specification of standby, continuous, or prime-rated systems
- Coordination of reactors and high-resistance grounding with the remainder of the electrical system
- Coordination of UPS battery recharging loads

The following additional items should be considered when planning generators for data centers:

- Exhaust muffler
- Muffler drain
- Louvers and dampers
- Proximity to building air intakes
- Impact of operating noise on surroundings
- Emergency and safety equipment
- Frequency droop tolerance of UPS input

The generators should support all loads related to the data center process or ITE loads, cooling and ventilation as well as noncritical and building loads. For larger campuses where the data center is an important but not the largest tenant, the generator plant may be sized to accommodate other loads on the site requiring standby power.

For all Classes, the generator load is suggested as the entire load of the data center as well as any other loads required to support the data center, such as well pumps, security systems and other campus- or site-based systems. When data centers are installed in health care facilities, the data center load qualifies as an equipment branch load for the emergency power system. For Class 2 data centers, it is recommended to have an additional generator(s) or a generator tap box located on the building external wall to quickly connect a temporary generator to the electrical distribution.

When the application of a data center affects life safety, the generator and the downstream power distribution system will be given an “emergency” designation, in which its use can be dedicated to specific loads and not shared with other loads. Two systems might be required: one for standby operations and one for emergency operations. This may be accomplished with a separate life-safety branch that exclusively serves life-safety loads, while data center loads would be served by other systems under a single generator or generator system.

9.6.2 Starting Systems

9.6.2.1 Introduction

The most common generator problem is a failure to start. Larger generators tend to have multiple starters based on the size of the engine. However, having multiple starters does not provide additional redundancy; multiple starters only allows for a quicker engine start.

9.6.2.2 Recommendations

For data center applications where the restoration and continuity of power is vital, the site's generator(s) need to start, and assume the facility's load as quickly as possible. Depending on the AHJ, generators that support emergency loads may be required to restore power to critical loads within ten seconds or less.

Faster starting can be attained by numerous methods such as larger-than-standard starters, stronger/higher ampere-hour batteries, or redundant starting systems. In all instances, starting systems can be upgraded using marine-grade starting systems in lieu of standard commercial or industrial systems.

Like all batteries, the batteries onboard the generators do best at their rated temperature. Higher or lower temperatures will result in shorter battery life or lower cranking power. For high availability applications, battery systems can be combined using a best battery selector or auctioning bridge.

9.6.3 Fuel System

9.6.3.1 Introduction

Poor fuel quality is a leading cause of system interruption during extended generator runs. Poor fuel quality tends to clog injectors and filters, thereby strangling the fuel supply to the generator. Fuel quality is managed in three separate ways: fuel additives, fuel treatment, and fuel filters on the generators.

Bulk fuel storage can be compromised by water, microbes, or particulates that infiltrate the fuel tank under normal weather and operating conditions. Fuel additives and treatments can help mitigate this condition, but they do not offer a foolproof method of safeguarding the fuel supply.

Fuel treatment takes place in a separate fuel polishing system on the primary fuel supply lines to the generator(s). The polishing system removes the majority of the microbes and particulates and water from the fuel and takes the pressure off the generator-based fuel filters as the single point of fuel cleaning. Fuel polishing should allow the filters to be bypassed if they become clogged, reverting to the generators for the primary fuel filtering function. The fuel polisher should be able to be serviced while fuel is passing through the system on the bypass loop.

The final stage of fuel filtering is the onboard fuel filters on the generator itself.

9.6.3.2 Requirements

Single-stage spin-on-type fuel filters (100 micron or 30 micron) with individual valves for removal while the engine is operating are the minimum requirement for Class F1 and Class F2 facilities. Three-stage, spin-on-type fuel filters (100 micron, 30 micron, and 10 micron) with individual valves for removal while the engine is operating are required for Class F3 and Class F4 facilities.

In case of turbine or other non-diesel engine generators, follow the manufacturers' fuel filtering requirements rather than the requirements shown here.

Marine-grade systems are required for all installations for Class F3 and Class F4 facilities.

NOTE: Marine-grade systems have all consumable components (e.g., fuel filters) and servicing systems used in continuous-duty engines such as those found in marine engines. These consumable components or supporting systems are required to be replaced, refilled, or serviced while the engine is operating under load without risk to the operator or the mechanic servicing the engine or to the surrounding environment via spills.

9.6.3.3 Recommendations

Marine-grade systems are recommended for all installations. Fuel lines on the generators should be marine-grade, with all connection points to the chassis routed through insulated bushings.

For filters located upstream of day tanks or for filters used by generators in N+1 or greater redundancy, spin-on-type is recommended, but is not required.

Generators should each have their own day tank to allow for fuel cooling when the engine is consuming fuel at less than rated levels and to avoid having the fuel tank being a single point of failure. While it is sometimes not practical to divide the main bulk fuel storage tank into individual or partitioned tanks, this is highly desirable for Class F3 and Class F4 facilities.

The data center's fuel supplier should have a large reliable source of fuel that is available for delivery when needed, regardless of day or time. The supplier should be able to continue to supply the data center with fuel if there is an area disaster. Alternatively, the data center's fuel tanks need to have enough capacity to provide electricity during an extended power outage caused by an area disaster such as an earthquake, flood, or hurricane.

9.6.4 Fuel Tank and Piping

9.6.4.1 Recommendations

All fuel systems with bulk fuel storage should incorporate the following basic features:

- Leak detection and annunciation for both the tank and piping
- Remote monitoring of fuel level
- Physical protection for piping from main tank to building
- Fuel filtration or polishing
- Security at tank fill points (e.g., locking covers)
- Training of operators to understand fill equipment operation to prevent accidental entry of water in tanks (underground tanks only)

9.6.4.2 Additional Information

Fuel tanks may serve a single generator or be part of a multiple generator system. Installing multiple bulk storage tanks versus a single larger tank may not increase the reliability of a system as multiple tanks may add complexity. Site issues can significantly affect the number of tanks that can be installed, as some sites may only have room for a single tank where others may not be suitable for underground tanks because of ground water or flooding issues.

9.6.5 Exhaust System

9.6.5.1 Introduction

Exhaust systems are linked to two issues for the site: the pollution abatement system and sound abatement requirements. Silencers come in three types: residential, industrial, and critical grades. The silencers affect engine efficiency with quieter silencers affecting engine capacity. Sound abatement on the air intake and radiator exhaust system can also affect the airflow to the engine. The silencers are linked to the overall noise abatement plan for the site.

In addition to silencers, pollution abatement systems may be required by local and regional authorities. Pollution abatement addresses two forms of emissions—particulate emissions and NOx emissions. The engine specification itself will need to be coordinated with any low emission site. Also, scrubbers (devices to remove impurities) may be required on the exhaust.

The exhaust system is typically airtight with welded construction and flexible metal connections between the engine exhaust manifolds, the silencers, and abatement systems.

9.6.5.2 Recommendations

Exhaust piping that terminates horizontally is typically angle cut to prevent water infiltration while vertical piping is provided with a flapper or hat-style cap. Flapper or hat style caps can obstruct air flow and may not be allowed because of air emission restrictions. In areas with freezing temperatures, consider the possibility of the flapper freezing in the closed position and not allowing the engine to start.

9.6.6 Cooling System

9.6.6.1 Introduction

Cooling systems can be via skid-mounted radiators, remotely mounted radiators, or high-reliability central water systems. For higher reliability applications, cooling systems are typically automotive-type glycol/water-based fluid radiator systems with crank-driven cooling fans that are isolated to the individual machine.

9.6.6.2 Requirements

If centralized cooling for the engine blocks is being considered, the water delivery system shall possess redundancy in the pumping and piping systems.

9.6.6.3 Recommendations

The cooling system should ensure that the generator windings and engine block water jacket remain within the manufacturer-specified temperature ranges.

Cooling system ratings have a direct and profound effect on the output kW of the generator set. Altitude must be considered when sizing generator sets, and this is typically accounted for in the radiator system. Remote or shaft-driven radiator fans also may present parasitic loads to the generator, depending on how the radiator is configured. Consult the engine manufacturer during the design and system sizing process.

9.6.7 Mounting

Generators offer the compounded issue of large live loads that vibrate while operating. Substantial foundations are required for any generator system, and this is coupled with some form of vibration isolation. Vibration isolation could be in the form of pads or spring-isolation devices. In areas subject to seismic events, snubber-type bases that allow for operation while the unit is being shaken are typical and are used pursuant to the site's given seismic risk.

9.7 Automation and Control

9.7.1 Introduction

Monitoring is defined as the telemetry and ability to view what is going on within a given system. In some cases, monitoring systems can integrate and manage alarm and trouble signals from the monitored systems.

For the purposes of this section, control is defined as any device that directly regulates a change in state in a given system. Controls are an active system, and may be either:

- Manually initiated and automatically operated based on human input or decision
- Automatically initiated and operated based on a predetermined script or response to a failure or external change of state

9.7.2 Monitoring

9.7.2.1 Requirements

Without monitoring, operators are not able to respond to failures or to determine the loading or operation of their systems. Monitoring is mandatory for all Classes with increasing levels of observation scope and granularity with increasing Class.

9.7.2.2 Recommendations

As Class level increases, monitoring increases by replacing summary alarms with individual alarm points and by presenting systems virtually for the system operators. For Class F4 systems, a virtual single line, which clearly shows system loading and power flow, should be provided. In some instances, a simulator is also provided where changes of state can be tried in a virtual setting to see the outcome prior to employing them in the live, working environment. Electrical systems should divulge all changes in state, alarms, pre-alarms and positions of all breakers, and switches as well as general system information.

Power quality monitoring (PQM) for data centers is recommended since IT systems may be sensitive to power quality, transients, harmonics, and other types of waveform disruption. Power monitoring is also vital as waveform disturbances offer a precise definition of experienced failures and outages. When addressing power system monitoring, there are three facets of observation:

- Power levels noting voltage, current, and frequency
- Harmonic content
- Waveform imaging and capture

Power monitoring offers sampling of the power system's quality in a manner similar to a mechanical system's monitoring of temperature or water chemistry to the chiller/cooling system. PQM should be located at portions of the electrical system that offer a complete view of the vital locations where power is being converted. No particular favor is made over switchgear-integrated monitoring or stand-alone systems. The key element is how they are used.

For the varying levels and locations for PQM as well as systems and component monitoring for each of the Classes, see Table 9-15 (located in Section 9.13).

9.7.3 Control

9.7.3.1 Recommendations

The operation of electrical systems should be automated to the extent possible to minimize human error, which is the predominant cause of system outages. The system should be thoroughly documented, and maintenance staff should be thoroughly trained. Training should include a good understanding of automated procedures and manual override procedures if it is necessary to override the control systems.

Power system control offers substantial challenges to both physical safety and operational assurance. Remote control of critical power systems offers an opportunity to remotely respond to changes of state. However, remote control also offers the hazard of operating large power systems without clear, in-person visual indication as to the result or consequence of the action. Remote control also introduces security concerns and will require provisions to prevent unauthorized access via the internet or other means.

Power system controls should follow these guidelines:

- Use local control only.
- Always implement remote monitoring.
- Utilize control methodologies that react only to the attendant system.

Upstream and downstream systems should react to the changes in state of adjacent or attendant systems without a direct, physical control connection. Controls should be autonomous from any centralized controls unless the facility chooses to operate the system remotely.

- Control interfaces on each piece of equipment should be clear and concise.
Color-coding equipment to denote the particular system, internal switchgear busing (known as mimic busing), position indicating lights, and clearly written labels and nameplates are best practices.
- Standard operating procedures should be posted on each piece of equipment.

9.7.4 System Integration

9.7.4.1 Recommendations

The use of a system integrator is typical for more complex or widespread monitoring systems. These systems are commonly referred to as an electrical power monitoring system (EPMS). The electrical system should integrate to a single “electrical” supervising management system. This system may be a stand-alone, dedicated electrical monitoring system or may be integrated into an overall monitoring and control system that addresses temperature and mechanical system control and monitoring.

The integrator offers a lower workload and database function that categorizes alarm and trouble signals by time or system. Aside from that, the electrical system’s monitoring integrator should also mask and manage duplicate alarms for subordinate systems through consolidated control points such as paralleled UPS modules or generators.

9.8 Lighting

9.8.1 Introduction

Lighting systems are to be designed to provide lighting levels sufficient in output and quality for the task in each area while being of maximum energy efficiency. Elements to be considered are:

- Fixture types
- Lamping types
- Ease of relamping
- Emergency lighting capabilities
- Lighting controls for both safety and for energy efficiency

9.8.2 General Recommendations

The following are recommended to be considered when planning lighting:

- Day lighting of personnel areas such as command center, offices, conference rooms, and break areas with day lighting interface controls is recommended where at all practicable.
- Indirect or a combination of direct/indirect lighting is recommended for personnel and processing equipment areas.
- Switching and controls are recommended to be located so as to be convenient for all of access points to ITE rows and working areas.

It is recommended that a three-level lighting protocol be used in data centers depending on human occupancy:

- Level 1: When nobody is scheduled to be in the data center space, the lighting level should be just high enough that security personnel (stationed outside the unoccupied data center spaces) can monitor the space with surveillance cameras. Cameras should be specified for low-light operation.
- Level 2: Motion detectors should automatically initiate a higher level of lighting once access is detected. The level of lighting should be high enough to clearly permit identification via security cameras. These motions sensors can also replace a manually-switched lighting control system.
- Level 3: Lighting should be a minimum of 500 lux (50 ft-candles) in the horizontal plane and 200 lux (20 ft-candles) in the vertical plane, measured 1 m (3 ft) above the finished floor in the middle of all aisles between cabinets. It is permissible to divide the space in zones and either activate level 3 lighting only in selected zones that require work on equipment or illuminate the complete facility with an override switch. When only selected zones have level 3 lighting activated, the remainder of the space should be on level 2 lighting for human safety reasons.

The motion sensor-based lighting controls would activate lighting in phases, depending on which area of the data center requires occupancy for work or passage. The lighting control system would “sweep” the area and extinguish the lighting after a preset time in order to conserve energy.

Lighting levels required to maintain Code-required egress from the space should be maintained at all times and should be coordinated with the Level 2 lighting requirement noted above.

9.8.3 Computer Rooms

9.8.3.1 Requirements

Computer room lighting systems shall adhere to all local code requirements, including (but not limited to):

- Emergency lighting: exit signage, egress lighting
- Energy efficiency requirements
- Building management systems

9.8.3.2 Recommendations

In locations where people are present, the computer room should have a minimum of 500 lux (50 ft-candles) maintained in the horizontal plane and a minimum of 200 lux (20 ft-candles) maintained in the vertical plane of the data racks, both measured at 1 m (3 ft) above the finished floor. The lighting uniformity (difference between highest and lowest light levels) within the lighting zone(s) should exceed 90% before any equipment or cabinets are installed.

Lighting fixtures should be selected to prevent glare on equipment monitors. Lighting control should be located at the room’s exits with occupancy sensors being highly desirable.

Fluorescent lighting fixtures should be specified with low-RF ballasts. While high-intensity discharge (HID) lighting, such as metal halide or mercury vapor, are not specifically excluded, the restrike time of the fixtures should be as short as possible to prevent long-term lighting outages in the room.

Since the data processing rooms are typically windowless, instant-on lighting is required for the safety of personnel working in the data processing areas during the time a utility outage occurs and the generators assume the load. In this case, 50 lux (5 ft-candles) maintained over 50% of the room is suggested.

- Portable, battery-powered lanterns are recommended to be placed in all computer rooms.

9.8.4 Support Areas

9.8.4.1 Requirements

Support area lighting systems shall adhere to all local code requirements, including (but not limited to):

- Emergency lighting: exit signage, egress lighting
- Energy efficiency requirements
- Building management systems

9.8.4.2 Recommendations

All support spaces should be lit pursuant to the Illuminating Engineering Society (IES) recommendations.

For control rooms, operations center, and other locations where computer screens are present, fixture systems should be selected that reduce or eliminate glare on computer displays. Lighting systems for this area should be commensurate with the noncritical office areas within the facility. The lighting uniformity (difference between highest and lowest light levels) in the rooms should exceed 90%.

Lighting control should be located at the room's exits with occupancy sensors being highly desirable.

Fluorescent lighting fixtures may be specified with standard RF ballasts. In some support spaces, such as generator rooms or large-area central plant spaces, HID lighting such as metal halide or mercury vapor may be used. Should HID sources be used, the restrike time of the fixtures should be as short as possible to prevent long-term lighting outages in the room.

9.9 Bonding, Grounding, Lightning Protection, and Surge Suppression

9.9.1 Introduction

The comprehensive electrical protection required for the critical facility is achieved using a system approach to integrate lightning protection, overvoltage and surge suppression, bonding and grounding, and electromagnetic shielding. This section covers these different systems, which are interdependent upon each other for proper function and efficacy.

Grounding is addressed in three sections: electrical distribution, PDU, and within the computer room.

Electrical system grounding is consistently misunderstood and, for most facilities, not adequately maintained, changed or integrated to the ITE loads that it serves.

It is the intent of this standard to provide a bonding and grounding system that substantially equalizes any non-transient potential differences so that all the enclosures, raceways, and all bonded metal found in the computer room are effectively at the same ground potential (substantially equalized). At higher frequencies, consideration must be given to the impedance of a conductor, not just the resistance. A conductor's impedance can be significantly influenced by its routing path in relation to other nearby circuit conductors and parallel paths such as a metal tray bottom.

Bonding and grounding of data centers relates most specifically to maintaining the facility's common electrical bonding and grounding system along with any desired supplementary bonding and grounding for the ITE. Bonding and grounding also addresses such vital issues as harmonic current management and fault current mitigation. Bonding and grounding also integrates voltage transient suppression by the application of SPD systems as well as lightning protection systems. The bonding and grounding system is one of the few electrical systems completely systemic to the entire critical facility.

If properly organized and installed, the ground system is essentially a radial system from the electrical service entrance. There are a few subtleties for critical facilities that vary from other buildings. Where generators are not treated as separately derived sources, neutrals and grounds are routed with the associated phase wiring and carried back (without being switched) to the main service and terminated on the main service's neutral and ground buses. Where generators are treated as separately derived sources, grounds are carried back to the main service and terminated on the main services ground bus.

Data center bonding and grounding addresses all bonding and grounding work within the critical environment. These systems include:

- The separately-derived system at the PDU
- Ground path to the load
- Critical environment grounding—supplementary at the ITE
- ITE bonding and grounding
- Personal grounding and static discharge.

Bonding and grounding for a data center involve several entities such as:

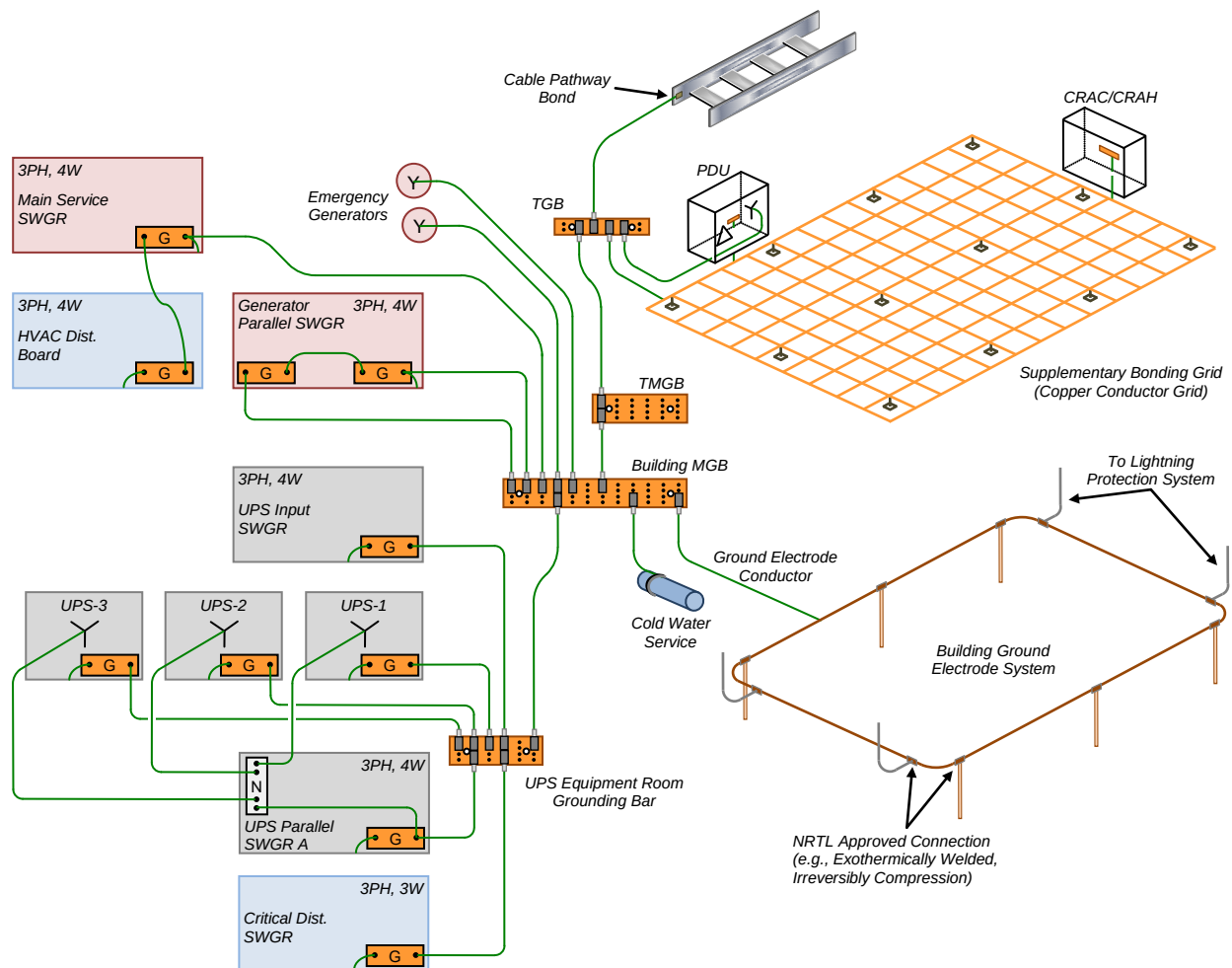
- A common grounding electrode system (GES) for the building, involving the intersystem bonding of a:
 - Grounding electrode system for the electrical power
 - Grounding electrode system for the lightning protection system (LPS)
 - Grounding electrode system for the telecommunications service provider cables and protectors
- Grounding electrode conductors for solidly grounding each power service entrance
- Grounding electrode conductors for solidly grounding each separately derived power source such as an engine-generator for standby power
- Grounding electrode conductors for solidly grounding each telecommunications service entrance

<List continues on next page>

- Bonding and grounding infrastructure for telecommunications utilizing components such as the BCT, TMGB, TBB, TGB, and GE as described in TIA-607-B
- Equipment grounding conductor for power distribution from the service/source to the load
- Structural metal
- Grounding conductors such as the down conductors for a LPS and SPDs
- The common bonding network (CBN) within the building
- Supplemental bonding and grounding structures for electronic equipment such as:
 - Mesh-bonding network (mesh-BN)
 - Isolated bonding network (IBN)
 - Supplementary bonding grid.

NOTE: The common bonding network (CBN) is the set of metallic components that are intentionally or incidentally interconnected to form the bonding network (a mesh) in a building. The CBN always has a mesh topology and connects to the grounding electrode system via one or more grounding conductors.

The data center or critical environment specifics are noted later in this section. A simplified example model for a critical facility bonding and grounding system is shown in Figure 9-35.



Note 1: Not all items shown are present in every data center.

Note 2: Actual wiring should take into account local rules and conditions.

Figure 9-35
Example Critical Facility Bonding and Grounding Diagram for Class F2 and Lower

Figure 9-36 provides an example of the bonding and grounding infrastructure of a data center that has two entrance rooms with one MGB with Figure 9-37 providing an example of a Class 4 bonding and grounding infrastructure supporting two entrance rooms and two electrical distributions, each with its own MGB.

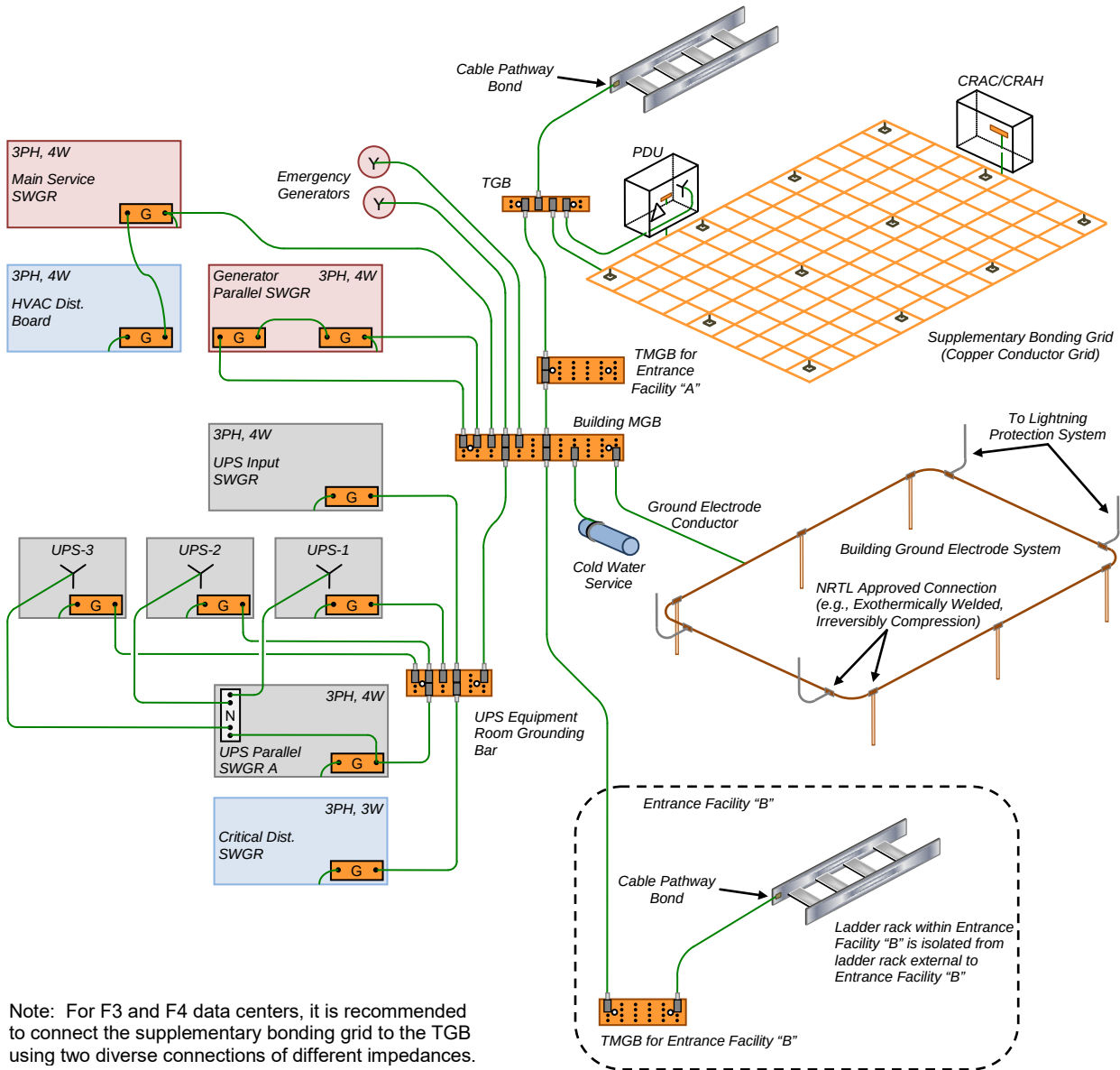


Figure 9-36
Example Critical Facility Bonding and Grounding Diagram For Class F3

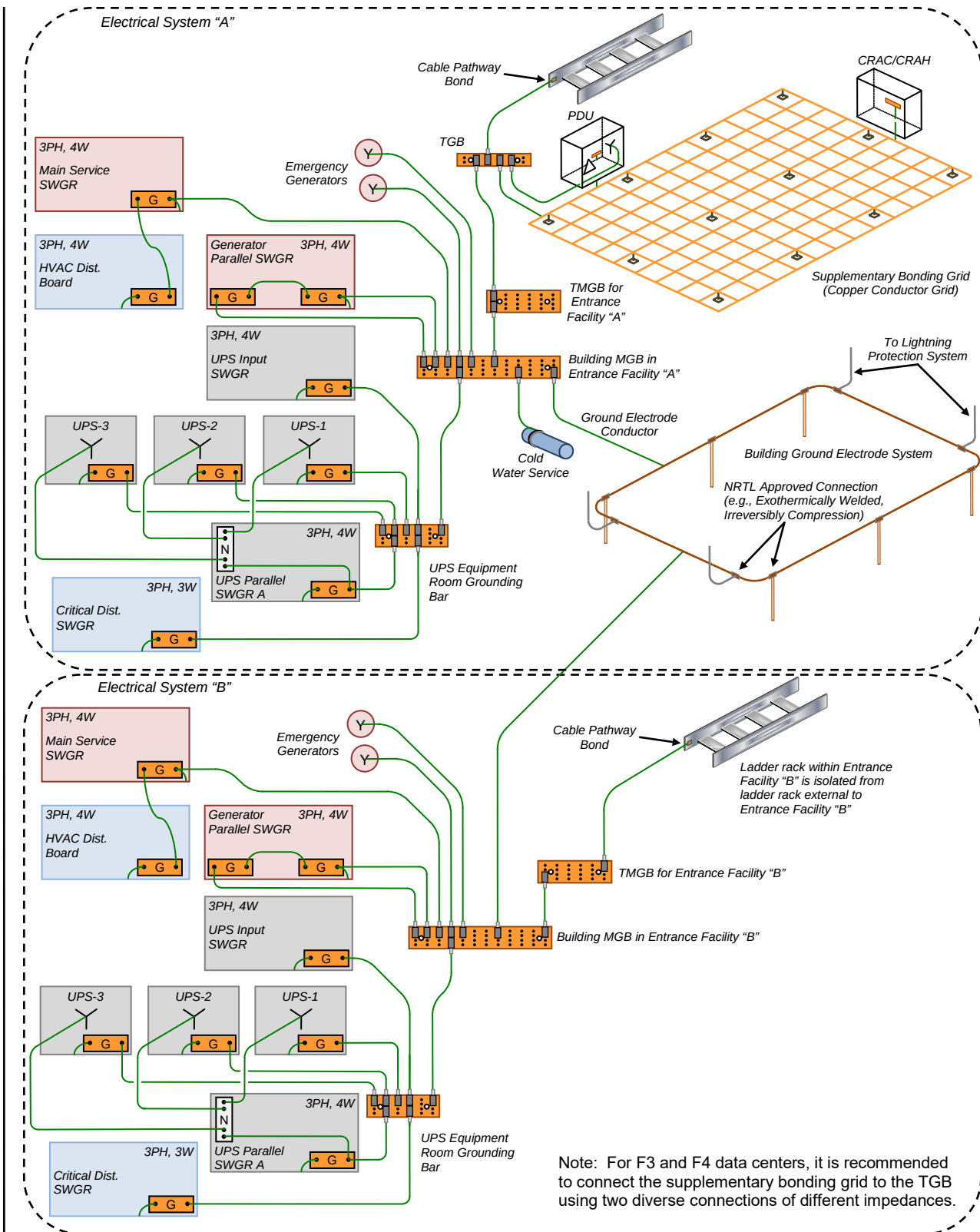


Figure 9-37
Example Class F4 Bonding and Grounding Diagram (Two MGB and Two Entrance Facilities)

Serving power systems and electronic equipment bonding and grounding primarily involves the serving power source and the power distribution to the IT and other electronic equipment. This primary level of bonding and grounding is required to be in accordance with the NRTL product safety listing of the power system and the electronic equipment (load). The entities of concern are the grounding electrode conductor (system) and equipment grounding (bonding) conductor (or green wire). These dedicated circuit conductors are required for the safe operation of the equipment, including any ground faults. In some instances, equipment may be designed as “double insulated,” whereby the NRTL requirements for the equipment grounding conductor may be eliminated (e.g., a two-prong plug or receptacle). Although data center electrical and electronic equipment may be considered “grounded” according to its NRTL requirements, supplementary bonding and grounding are recommended.

High-resistance/impedance grounding (HRG) systems can be used in lieu of solidly grounded systems. HRGs are typically designed to limit a ground fault current to 10 Amps or less. The advantages of using HRGs are:

- Safety enhancements because of mitigation of phase-to-ground fault currents
- Operational enhancements because of reduction of ground fault current trips
- Reduced cost because of the elimination of four-wire feeders

Historically, HRGs were utilized in industrial facilities with critical processes. More recently, they are being deployed in a growing number of mission-critical facilities. They are most useful where process control requires an orderly shutdown to avoid high costs of restoration of the process.

Typically, the HRGs are installed at the service transformer. They function down to the first separately-derived source in the distribution system. Where used for ITE installations, consideration should be given to any impact on the resistance/impedance of the grounding systems. HRGs may influence the level of electrical noise versus earth ground at higher frequencies such as for filters. The impact may occur because of reactance of the resistance/impedance devices such as an inductor or wire-wound resistor. Inductive/reactance grounded power systems are not recommended for low voltage systems. Check with the UPS system manufacturer if it is not connected to solidly grounded neutral sources as they typically will provide “neutral” grounding kits for their UPSs.

See NECA/BICSI 607 for additional requirements and recommendations for planning and installation of telecommunications bonding and grounding.

9.9.2 General Recommendations

The following considerations are important for understanding the complexities of bonding and grounding for a data center:

- All dead metal objects within the data center should be grounded (this includes empty cabinets and racks and ladder racks).
- Equipotential grounding becomes increasingly difficult across an expanse such as a building or larger data center.
- Distributed grounding (within a building or complex) cannot accomplish equipotential grounding.
- A dedicated and separate ground for data center equipment is NOT recommended and is entirely likely to be an electrical safety violation.
- Especially where multiple services (power and communications) enter the building at separated locations, a buried ground ring is recommended to provide equipotential bonding. Where multiple power service entrances are involved, the ground ring conductor should be sized at 107 mm² (4/0 AWG) minimum bare copper.
- Where equipment is designed for double insulation, grounding that equipment may be a secondary concern (pending its product safety listing requirements and electromagnetic emissions compliance).
- Any electrical grounding infrastructure (such as NECA 331) placed for the electrical power system should not replace the separate bonding and grounding infrastructure for telecommunications (TIA-607-B).
- The infrastructure described in TIA-607-B is better placed in the central portions of the building and away from exterior locations where lightning current activity is more likely.

<List continues on next page>

- Supplementary bonding and grounding of data center equipment is recommended (this is over and above bonding and grounding of the serving power distribution) as it:
 - Provides for more locally grounded equipment
 - Maintains a level of grounding even if the serving power circuit grounding is interrupted
 - Provides dispersed path(s) for ESD currents to follow
 - Provides conductive paths among interconnected equipment where common configurations include grids and planes. A mesh-BN (depending on its installation techniques), inclusion of a supplementary bonding grid, the mesh density, and the routing pattern of signal and power cabling may:
 - Further reduce the levels of inter-unit common-mode electrical noise on signal and power cabling
 - Provide a lower resistance and lower impedance inter-unit ground reference
 - Reduce damage to inter-unit equipment during power fault and surge events
 - An isolated bonding network (IBN) may be utilized for certain telecommunications applications whereby the electronic equipment system is only grounded via a single point connection window. This concept has been used by the telecommunications service providers (primarily for DC powered systems, but may also be applicable for AC powered systems).
- Data circuits between data centers and different floors should be decoupled to prevent issues related to unwanted electrical transients. Fiber optic circuits and links are ideal for decoupling. Some types of circuits may utilize suitable transformer isolation for decoupling.

9.9.3 Lightning Protection

9.9.3.1 Introduction

Lightning events can cause fires, damage to buildings, and breakdowns of electrical, telephone, and computer installations, which may result in considerable losses in operational revenues and increased customer dissatisfaction. Damage results from electromagnetic fields from the lightning strike, voltage differentials in ground systems, and structural damage from ohmic heating or mechanical forces. This damage can be attributed to insufficient direct strike protection; deficient grounding, bonding, and shielding techniques for the susceptibility level of the installed electronic equipment systems; and deficient selection and installation of surge protective devices.

Depending on the geographical location for the data center, there may be local guides available specific to the country or region, such as the risk analysis guide provided in NFPA 780, which takes into account geographical location and building construction among other factors in determining the suitability of a lightning protection system. If a lightning protection system is installed, it shall be bonded to the building grounding system as required by the prevailing standards and AHJ and as required for maximum equipment protection.

9.9.3.2 Requirements

For some locations, lightning protection is required by AHJ for basic building safety and protection.

If a lightning protection system is present, the lightning protection system shall be:

- Applied as a comprehensive system
- Integrated with properly sized and installed SPDs
- Implemented to cover all systems and buildings serving the critical environment

9.9.3.3 Recommendations

Where protection from lightning-caused voltage fluctuations and transients is to be provided for protection of critical facilities, installation should be in accordance with industry recognized standards such as NFPA 780, IEC 62305-3, or IEC 62305-4.

9.9.4 Surge Suppression/Surge Protective Devices (SPDs)

9.9.4.1 Introduction

Surge suppression, as used in this section, encompasses all surge protective devices or SPDs.

NOTE: Within surge suppression for low voltage AC power circuits, the term *surge protective device (SPD)* has replaced the term *transient voltage surge suppression (TVSS)* with TVSS no longer in use.

Surges and transient power anomalies are potentially destructive electrical disturbances with the most damaging being overvoltage occurrences and short duration events. High-energy transient power anomalies can arise from inductive load switching or other events within the power system or from capacitive and inductive coupling from environmental events such as nearby lightning activity. Environmental and inductive power anomalies are wideband occurrences with a frequency range from close to DC to well into the RF high-frequency spectrum. It is critical that each point-of-entry (e.g., power, HVAC, telephone, LAN, signal/control, RF) into the equipment area be protected against these anomalies. This protection is essential to reduce the risk of personal injury, physical equipment damage, and loss of operations. Although lightning can cause the most visible damage, it is not the predominant cause of transient voltages.

Sources of transient voltage include, but are not limited to:

- Power company switching
- Generator transfer
- Shared commercial feeders with poor line regulation
- Load switching
- Fault currents
- HVAC units
- Heating elements
- Power tools
- Electric motors
- Fluorescent lights.

SPDs and large-scale surge suppression are an integral part of the high voltage lightning protection for a facility. Additional low voltage transient mitigation is typical for an information technology facility to protect against internally-generated transient events.

For lower Classes of data centers, SPDs are located on the utility entrance with transients not being addressed further downstream unless the site demands it. For higher reliability Classes, SPDs are prevalent throughout the power system. As the data center Class increases, SPDs may be found in the following locations:

- Utility service entrances
- Generator buses
- UPS inputs
- UPS outputs
- UPS power distribution switchboards
- PDUs and critical power distribution panels

9.9.4.2 Requirements

The installation of surge protective devices is a requirement for all data centers Class F1 and higher. A lack of surge protective devices would result in a Class F0 rating.

SPDs shall be provided and installed in the locations specified in Table 9-13 based on the Facility Class.

SPDs shall not be mounted inside the switchgear (unless specifically designed, manufactured, NRTL listed, and properly installed for integral installation) and shall be installed with minimum lead lengths and separation of input/output wiring in order to perform properly. For application guidance on the use of facility level SPDs for AC power systems, see IEEE C62.72 and IEEE 1100.

NOTE: For DC power surge protection, see IEEE 1100.

Table 9-13 SPD Locations as per Class

<i>System</i>	<i>Class F0</i>	<i>Class F1</i>	<i>Class F2</i>	<i>Class F3</i>	<i>Class F4</i>
Utility Service Entrance	Recommended	Required	Required	Required	Required
Generator Buses	Recommended	Recommended	Required	Required	Required
UPS Rectifier Inputs	Optional	Recommended	Required	Required	Required
UPS Static Bypass Inputs	Optional	Recommended	Recommended	Required	Required
UPS Maintenance Bypass Inputs	Optional	Recommended	Recommended	Required	Required
UPS Outputs	Optional	Optional	Optional	Optional	Optional
Critical Switchboards (downstream from UPS)	Optional	Optional	Optional	Optional	Optional
PDU or RPP	Optional	Optional	Optional	Optional	Optional

9.9.4.3 Recommendations

SPDs should meet the following minimum criteria:

- Listed to AHJ requirement (e.g., UL 1449)
- Provide surge current diversion paths for all modes of protection:
 - L-N, L-G, and N-G in WYE systems
 - L-L and L-G in DELTA systems.
- Modular in design with redundant protection circuitry
- Visible indication of proper SPD connection and operation
- Audible alarm for diagnostic monitoring, activated upon failure of a SPD
- EMI/RFI filtering using MIL-STD-220A methodology or equivalent AHJ requirement

For application guidance on the use of facility level SPDs for AC power systems, see IEEE C62.72, IEEE 1100, and NFPA 70, Article 285.

Over time, SPDs have a risk of ground faults because of degradation of insulation. One method to mitigate insulation degradation is to monitor neutral current for signs of degradation.

9.9.5 Telecommunications Surge Protection

9.9.5.1 Requirements

9.9.5.1.1 Primary Protection

The purpose of primary protection is to help ensure personnel safety and help protect internal cables from extremely high voltage. The installation of primary SPDs shall comply with all applicable codes. The devices shall be designed to comply with one or more of the following:

- UL 497
- UL 1449 (latest edition)

and shall be marked with one or more of the following:

- UL listing
- CE certification listing mark (where recognized)
- Other local codes or standards as established by the AHJ

The SPD shall be installed at the entrance point into any building and within close proximity (adjacent) to the electrical service entrance and the building electrical main ground bar. Minimizing the grounding conductor lead-length between the SPD and electrical service entrance will improve the efficacy of the SPD device by reducing the self-inductance of the grounding lead. This will help reduce the voltage rise between the SPD and the electrical service entrance. In lightning prone areas, a SPD shall also be installed on each end of an inter-building cable run to help ensure that high energy is not allowed to penetrate the building interior. In some applications, a fused type primary SPD may be required. To reduce the need for fuse replacement, devices that incorporate resettable fuse technology are recommended.

The primary SPDs in telephone circuits, data circuits, and control circuits shall be grounded in accordance with NFPA 70 or other applicable codes or standards. Primary SPDs shall have the ground terminal bonded to the building MGB, TMGB, or a dedicated ground bus conductor. The conductor shall be free of sharp bends. The grounding conductor for a single line primary SPD shall be 5.26 mm² (10 AWG) or larger; the grounding conductor for multiple line primary SPDs shall be 13.3 mm² (6 AWG) or larger.

9.9.5.1.2 Secondary Protection

The primary purpose of secondary SPDs is to limit the magnitude of current that can be imposed on the secondary wiring from the primary SPD to the ITE. To be effective, the secondary protection must properly coordinate with the primary protection. A collateral purpose is to limit transient overvoltages to within the prescribed withstand level of the protected equipment. The SPD also serves as a barrier against transient anomalies that may be induced between the cable entrance point and the equipment and in cable runs within the building.

Secondary SPDs shall be installed as close to the equipment being protected as possible. This includes, but is not limited to, the circuits associated with the base stations, repeaters, remotes, modems, consoles, network interface units and channel banks that extend from the room or equipment area. Secondary SPDs shall comply with safety and performance standards for their designated function. The devices shall bear the UL 497A listing mark, the international CE certification mark (where recognized), or as required by AHJ.

A separate bonding conductor shall be used to bond each secondary SPD grounding conductor or ground terminal of the frame to the TMGB, TGB, or other approved ground bus conductor that serves the associated equipment. The grounding conductor for a single line secondary SPD shall be 5.26 mm² (10 AWG) or larger; the grounding conductor for multiple line secondary SPDs shall be 13.3 mm² (6 AWG) or larger. If a separate rack ground bar is installed for the SPDs, it shall be effectively bonded back to the equipment ground bus system.

This conductor shall be as short as possible, free of sharp bends, and shall be routed as directly to the equipment grounding conductor or ground bus as is possible. The operating voltage and SPD configuration is application dependent. Where the ITE is already rated for internal secondary protection, the stand-alone secondary protector is not required.

9.9.5.2 Recommendations

The selected level of secondary surge suppression rated voltage should be chosen to ensure selective coordination with the protected equipment.

When several secondary SPDs are installed at an equipment cabinet or rack, the SPDs should be placed at a central location within the cabinet or rack so that they can be effectively bonded back to the equipment cabinet or rack rack ground bar or back to a separately installed rack ground bar.

9.9.6 Building Ground (Electrode) Ring

9.9.6.1 Requirements

A building ground electrode ring shall be installed for facilities where a lightning protection system is installed or where there are multiple power service entrance locations along the periphery of the facility.

All below grade grounding connections shall be made by NRTL-approved methods such as exothermic weld or high-compression connectors.

As required by local codes and standards, the ground ring shall be bonded to structural metal at every other column or more often. Concrete-encased electrodes (also known as Ufer electrodes) shall be used in new construction as a method of supplementing the grounding electrode system. Concrete-encased electrodes improve the effectiveness of the grounding electrode system because of concrete having hygroscopic properties and by providing a much larger surface area in direct contact with the surrounding soil:

- Concrete-encased electrodes shall be encased by at least 51 mm (2 in) of concrete, located within and near the bottom of a concrete foundation or footing that is in direct contact with the earth.
- Concrete-encased electrodes shall be at least 6 m (19.7 ft) of bare copper conductor not smaller than 21.1 mm² (4 AWG) or at least 6 m (19.7 ft) of one or more bare or zinc galvanized or other conductive coated steel reinforcing bars or rods at least 12.7 mm (0.5 in) in diameter.
- Concrete-encased electrodes shall be bonded to any other grounding electrode system at the site.

This building grounding system shall be directly bonded to all major power distribution equipment, including all switchgear, generators, UPS systems, and transformers, as well as to the telecommunications systems and lightning protection system. The facility shall possess a building electrical main ground bus (MGB) where all the large-load feeder facility grounds terminate. This is the location, coupled with the telecommunications main grounding busbar (TMGB), where the grounding system can be validated for both continuity and impedance.

9.9.6.2 Recommendations

A building ground electrode ring should be installed for all facilities. Single or triplex ground rod fields as the only earthing vehicle are not adequate for a critical facility. Generally, the direct burial connections should meet appropriate electrical testing requirements as set out in the applicable standards and codes to ensure durability. Designs may vary according to the site parameters such as available real estate, earth resistivity, frost line level, and the depth of the water table.

Ground bus bars should be placed so as to facilitate bonding and visual inspection.

The ground ring should be 107 mm² (4/0 AWG) minimum bare copper wire buried a minimum 800 mm (30 in) deep and a minimum 1 m (3 ft) from the building wall. For larger sizes, stranded conductors are recommended. Ground rings encircling buildings should be installed just beyond the roof drip line. The size of the ground ring conductor is recommended to be the same as the largest size required by AHJ for a grounding electrode conductor to promote the accomplishment of intersystem bonding. Additionally, ground rods should be connected to the ground ring. Typical ground rods are 19 mm by 3 m (3/4 in by 10 ft) copper-clad steel ground rods spaced every 6 to 12 m (20 to 40 ft) along the perimeter ground loop.

Test wells for the building ground electrode ring should be provided at the four corners of the loop.

In its entirety, the common grounding electrode system should not exceed 5 ohms to true earth ground as measured by the fall of potential method (IEEE 81). As noted in the NEC, IEEE 1100, and IEEE142, common bonding of different systems plays a crucial role along with grounding.

9.9.7 Supplementary Bonding and Grounding

9.9.7.1 Introduction

Supplementary bonding and grounding methods are those provided in addition to the bonding and grounding measures typically required by the applicable electrical safety codes and product safety standards. Supplementary bonding and grounding methods are intended to improve facility and equipment performance related to bonding and grounding. Examples of supplementary bonding and grounding entities may include metallic raceways, racks and cable trays; under the raised floor or above the cabinet and rack metallic grid work; metal plates and metal sheets; multiple bonding conductors from equipment to a grounding/bonding structure, etc.

9.9.7.2 Supplementary Bonding and Grounding Structures

A grounding system for a data center with raised floor is illustrated in Figure 9-38. It includes not only the power system ground but also supplementary bonding and grounding.

A supplementary bonding and grounding system commonly in the form of a mesh-bonding network (mesh-BN) equipped with a supplementary bonding grid (SBG, also historically known as a signal reference structure—SRS) is frequently utilized in data centers where there is a raised floor. As noted in IEEE 1100, the default equipment bonding topology is the common bonding network (CBN) and the supplementary bonding grid can be readily utilized for efficient direct bonding of equipment and other apparatus to the grounding system. For the typical data center, the supplementary bonding grid becomes a component of the mesh-BN. The supplementary bonding grid is an externally installed network of conductors used to effectively bond together disparate metal cabinets, rack frames, and enclosures. Such an arrangement provides efficient grounding and inter/intra-unit bonding of metal cabinets, racks, and miscellaneous metal objects (especially when they are not powered). Additionally, the mesh-BN ensures grounding reliability of the equipment in the event the equipment grounding conductor of the serving power circuit is compromised or disconnected during maintenance. Electrostatic charge buildup and dissipation is also greatly aided by the multiple grounding paths of the mesh-BN (see Figure 9-38).

9.9.7.3 Mesh-BN

9.9.7.3.1 Introduction

The supplementary bonding grid (SBG) may be a recommendation from, or an actual part of, the equipment manufacturer's installation package. Typically, it is part of an aftermarket, field-installed wiring effort.

The mesh-BN has three primary purposes:

- It may enhance the reliability of signal transfer between interconnected items of equipment by reducing inter-unit common-mode electrical noise over a broad band of frequencies. When properly designed, installed and utilized it can be effective for noise control across low-frequency single-ended signaling links or poorly designed communication links. This function is typically limited to around 30 MHz using flat strap for 600 mm (24 in) grid spacing.
- It is intended to prevent damage to inter-unit signal circuits by providing a low impedance (low inductance) path and thus an effective ground reference for all externally installed AC and DC power, telecommunications, or other signal level, line-to-ground/chassis-connected SPD equipment that may be used with the associated equipment.
- The mesh-BN is intended to prevent or minimize damage to inter-unit signal-level circuits and equipment power supplies when a power system ground-fault event occurs.

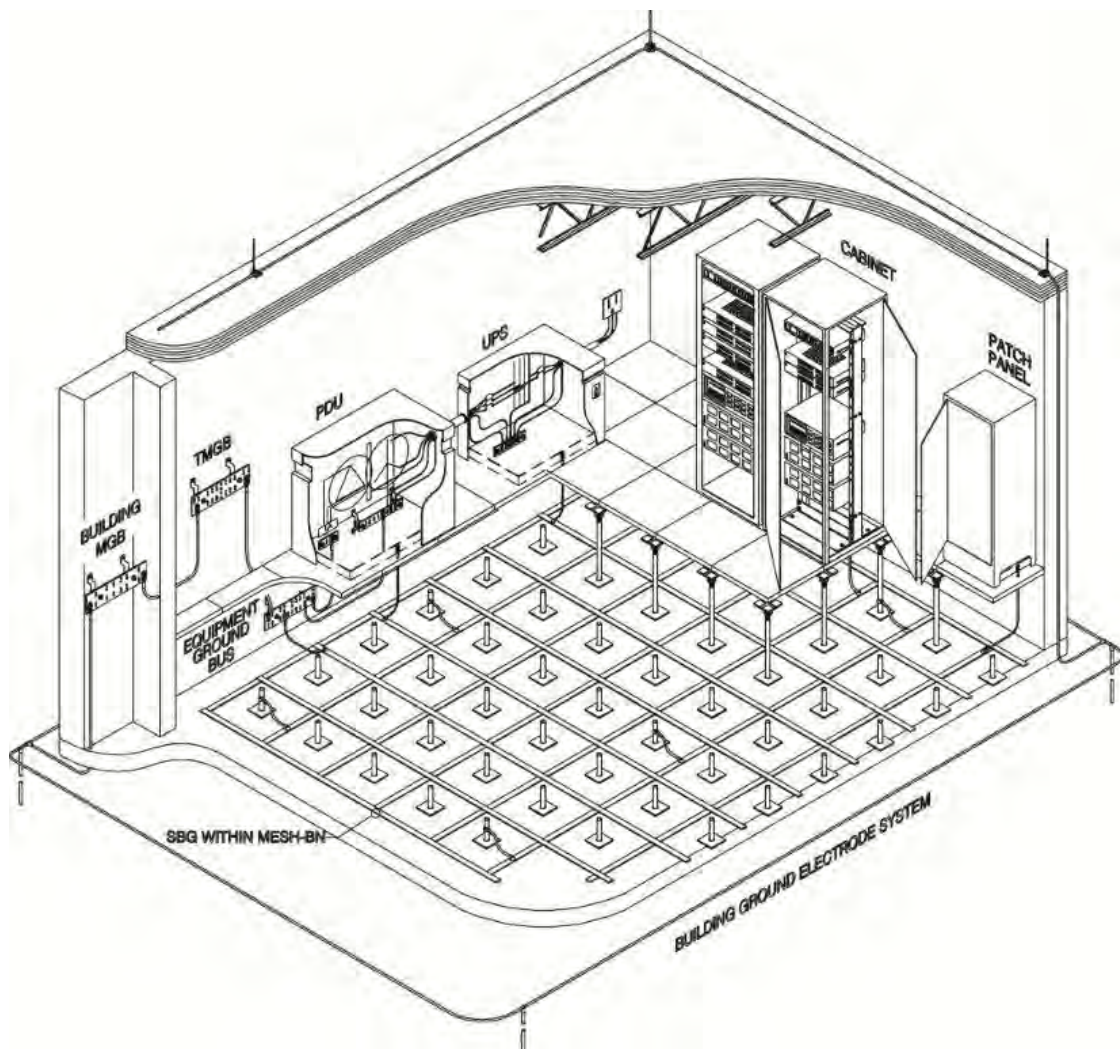


Figure 9-38
Typical Data Center Grounding Schema (shown with raised floor)

The mesh-BN creates an equipotential ground reference for the computer room and may reduce stray high-frequency signals.

The mesh-BN may include a supplementary bonding grid in the form of a pre-fabricated or field assembled bare round wire or flat copper strip joined together via welding, brazing, compression or a suitable grounding clamp arrangement at each of the crossing points. The mesh-BN can also include field assembling a grid from the raised floor pedestals using standard or bare round wire.

9.9.7.3.2 Requirements

When used, the mesh-BN becomes an integral part of the CBN; it shall not be insulated or isolated from the building electrical system ground. Where utilized, the mesh-IBN (isolated bonding network) shall be insulated or isolated from the CBN except through a single point connection window. The mesh-IBN typically does not utilize an access floor or underfloor bonding grid as a supplementary bonding entity to the mesh-IBN. The reason is that the cabinets and racks are insulated/isolated from the flooring in order to accomplish the single point grounding scheme back to the single point connection window. Otherwise, the mesh-IBN intra-unit bonding is very similar to that used in a mesh-BN. The mesh-IBN is further described in IEEE 1100. The mesh-IBN is not considered typical for a commercial data center installation but may be encountered in an access provider data center.

If ground clamps are used, they shall be listed (e.g., UL 467) for the application. Wire hangers or positioning devices (e.g., UL 2239) shall not be used as ground clamps.

If constructed using round conductors, the bonding grid shall be no smaller than 13.3 mm² (6 AWG) and up to 42.4 mm² (1 AWG) is typical. The conductors may be bare or insulated copper.

All metal surfaces, with the exception of lighting fixtures, door frames, window frames, and pathways shorter than 1 m (3 ft), shall be bonded to the bonding grid.

NOTE: Conduit sleeves, metallic firestop systems, and other isolated pathways and devices shorter than 1 m (3 ft) do not need to be bonded to the grounding system.

9.9.7.3.3 Recommendations

The mesh-BN should include a SBG such as a copper conductor grid on 600 mm to 3 m (24 in to 10 ft) centers that covers the entire computer room space. The ideal spacing for the grid is between 600 mm to 1.2 m (24 in to 4 ft). If the declared bandwidth is to be realized and the SBG is to provide enhanced reliability of signal transfer (as discussed in the introduction above) by reducing inter-unit common-mode electrical noise over a broad band of frequencies, the grid spacing must be kept at 600 mm (24 in) or less and the associated cabling must be routed in close proximity to the SBG.

The flat copper strip form of the supplementary bonding grid is typically installed with a prefabricated mesh. The grid should be prefabricated out of a minimum 0.40 mm (26 gauge) × 50 mm (2 in) wide copper strip with all crossing interconnections welded, not punched (see Figure 9-39). The grid spacing of the mesh-BN should be 600 mm (24 in). Adjacent rolls of mesh-BN are exothermically welded in the field to form a continuous grid (see Figure 9-40). The copper strips are typically factory welded into a grid pattern prior to installation and then rolled out onto the floor in sections with some minor exothermic welding performed on site prior to occupancy and IT operations commencing to complete the installation.

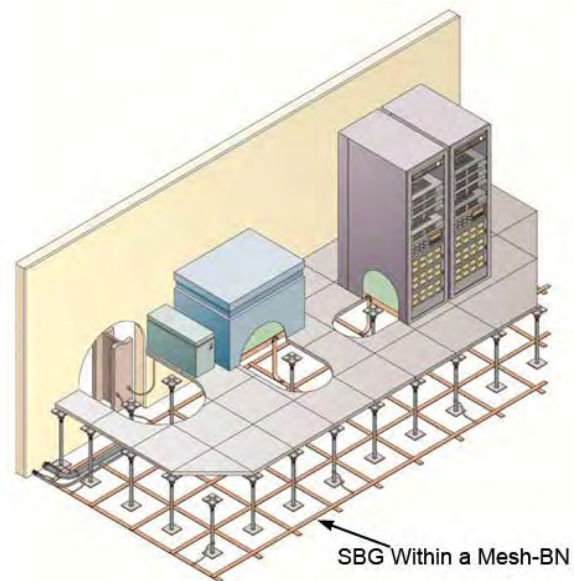


Figure 9-39
Typical Configuration of Flat Strip-Type SBG
Within a Mesh-BN

In all cases, the SBG should be bonded to the pedestals of the raised floor system. If the grid is in the form of a flat strip grid (600 mm (24 in) spacing), at least every 6th pedestal should be bonded to the grid. If the grid is in the form of a fabricated bare round wire mat, then at least every 3rd pedestal should be bonded to the grid. If the grid is formed from the raised floor pedestal system, then at least every second pedestal should be bonded to the grid. The bonding jumper from the pedestal to the supplementary bonding grid should be no greater than 600 mm (24 in) in length. When using the access floor with bolted stringers as the supplementary bonding grid, note that it may not be as effective as a bonding grid that is built in place using copper conductors and exothermically-welded joints or mechanical conductor clamps. Considerations include the removal of access floor tiles for temporary work, etc.

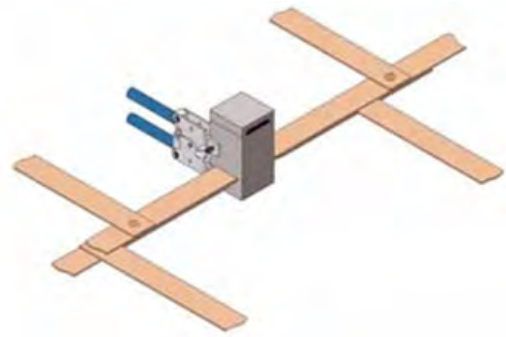


Figure 9-40
Adjacent Rolls Of Flat-Strip-Type SBG Being
Exothermically-Welded Together

A SBG may be fabricated from standard, bare round wire or flat copper strip joined together via welding, brazing, compression or a suitable grounding clamp arrangement at each of the crossing points (see Figure 9-40). Because of the larger surface area, flat strap provides better transient protection, especially at higher frequencies.

For a wire grid, bare (non-insulated) copper is preferred because it provides greater ease of attachment of equipment to the mesh-BN. Since the immediate grid area is being rendered to the same potential, inadvertent or intermittent contact points should not be an issue if personal grounding systems are being used.

The grounding and bonding infrastructure and ITE components should have the connections listed in Table 9-14.

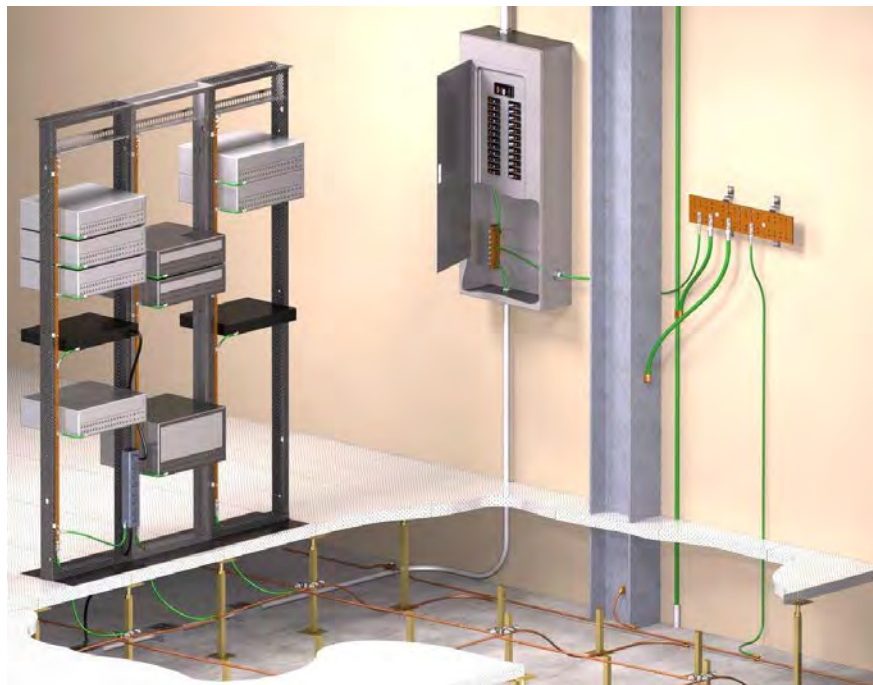


Figure 9-41
Data Center Grounding Infrastructure (Room Level) Example

Table 9-14 Grounding and Bonding Connection Schedule

<i>Connection</i>	<i>Minimum Conductor Size</i>	<i>Note No.</i>
TMGB – Building Main Ground Bus	130 mm ² (250 MCM) bare	
EGS – TMGB	130 mm ² (250 MCM) bare	
PDU – TMGB/TGB	Per applicable code (e.g., NEC 250-122)	
HVAC equipment – mesh-BN/SBG	13.3 mm ² (6 AWG) bare	
Steel column – mesh-BN/SBG	21.1 mm ² (4 AWG) bare	1 and 2
Rebar mat foundation – mesh-BN/SBG	21.1 mm ² (4 AWG) bare	3
Cable management – cable tray, conduit	13.3 mm ² (6 AWG) bare	4
Access floor pedestal – mesh-BN/SBG	13.3 mm ² (6 AWG) bare	5
Sprinkler piping – mesh-BN/SBG	13.3 mm ² (6 AWG) bare	
HVAC ductwork – mesh-BN/SBG	13.3 mm ² (6 AWG) bare	
Cabinets – mesh-BN/SBG	13.3 mm ² (6 AWG) bare	6
Equipment enclosures – mesh-BN/SBG	13.3 mm ² (6 AWG) bare	6
Frames – mesh-BN/SBG	13.3 mm ² (6 AWG) bare	6
Other metallic system enclosures – mesh-BN/SBG	13.3 mm ² (6 AWG) bare	

NOTE 1: Size in excess of TIA -607-B for the design of the telecommunications bonding and grounding infrastructure. Ground size should be this size or should match the ground conductor required at the electrical service entrance, whichever is larger.

NOTE 2: Proper NRTL listed mechanical lugs and clamps or exothermically-welded connections to steel column.

NOTE 3: Weld to rebar mat before pour.

NOTE 4: Every joint should have a bonding jumper.

NOTE 5: Utilize mechanical lugs, clamps, or exothermically-welded connections on pedestal body and spade-type tab under stringer screw-down.

NOTE 6: Cabinets, racks, frames, and equipment enclosures shall be individually bonded to the mesh-BN/SBG—not bonded serially.

9.9.7.4 Equipment Bonding and Grounding to the Mesh-BN

9.9.7.4.1 Requirements

All metallic enclosures shall be supplementary grounded and bonded in addition to required safety grounding provided by the serving power circuit. This provides for both staff safety as well as grounding continuity, which is the logical extension of the data center grounding infrastructure to the load itself. Each equipment cabinet and equipment rack requires its own grounding connection within the mesh-BN. A minimum of a 13.3 mm² (6 AWG) insulated stranded copper conductor exothermically welded or mechanically terminated within the mesh-BN and mechanically terminated to the cabinet via a proper machine screw through-bolt connection or factory-provided spot weld.

Bare metal-to-bare metal contact is mandatory for all ITE enclosure bonding connections with anti-oxidant applied at the connection point of the equipment either in the field or by the factory prior to shipping the equipment.

Each cabinet or rack shall have a suitable connection point (or points where multiple connections are desirable) to which the rack framework grounding conductor can be bonded.

Alternatives for this connection point are:

- **Rack ground bus:**
Attach a dedicated copper ground bar or copper strip to the rack. A bond between the ground bar or strip and the rack shall exist. The mounting screws shall be of the thread-forming type, not self-tapping or sheet metal screws. Thread-forming screws create threads by the displacement of metal without creating chips or curls, which could damage adjacent equipment.
- **Direct connection to the rack:**
If dedicated copper ground bars or strips and associated thread-forming/self-tapping screws are not used, then paint shall be removed from the rack at the connection point, and the surface shall be brought to a shiny gloss for proper bonding using an approved antioxidant.
- **Bonding to the rack:**
When bonding the rack framework grounding conductor to the connection point on the cabinet or rack, it is desirable to use two-hole lugs. The use of two-hole lugs helps to ensure that the ground connection does not become loose because of excessive vibration or movement of the attaching cable.

9.9.7.4.2 Recommendations

The recommended method for all bonding is the use of an insulated, stranded copper grounding wire, sized as recommended, and terminated by a two-hole compression lug or exothermic weld.

A rack grounding busbar (RGB) or 13.3 mm² (6 AWG) rack bonding conductor (RBC) ground wire should be installed in each cabinet or rack, mounted on the backside of one upright running the entire height of the cabinet to provide an easy access grounding facility within each cabinet or rack. See Figure 9-42.

9.9.8 Information Technology Equipment Interconnections

9.9.8.1 Introduction

An integral part of the bonding and grounding network in the access floor area or any critical environment is the grounding of the IT support equipment and static discharge management during ongoing operations. This includes the connection of a cabinet of ITE chassis to the mesh-BN, connections between various IT systems and cabinets, and personal grounding checks and static charge dissipation.

9.9.8.2 Rack Connections to the Mesh-BN

It is common for cabinets to be physically connected for structural integrity, and they also may be logically, virtually, or network connected, acting as an integral platform.

This is achieved by the manufacturer assembling the cabinet or rack in such a way that there is electrical continuity throughout its structural members. For welded racks, the welded construction serves as the method of bonding the structural members of the rack together.

All adjacent cabinets and systems should be bonded in order to form grounding continuity throughout the rack structure itself.

Electrical continuity cannot be assumed using nut and bolt connections used to build or stabilize equipment cabinets and racks. Bolts, nuts, and screws used for rack assembly may not be specifically designed for grounding purposes, and unless grounding bonding jumpers are installed, do not assume electrical continuity for the cabinet lineup. Further, most cabinets and racks are painted, and as paint is nonconductive, this negates any attempt to accomplish desired grounding. Therefore, paint or cabinet coating has to be removed in the bonding area for a proper bond to be formed.

Most power is routed over the top or bottom of the rack. Without a reliable bond of all four sides of the rack, a safety hazard exists from potential contact with live feeds.

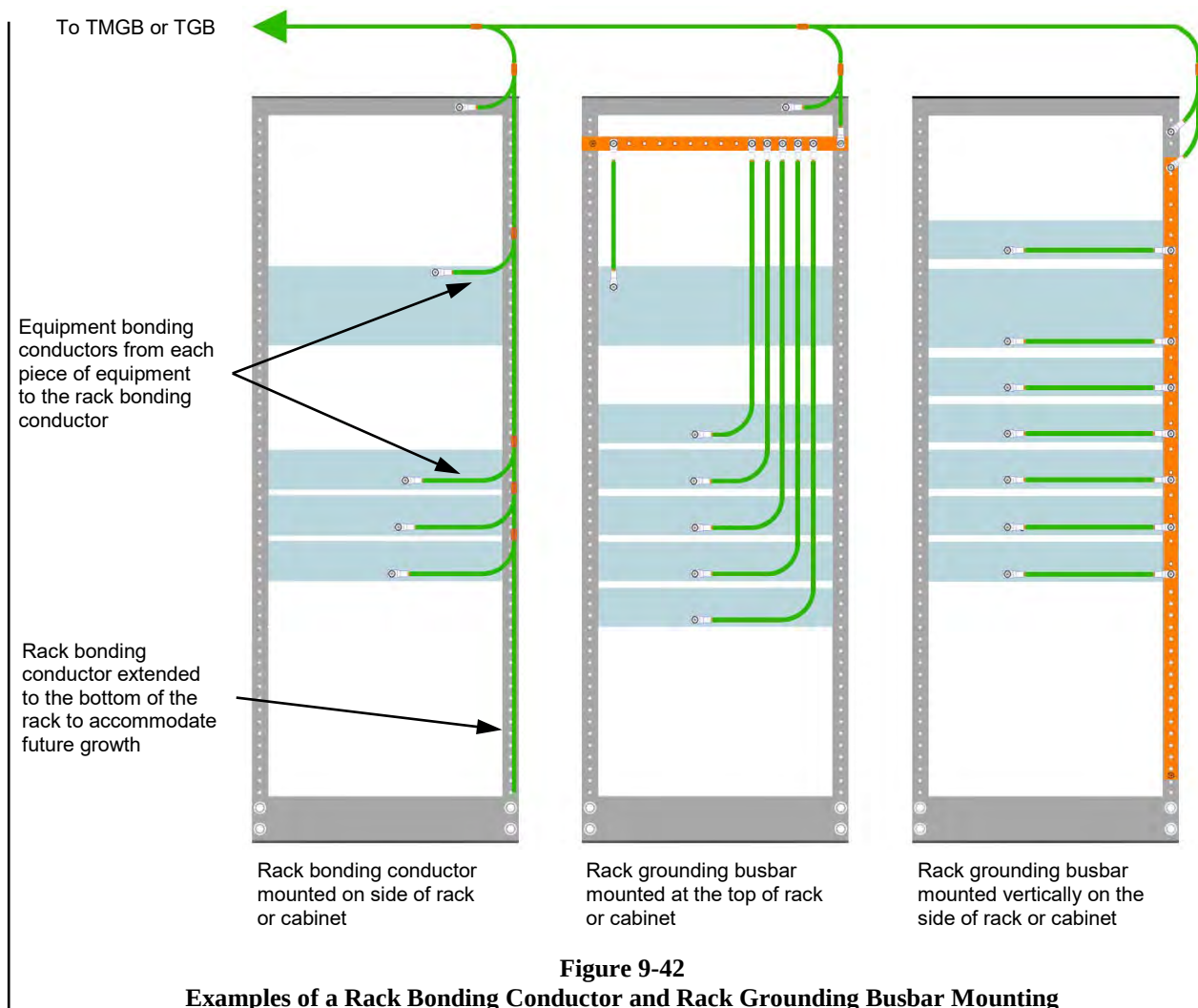


Figure 9-42
Examples of a Rack Bonding Conductor and Rack Grounding Busbar Mounting

9.9.8.3 ITE Bonding to the Cabinet or Mesh-BN

9.9.8.3.1 Requirements

The ITE chassis shall be bonded to the rack using one of the following methods:

- Manufacturer-provided grounding location:

Ideally, the manufacturer will supply a separate grounding hole or stud. This hole or stud shall serve as the primary grounding site for the ITE chassis and shall be used with a conductor of proper size to handle any fault currents up to the limit of the circuit protection device feeding power to the equipment unit. Each end of this chassis grounding conductor will be bonded to the chassis hole or stud, and the other end will be properly bonded to the copper ground bar or strip. In some instances, it may be preferable to bypass the copper ground bar or strip and bond the chassis grounding conductor directly to the data center grounding infrastructure.

- Grounding via the mounting system:

If the equipment manufacturer suggests grounding via the chassis mounting flanges and the mounting flanges are not painted, the use of thread-forming screws and normal washers will provide an acceptable bond to the rack.

If the equipment mounting flanges are painted, the paint can be removed, or the use of the same thread-forming screws and aggressive paint-piercing lock washers, designed for this application, will supply an acceptable bond to safety ground through the rack.

Grounding through the equipment AC (alternating current) power cord does not meet the intent of this section where the power path and the equipment path offer redundant and specific ground paths for the ITE loads. While the AC-powered equipment typically has a power cord that contains a ground wire, the integrity of this path to ground cannot be easily verified. Rather than relying solely on the AC power cord ground wire, it is desirable that equipment be grounded in a verifiable manner such as the methods described in this section.

Once the cabinets or racks are grounded, the equipment installed within the cabinet or rack shall be bonded to the mesh-BN ground reference as well. Some of this has been undertaken by equipment manufacturers for enterprise-level or factory-configured systems. For field-assembled rack-mounted systems, equipment grounding must be added to complete the ITE-to-mesh-BN grounding connection via the cabinet chassis.

9.9.8.3.2 Recommendations

Cabinet doors and side panels should be bonded to the cabinet frame with the frame connected to the grounding system. (See Figure 9-43).

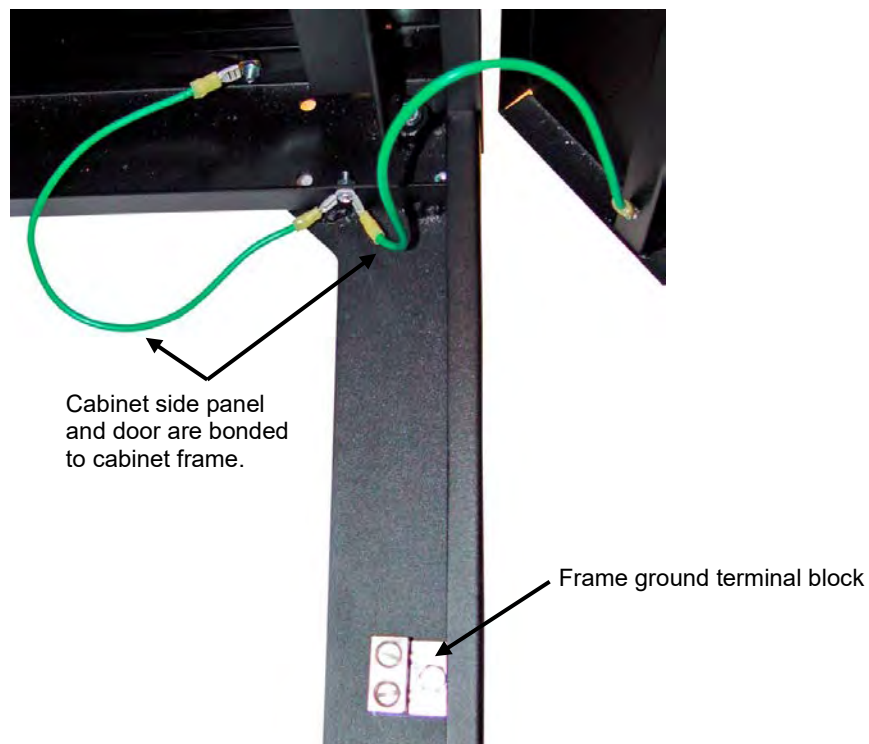


Figure 9-43
Example of Bonding of Cabinet Side Panel and Door

9.9.8.4 Personal Grounding and Static Discharge

Electrostatic discharge (ESD) is the spontaneous transfer of electrostatic charge. The charge flows through a spark (static discharge) between two bodies at different electrostatic potentials as they approach each other.

CAUTION: Electrostatic discharge (ESD) may cause permanent damage or intermittent malfunction of networking hardware. Anyone that touches network equipment or network cabling becomes a potential source of ESD as it relates to telecommunications equipment. Network cabling that has been installed but not connected may become charged when these cables are un-spooled and slid over carpet or other surface that contributes to the buildup of ESD. The charged cabling may become a source of ESD to the telecommunications equipment to which it connects. Charged cabling should be discharged to an earth ground prior to connection to network equipment. ESD charges may remain for some time, especially in dry conditions.

Factors affecting ESD charge retention include:

- Cable design
- Dielectric materials
- Humidity
- Installation practices

Low humidity and static-generating building materials are the primary causes of ESD. There should be no significant ESD charge retention difference between types of telecommunication cabling as all cables have a nearly identical ability to acquire a static charge (see Sections 14.8 and 14.9 for additional information about telecommunication cabling).

It is important to follow all ESD specifications and guidelines provided by the applicable network equipment manufacturer. Mitigation techniques, such as anti-static flooring and humidity control, are important for critical installations.

The use of static discharge wrist straps when working on or installing network or computer hardware is specified in most manufacturers' installation guidelines. Wrist strap ports should be attached to the rack by a means that ensures electrical continuity to ground. Pedestrian static discharge mats may be required for certain access floor environments or spaces with standard resistance flooring.

9.9.9 Power System Bonding and Grounding

9.9.9.1 Introduction

In the past, 4-wire systems were normal in critical facilities, mimicking the X-O bonding and services in traditional commercial spaces. This led to some substantial problems caused by ITE loads producing harmonics that were able to readily propagate through the power system. These harmonics caused problems such as large-scale and objectionable ground currents (often in the hundreds of amps), the failure of small X-O bonds on branch circuits, and ITE disruption and failure. Nuisance tripping of ground fault elements was also experienced.

The designer is faced with the question of what purpose the neutral serves in the 480/277 V_{AC} and 208/120 V_{AC} system. Only lighting and small-scale loads are served by the 480/277 V_{AC} and 208/120 V_{AC} neutral (when compared to the critical facilities overall load).

Without some form of isolation for these noncritical 480/277 V_{AC} and 208/120 V_{AC} neutrals, the incoming 480 service would be forced to generate a neutral at the highest point in the low-voltage electrical system to serve this minority of loads. This allows harmonics to propagate across several systems because they are being connected to a 4-wire switchboard or system. The balance of the loads in the facility are essentially 3-wire since there is no need for X-O bonds or a separately-derived system for the 3 phase, 3-wire mechanical system, or for the rectifier side of the UPS system. Some form of a separately-derived system or X-O bond is required for these small 480/277 V_{AC} and 208/120 V_{AC} loads. However, because generating a fourth wire for those systems and their X-O bond presents an issue for most of the electrical system, an isolation transformer for the small 480/277 V_{AC} loads is desirable.

Since isolating these loads is a positive design element and that an isolation transformer will be provided for the small 480/277 V_{AC} loads, 3-wire feeds then become the standard for the balance of the loads in facility. This indicates that the X-O bond for the 208/120 V_{AC} loads within the critical environments and below the inverters of the UPS systems are below the UPS on the load side of those systems.

All loads in the critical environment will be provided with dedicated and insulated ground wires from the load to the derived ground point at the PDU.

9.9.9.2 Bonding and Grounding – AC and DC Powered Telecommunication Systems

IEEE 1100 integrates many of the traditional telecommunications recommendations and describes how to integrate the AC and DC power systems to accomplish the important safety and performance objectives of each. The key concepts related to bonding and grounding deal with both the serving power system and the ITE. The serving power system is grounded to the building's grounding electrode system. The grounding electrode system is connected to the common bonding network within the building (see Figure 9-44). For ITE, IEEE 1100 refers to multipoint connections as the common bonding network and a single point of connection as an isolated (insulated) bonding network.

Much of the guidance on bonding and grounding DC power systems for telecommunications and ITE is rooted in the traditional telephone (telecommunications) utility (regulated) industry. The basis of this guidance is supported in IEEE 1100 for the commercial (deregulated) industry with some modifications made to meet requirements of the commercial market segment.

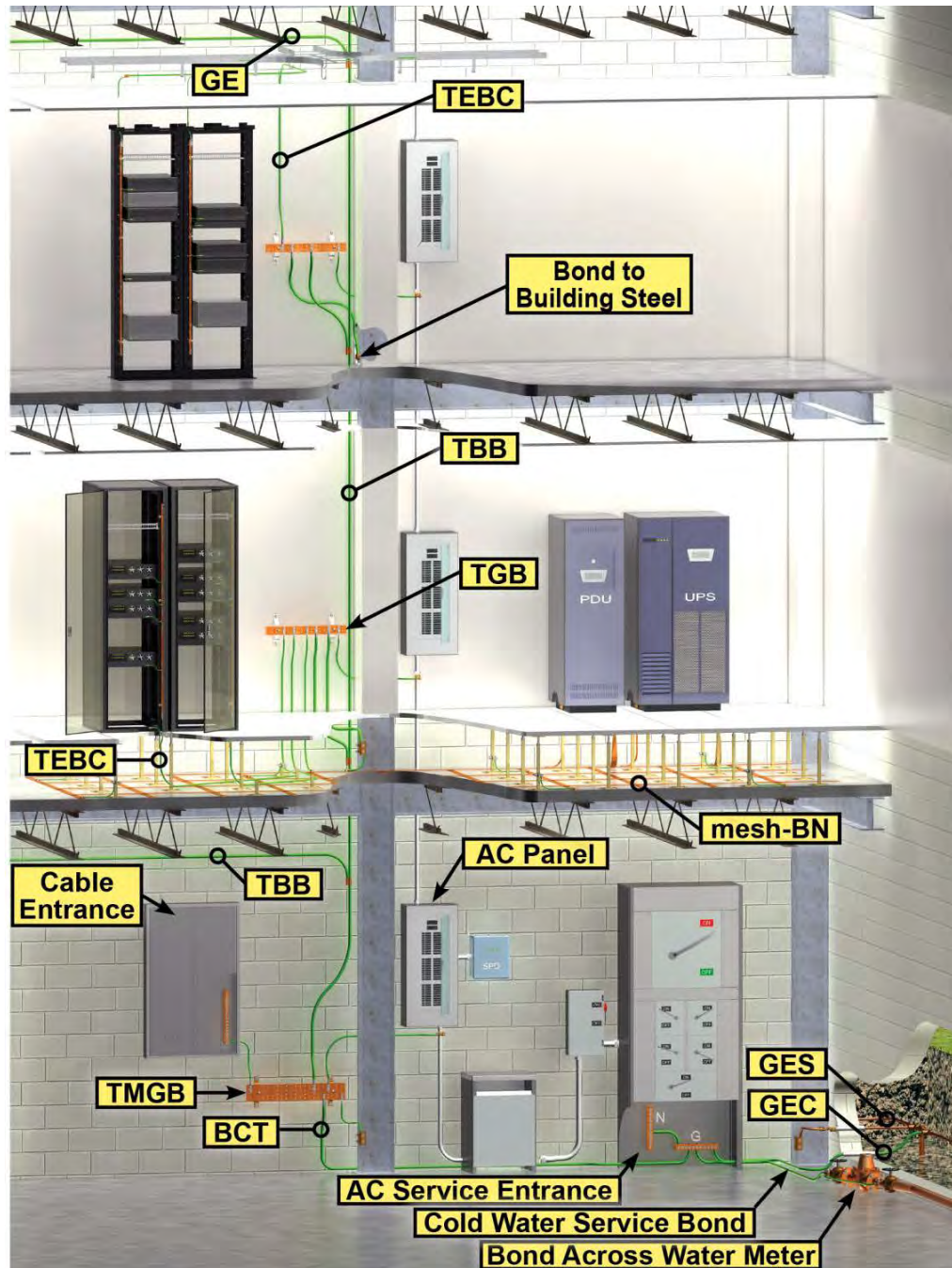


Figure 9-44
Telecommunications Bonding and Grounding Infrastructure

A significant observation is that, historically, telecommunications is DC powered and historically ITE is AC powered. Therefore, the bonding and grounding standards for these different types of power systems is historically different because of the DC being predominantly utilized in a regulated environment considered “under the exclusive control of the utility” (NFPA 70).

For the data center, a telecommunications bonding and grounding infrastructure, in accordance with TIA-942-A, TIA-607-B, and IEEE 1100, is expected. This infrastructure is bonded to the electrical power grounding electrode system, to structural metal (where accessible), and to the serving AC power panel equipment ground at each floor. Grounding needed for the data center equipment is obtained from the expected ground bar on that floor (such as a TGB). Note that this bonding and grounding infrastructure is not the same physical structure as the grounding infrastructure that might be placed for the electrical power system.

In no situation should a totally separate grounding system be deployed because this may lead to safety and performance problems.

Noise concerns for the data center equipment do involve common mode noise generated and distributed by the power system to the electronic load equipment. Generally, the equipment AC input power supplies are quite tolerant of common mode noise. It should also be expected that server and other equipment manufacturers will design and test their equipment’s (higher voltage) DC input power supplies to ensure that they will be similarly robust. This is already accomplished for 48 V_{DC} telecommunications equipment meeting the requirements of Telcordia GR-1089-CORE-2006 and placed into a common bonding network (CBN).

9.9.9.3 Bonding and Grounding—Telecommunications DC Systems

Generally, telecommunications DC power systems date back to the first telephone systems where DC was used for signaling circuits and for operating switching and control relays. Centralized (bulk) DC power plants (systems) had primary components such as rectifiers, a powerboard, primary and secondary distribution feeders, and fuse bays. The DC power system was grounded to earth (often more than once). The grounded conductor was termed the return. The connected load equipment was called telecommunications load equipment (TLE [hereafter referred to as ITE]).

Modern DC power systems are more compact, use much smaller footprint components, and are more efficient. Today, a small, centralized DC power system can be contained in a single rack. For standards compliance purposes, this equipment is generally classified as ITE. For the purposes of evaluating DC powered ITE, robustness of the system is a key consideration. Accordingly, certain questions arise regarding grounding, bonding, and protection of the installation. Example questions include:

- Is the ITE suitably robust (per Telcordia GR-1089-2006) to operate in a Common Bonding Network (CBN)?
- Is the ITE not suitably robust (per Telcordia GR-1089-2006) and therefore, must be operated in an isolated bonding network (IBN)?

NOTE: The significant role of the IBN topology is to isolate the ITE from currents flowing through the CBN, especially lightning.

- Is the DC power supply dedicated to a single type of equipment bonding network (CBN or IBN), or is it to be a shared resource?
- Where is the planned location for the DC power supply relative to the location of the ITE?
- Is any of the ITE required to integrate the return and DC equipment grounding conductor (DCEG) at the DC power input?
- Availability requirements for ITE in a data center may not need to be specified to all of the points required for a telecommunications service provider (TSP) such as at a telecommunications central office. The availability specification will determine if an IBN may be appropriate for the data center or a portion of the data center.

Generally, the modern centralized DC power system is designed to operate as a single-point grounded system. An equipment-grounding (bonding) conductor is installed as part of the distribution circuit to ground any metal parts of the ITE and to clear any ground faults by facilitating the timely operation of the upstream overcurrent protection device. The system grounding (electrode) conductor is termed the DCG and is connected to the return near the DC power source. The return is only grounded once. This arrangement is very similar to bonding and grounding an AC power system per NFPA 70 with some possible variations allowed by UL60950. See Figure 9-45 through Figure 9-49.

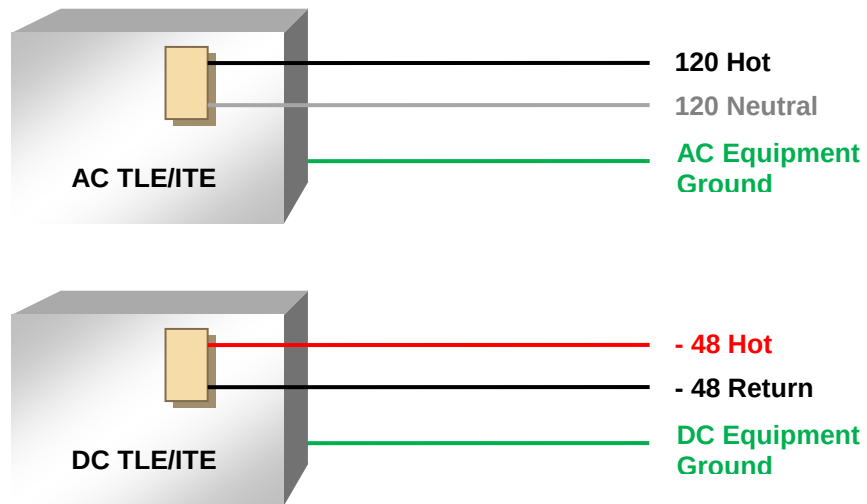


Figure 9-45
Similarity of Recommended Grounding for AC and DC Power Systems and Load Equipment

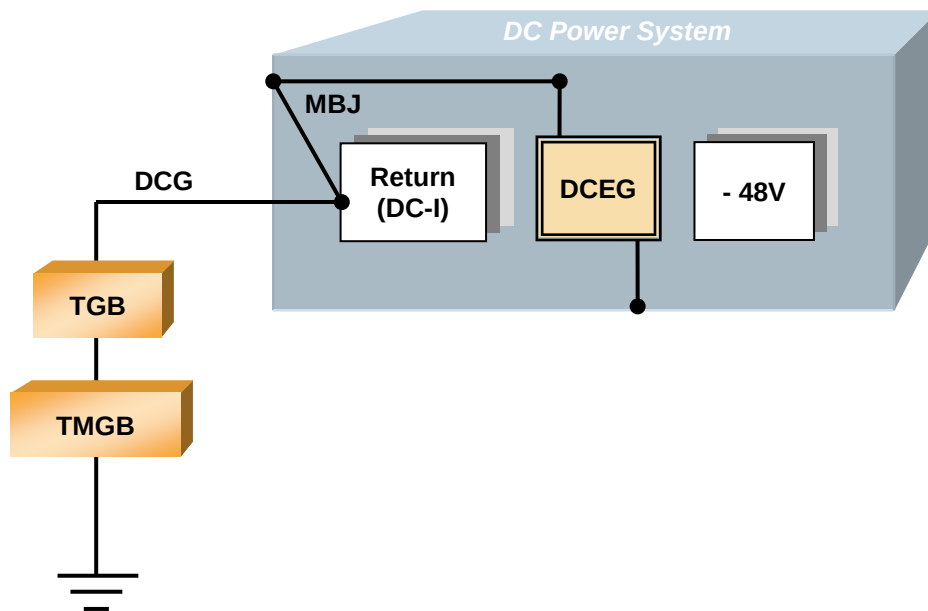


Figure 9-46
DC Power System Showing a Single-Point Grounded Return

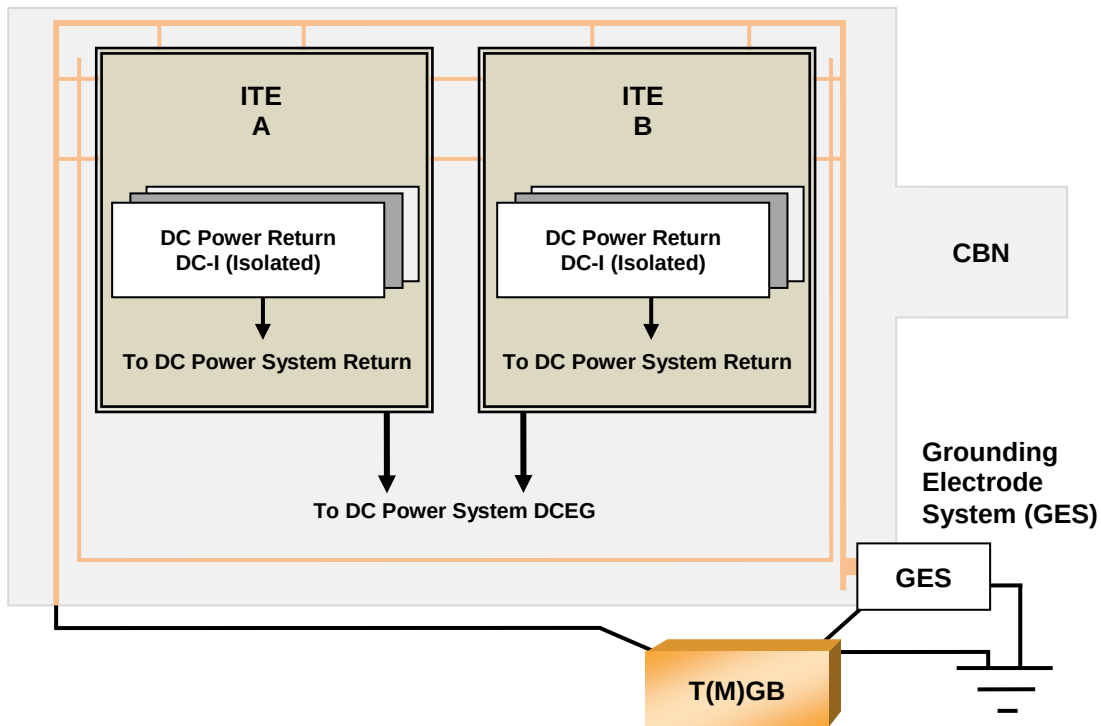


Figure 9-47
Information Technology Equipment Showing Grounding of DC Power Input (Return Is Insulated)

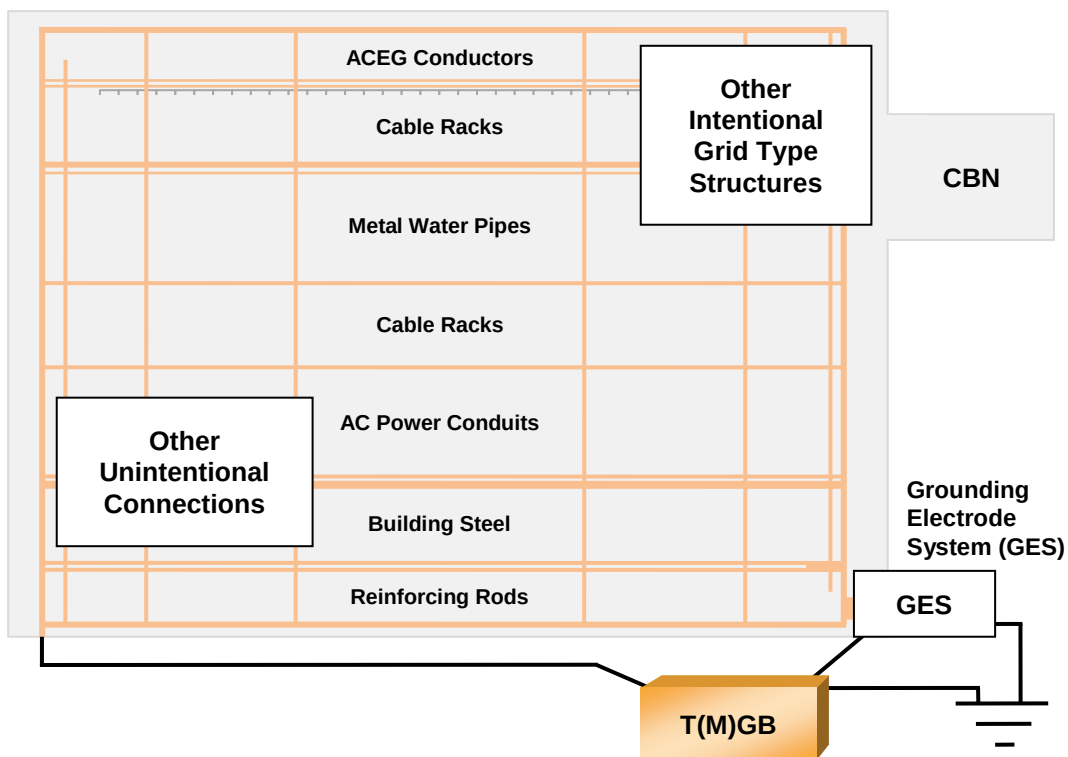


Figure 9-48
Common Bonding Network

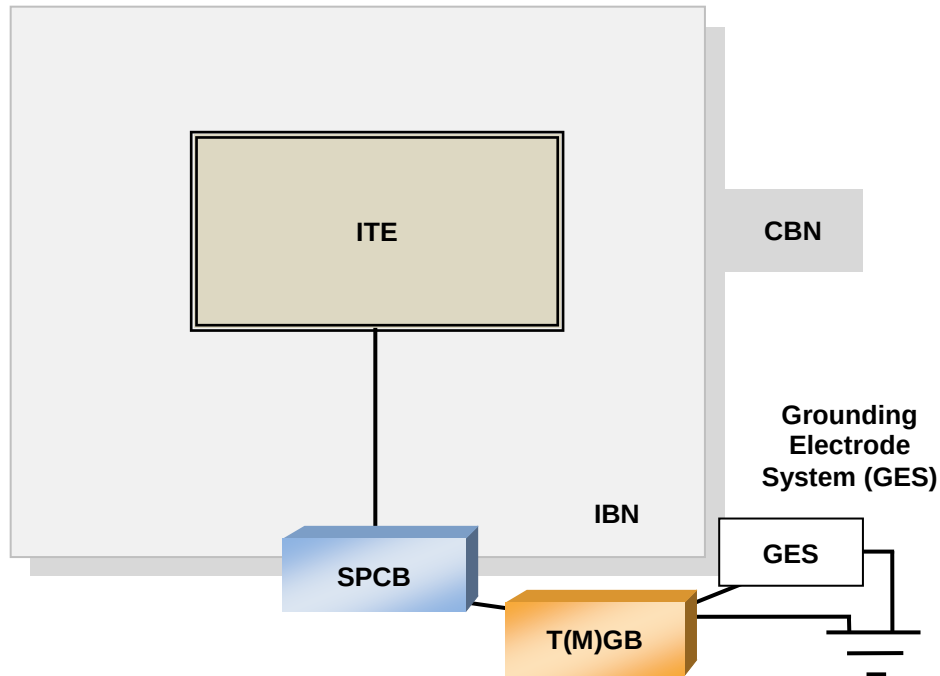


Figure 9-49
Isolated (Insulated) Bonding Network

9.9.9.4 Bonding and Grounding—Higher Voltage DC Systems (above 160 V_{DC})

9.9.9.4.1 Requirements

DC power systems for data centers shall meet applicable bonding and grounding requirements. Grounding and bonding methods shall comply with all requirements of the AHJ, including those for point-of-system grounding connections, equipment grounding, and conductor sizes for the grounding electrode system and equipment bonding jumpers.

9.9.9.4.2 Recommendations

For 380 V_{DC} systems, the preferred grounding method is high resistance mid-point grounding of the output of the DC power source (DC rectifier or DC UPS or other DC source equipment); however, other means of grounding are possible as solid mid-point grounding, positive side grounding, negative grounding, and even floating point (ungrounded) systems. The selection of the grounding methods depends primarily on the protection and fault detection for the entire system, and it should be consistent through the entire network. For more detailed requirements, please refer to the applicable standards.

9.9.9.4.3 Additional Information

There are several existing standards outlining recommended practices, including IEEE C2, IEEE 1100, and ANSI T1.311.

Applying DC power system telecommunications utility practices to the nonregulated environment of a data center requires additional considerations. These considerations include:

- The point at which the DC system grounding electrode conductor (DCG) attaches to the centralized DC power system and whether it is allowed to occur between the source and the telecommunications load equipment (per UL60950).
- Whether the DC power system equipment grounding conductor (DCEG) is allowed to be routed separate from the DC supply and return circuit conductors per UL 60950.
- Whether the DC equipment ground is permitted to be bonded to the return at the load equipment per UL 60950.

Based upon these considerations, the prudent approach is to utilize IEEE 1100 as the base document for bonding and grounding the DC power system in a data center as it:

- Provides a topology similar to that of an AC power system
- Provides a single-point grounding of the DC power system at the source location
- Provides a co-routed DC equipment grounding conductor with the circuit wiring (supply such as – 48 V return)
- Prohibits bonding of DC equipment grounding conductor to the “return” at the load equipment
- Provides fully controlled paths for direct current

9.10 Labeling and Signage

9.10.1 Introduction

Labeling and signage falls into several categories:

- Building information such as room names and numbers
- Hazard and safety such as chemical and shock hazard signage, exit signs, wet or open floor rope-offs, safety data sheet (formerly called material safety data sheet) locations, EPO signage, and warning signs for personnel, operation, or safety
- Indicating signage such as equipment labeling and the color-coding of systems
- Informational such as routine and exceptional informational posting on bulletin boards

9.10.2 Requirements

Systems and labeling shall be color coded according to IEEE standards (e.g., IEEE), and are subject to approval by the AHJ.

Labeling shall be integrated to the individual systems and shall provide the operator an understanding of system status under cursory examination. Labeling works hand in hand with the graphical user interface (GUI) and the physical organization of the equipment and systems themselves.

The GUI is typically a visual dashboard for the complete operation of the system. Information that the GUI typically includes are a color -coded power flow diagram, electrical performance, electrical characteristics, and alarm status.

Equipment may have a mimic bus display, indicating how power flows through the system and how the individual breaks are connected. It may also be color-coded for the critical, utility, and generator power systems. For example, a critical power system with four distinct UPS systems could be labeled UPS-A, UPS-B, UPS-C, and UPS-D. Such a system could bear a unique color-coding where the A system might be red, the B system might be blue, the C system might be green, and the D system might be yellow. This color-coding would be carried all the way through the system.

All branch and data center circuits shall be marked with their individual circuit designations. Conduit systems and junction boxes shall also be color-coded by system, and power feeders may also bear their specific designation (e.g., UPS A Input). Conduit color-coding may be via a label, cladding, or painting.

9.10.3 Recommendations

Circuits that are on the output of an UPS or that support critical loads should be color-coded to readily distinguish them from non-critical circuits. This color-coding may be in the form of colored self-adhesive labels or nameplates.

Equipment labeling should possess all critical information concerning the system to which it is affixed. This information should include:

- Equipment nomenclature and designation (e.g., Generator AH54)
- System capacity rating in kVA and kW (e.g., 750 kVA/675 kW)
- Input voltage, phasing, and connection (e.g., 480V, 3-phase, 3-wire)
- Output voltage, phasing, and connection (e.g., 480V, 3-phase, 3-wire)
- Power factor (e.g., 0.9 lagging)
- System or switchboard serving this piece of equipment
- System, switchboard, or load that is being served by this equipment

| See Figure 9-50 for an example of an equipment nameplate.

9.10.3.1 Arc Flash Labels

A Class F3 or Class F4 data center can be designed to allow concurrent maintenance so that work should never be required on energized equipment. However, such architecture may be prohibitively expensive or inappropriate for the application. So-called “hot work” is not a best practice and should be avoided whenever possible, but in a 24/7 data center operation, scheduled down time may not be available on demand. Work on energized equipment would require an authorized energized equipment work permit (EEWP).

Labeling should conform to requirements of local codes, but typical minimum requirements identify:

- Voltage
- Fault current
- Flash and shock boundaries
- Incident energy levels
- Recommended minimum levels of PPE

Figure 9-51 shows an example of an arc flash label.

9.11 Testing and Quality Assurance

9.11.1 Requirements

All functional testing shall examine normal, failure and maintenance modes of operation.

9.11.2 Recommendations

Testing and design/construction quality assurance are vital to validate that the design and installation will operate as intended. While this may appear to be a daunting task, by approaching this process as a sequential, reinforcing, non-redundant set of activities, it can present a logical and direct solution to systems validation needs.

For electrical systems and the sheer complexity and safety required to operate these systems, there are two fundamental camps—basic electrical construction quality control and system functional testing. The electrical quality control considerations include feeder continuity testing, basic switchgear testing, feeder landing/torque testing, labeling, overcurrent short circuit validation, trip settings per the coordination study, and safety signage such as arc flash indication. Basic system startup, assisted by the manufacturer’s representatives, is also included in this group of activities.

The system functional testing assumes that the basic field quality controls will render a complete, safe, and functional system pursuant to the design and specifications. Testing steps assume that the installation has fully met the requirements of a specific testing level prior to proceeding to the next phase of testing.

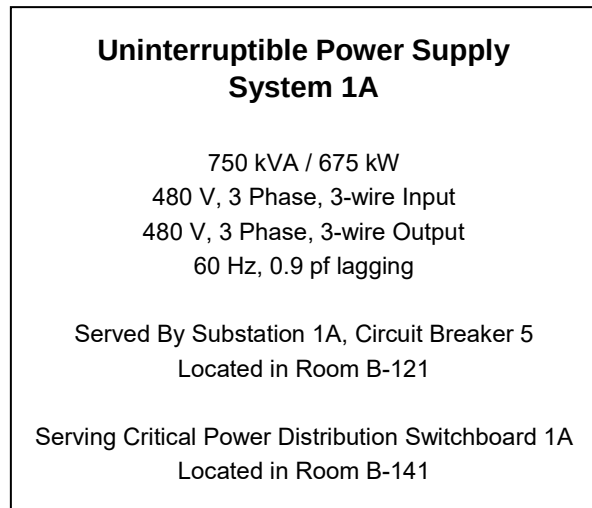


**Figure 9-50
Sample Equipment Nameplate**

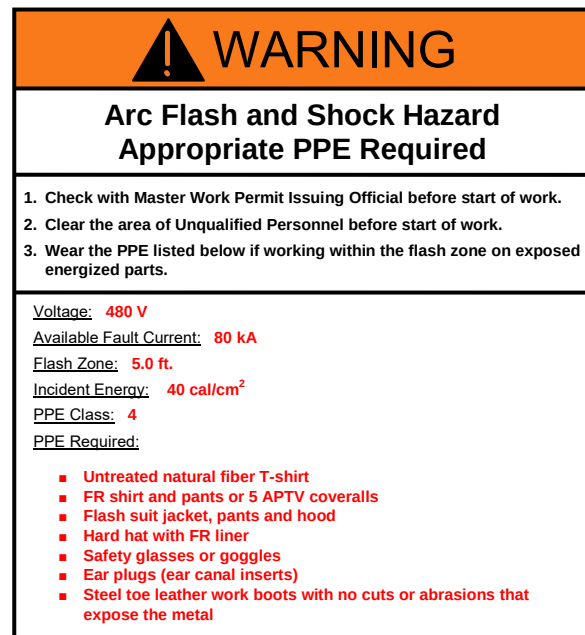


**Figure 9-51
Arc Flash Warning Label**

9.12 Ongoing Operations

9.12.1 Recommendations

Facility and maintenance operations are an integral part of any critical facility. Human error is the leading factor in outages and errors related to MTBF, and these errors also bear upon MTTR, the crux of availability. There are recognized best practice management frameworks that cover these in detail, but the following are some high-level recommendations:

- All work should be scripted and specific to the activity being undertaken, and all risks associated with such activity should be identified prior to performing the tasks.
- IT and facility operations should work collaboratively regardless of Class or business.
- Planned activities should include preventive and programmable maintenance, repair and replacement of components, addition or removal of capacity components, and testing of components and systems.
- Work on energized equipment should be eliminated whenever possible. Where such work is unavoidable, personnel should be trained, certified, authorized, and provided appropriate personal protective equipment.

9.13 Electrical Systems Matrix

Table 9-15 provides a summary of Section 9, *Electrical Systems*, with the items in the table presented in sequential order. Additional information has also been placed in the table that was not necessarily presented or explained in the preceding text. Readers are cautioned that some of the additions can include requirements where so indicated, and that Table 9-15 is to be used in conjunction with the text of Section 9.

Table 9-15 Electrical Systems Availability Classes

System/Class	Class F0	Class F1	Class F2	Class F3	Class F4
<i>9.1 (Electrical systems) Overview</i>					
Common industry description	Single path without any one of the following: alternate power source; UPS; proper ITE grounding	Single path	Redundant component/single path	Concurrently maintainable and operable	Fault tolerant
Number of power delivery paths to the critical load	One	One	One	Two, one active minimum with one passive/non-UPS power or one additional active	Two or more active
Redundant system components (e.g., UPS and generators)	No	No	Yes	Yes	Yes
Distinct UPS sources (e.g., A and B)	Optional/may not be present	Single or N	Single or N	Single or more, depending on the critical power topology	At least two resulting in a minimum of N + 2
System allows concurrent maintenance and operations	No	No	Within some systems with paralleled components, but not consistent throughout the electrical system.	Yes	Yes

Table continues on next page

<i>System/Class</i>	<i>Class F0</i>	<i>Class F1</i>	<i>Class F2</i>	<i>Class F3</i>	<i>Class F4</i>
System allows fault tolerance and self-healing failures?	No	No	No	Possible, depending on system configuration	Yes
Redundancy loss during maintenance or failure?	Yes. Redundancy is zero, so load loss or systems interruption would be expected.	Yes. Redundancy is zero, so load loss or systems interruption would be expected.	Yes for the power paths. Redundancy may exist in paralleled systems, and system topology may prevent load loss or interruption during routine maintenance or expected failures.	Yes, but the redundancy level reduced to N during maintenance or after a failure	No, but the redundancy level reduced to a level of >N during maintenance or after a failure.
Computer and telecommunications equipment power cords	Single- or dual-cord feed with no redundancy up to critical power system capacity. No ability to switch automatically between input sources via static switch-based PDU or panel.	Single- or dual-cord feed with no redundancy up to critical power system capacity. No ability to switch automatically between input sources via static switch-based PDU or panel.	Single- or dual-cord feed with no redundancy up to critical power system capacity. No ability to switch automatically between input sources via static switch-based PDU or panel.	Single-, dual- or poly-cord feed with either 100% capacity on each cord or adequate capacity on each cord mapped to the individual ITE system should a given source fail (i.e., 5 to make 6 or 2 to make 3 inputs).	Single-, dual- or poly-cord feed with either 100% capacity on each cord or adequate capacity on each cord mapped to the individual ITE system should a given source fail (i.e., 5 to make 6 or 2 to make 3 inputs).
Ability to add systems or components without interruption to existing loads	No	No	No	If planned during the initial design	Yes
Single points of failure	One or more	One or more	One or more	None	None
UPS redundancy	N or <N	N	A minimum of N+1	A minimum of N+1	Multiple N, 2N, 2N+1 or any configuration greater than N+1 that does not compromise redundancy during failure or maintenance modes of operation
UPS topology	Single module or parallel non-redundant system	Single module or parallel non-redundant modules	Parallel redundant modules or distributed redundant modules	Parallel redundant or distributed redundant or isolated redundant system	Parallel redundant or distributed redundant or isolated redundant system

Table continues on next page

System/Class	Class F0	Class F1	Class F2	Class F3	Class F4
9.2 Utility service					
Utility entrance	Single feed	Single feed	Single feed	One source with two inputs or one source with single input electrically diverse from backup generator input	One or more sources with two inputs. Dual feeds from different utility substations recommended
Multiple services	Not required	Not required	Optional – multiple services only based upon the service size	Optional – multiple services only based upon the service size	Recommended – multiple services based upon the service size
Service entrances physically separated	N/A	Optional	Optional	Recommended	Required
Location	Secured or unsecured	Secured or unsecured	Secured or unsecured	Secured	Secured
Underground or overhead	Underground or overhead	Underground or overhead	Underground or overhead	Underground (recommended)	Underground (required)
Concrete-encased for underground	Optional	Optional	Optional	Recommended	Recommended
9.2.2 Low voltage services					
Utility – generator transfer scheme	Typically not available	ATS or breaker	ATS or breaker	ATS or breaker	ATS or breaker
Main	80% rated	80% rated	80% rated	80 - 100% rated	100% rated
Data center loads served from	Non-dedicated switchboard	Main switchboard	Main switchboard	Dedicated subsystem	Dedicated subsystem
Location	Indoor or outdoor	Indoor or outdoor	Indoor	Indoor	Indoor
Rating	Series or fully rated	Series or fully rated	Fully rated	Fully rated	Fully rated
Construction	Switchboard	Switchboard	Switchboard	Switchboard or switchgear	Switchgear
Breaker types	Fixed or drawout	Static or drawout	Static or drawout	Drawout only	Drawout only
9.2.3 Medium voltage services					
Utility – generator transfer scheme	ATS or breaker if generator or alternate source is available	ATS or breaker	ATS or breaker	ATS or breaker	ATS or breaker
Main	100% rated	100% rated	100% rated	100% rated	100% rated
Data center loads served from	Main switchboard or non-dedicated switchboard	Main switchboard	Main switchboard	Dedicated subsystem	Dedicated subsystem
Location	Indoor or outdoor	Indoor or outdoor	Indoor	Indoor	Indoor
Rating	Fully rated	Fully rated	Fully rated	Fully rated	Fully rated

Table continues on next page

<i>System/Class</i>	<i>Class F0</i>	<i>Class F1</i>	<i>Class F2</i>	<i>Class F3</i>	<i>Class F4</i>
Construction	Switchboard or switchgear	Switchboard or switchgear	Switchboard or switchgear	Switchboard or switchgear	Switchgear
Breaker Types	Fixed-mount or drawout	Fixed-mount or drawout	Fixed-mount or drawout	Fixed-mount or drawout, depending on system redundancy	Fixed-mount or drawout, depending on system redundancy
<i>9.2.4 Protective relaying</i>					
Type	Commercial or utility grade	Commercial or utility grade	Commercial or utility grade	Commercial or utility grade	Utility grade
<i>9.3 Distribution</i>					
Cable terminations	Mechanical or compression lug	Mechanical or compression lug	Mechanical or compression lug	Mechanical or compression lug	Compression lug
Busway terminations (where used)	Locking washer	Locking washer	Locking washer	Locking or Belleville washer	Locking or Belleville washer
Busway treatment (where used)	Tinned joints optional	Tinned joints optional	Tinned joints optional	Tinned joints optional	Tinned joints recommended
<i>9.3.7 Utility/generator transfer control and generator paralleling switchgear</i>					
Transfer system	Automatic transfer switch or interlocked circuit breakers, if generator present	Automatic transfer switch or interlocked circuit breakers	Automatic transfer switch or interlocked circuit breakers	Automatic transfer switch or interlocked circuit breakers	Automatic transfer switch or interlocked circuit breakers
Critical load system transfer	Automatic or manual transfer if a generator is present. Maintenance bypass optional. UPS power system may be optional.	Automatic transfer with maintenance bypass feature for serving the switch with interruption in power; automatic changeover from utility to generator when a power outage occurs.	Automatic transfer with maintenance bypass feature for serving the switch with interruption in power; automatic changeover from utility to generator when a power outage occurs.	Automatic transfer with maintenance bypass feature for serving the switch with interruption in power; automatic changeover from utility to generator when a power outage occurs.	Automatic transfer with maintenance bypass feature for serving the switch with interruption in power; automatic changeover from utility to generator when a power outage occurs.
Transfer type	Open or closed transition	Open or closed transition	Open or closed transition	Open or closed transition	Open or closed transition
Transfer and control points	One for the whole critical load.	One for whole critical load	Multiple ATSS or 2N on the utility	One for each UPS system; one for each mechanical branch and one for the non-critical load or common loads	One for each UPS system; one for each mechanical branch and one for the non-critical load or common loads
UPS	One, combined with all loads if generator present	One for whole critical load	Dedicated to UPS	Dedicated to UPS path	Dedicated to UPS path
Mechanical	One, combined with all loads if generator present	One for whole critical load	Dedicated to mechanical	Dedicated to each mechanical path	Dedicated to each mechanical path

Table continues on next page

System/Class	Class F0	Class F1	Class F2	Class F3	Class F4
Non-critical load	One, combined with all loads if generator present	One for whole critical load	Dedicated to non-critical load	Dedicated to non-critical load	Dedicated to non-critical load, maintain diversity of system
Generator control switchgear	If needed	If needed	If needed	If needed	If needed
Location	Indoor or outdoor	Indoor or outdoor	Indoor	Indoor	Indoor
Rating	Fully rated	Fully rated	Fully rated	Fully rated	Fully rated
Construction	Switchboard or switchgear	Switchboard or switchgear	Switchboard or switchgear	Switchboard or switchgear	Switchgear
Breaker types	Fixed-mount or drawout	Fixed-mount or drawout	Fixed-mount or drawout	Fixed-mount, with drawout preferred	Drawout only
Controls	Single/Stand-Alone	Single/Stand-Alone	Single or Redundant	Redundant	Redundant
Relay type	Commercial grade	Commercial grade	Commercial or industrial grade	Commercial or industrial grade	Industrial grade
9.3.8 Unit substations					
Transformer MV primary protection	Fused or breakers, depending on utility	Fused or breakers, depending on utility	Fused or breakers, depending on utility	Fused or breakers, depending on utility	Fused or breakers, depending on utility
Transformer specification	High-flash point oil, air or cast core	High-flash point oil, air or cast core	High-flash point oil, air or cast core	High-flash point oil, air or cast core	High-flash point oil, air or cast core
Rating	Fully rated	Fully rated	Fully rated	Fully rated	Fully rated
Construction	Switchboard or switchgear	Switchboard or switchgear	Switchboard or switchgear	Switchboard or switchgear	Switchgear
Breaker Types	Fixed-mount or drawout	Fixed-mount or drawout	Fixed-mount or drawout	Fixed-mount, with drawout preferred	Drawout only
Controls	Single/Stand-Alone	Single/Stand-Alone	Single or Redundant	Redundant	Redundant
9.3.9 UPS					
UPS Maintenance Bypass Arrangement	Optional	UPS module, static switch and maintenance bypass from same switchboard	UPS module, static switch and maintenance bypass from same switchboard	UPS module may be fed from opposite system for redundancy. Alternatively, the downstream critical load being served may be provided from a separate and redundant UPS power system and path. This redundant path may be connected upstream at an ASTS or at the load itself via multiple power cords	UPS module may be fed from opposite system for redundancy. Alternatively, the downstream critical load being served may be provided from a separate and redundant UPS power system and path. This redundant path may be connected upstream at an ASTS or at the load itself via multiple power cords

Table continues on next page

<i>System/Class</i>	<i>Class F0</i>	<i>Class F1</i>	<i>Class F2</i>	<i>Class F3</i>	<i>Class F4</i>
UPS power distribution – panelboards	Panelboard incorporating standard thermal magnetic trip breakers if UPS present.	Panelboard incorporating standard thermal magnetic trip breakers	Panelboard incorporating standard thermal magnetic trip breakers	Panelboard incorporating standard thermal magnetic trip breakers	Panelboard incorporating standard thermal magnetic trip breakers
Method of distribution to computer and telecommunications equipment	PDU or individual panelboards if UPS present.	PDU or individual panelboards	PDU or individual panelboards	PDU	PDU
Multi-system UPS power system synchronization	N/A	N/A	Optional	Optional. May be via static inputs or an external control system.	Optional. May be via static inputs or an external control system.
UPS power system segregated from mechanical or support loads	N/A	Optional	Recommended	Recommended	Recommended
External maintenance bypass	Optional	Recommended	Recommended	Recommended	Recommended
9.3.10 Critical distribution switchboards					
Location	Indoor	Indoor	Indoor	Indoor	Indoor
Rating	80% - 100% rated	80% - 100% rated	80% - 100% rated	80% - 100% rated	Fully rated
Construction	Switchboard or switchgear	Switchboard or switchgear	Switchboard or switchgear	Switchboard or switchgear	Switchgear
Breaker Types	Fixed-mount or drawout	Fixed-mount or drawout	Fixed-mount or drawout	Drawout only	Drawout only
Controls	Single/Stand-Alone	Single/Stand-Alone	Single or redundant	Redundant	Redundant
9.3.11 Power distribution units					
Inputs	Single	Single	Single or dual	Single or dual	Single or dual
Transformer K-rating	K-rated, depending on load or application	K-rated, depending on load or application	K-rated, depending on load or application	K-rated, depending on load or application	K-rated, depending on load or application
Location	In computer room, service gallery (subject to AHJ approval), or electrical room	In computer room, service gallery (subject to AHJ approval), or electrical room	In computer room or service gallery (subject to AHJ approval)	In computer room or service gallery (subject to AHJ approval)	In computer room or service gallery (subject to AHJ approval)
Rating	Continuous duty	Continuous duty	Continuous duty	Continuous duty	Continuous duty
Breaker Types	Fixed-mounted	Fixed-mounted	Fixed-mounted	Fixed-mounted	Fixed-mounted
Controls	Stand-alone	Stand-alone	Stand-alone	Stand-alone	Stand-alone

Table continues on next page

System/Class	Class F0	Class F1	Class F2	Class F3	Class F4
9.3.12 Static transfer switches					
Use of STS	Critical load switching when alternate source is available	Critical load switching when alternate source is available	Critical load switching when alternate source is available	Critical load switching	Critical load switching
Configuration	Primary or secondary	Primary or secondary	Primary or secondary	Primary or secondary	Primary or secondary
Inputs	Two	Two	Two	Two or three	Two or three
Location	In computer room, service gallery, or electrical room	In computer room or service gallery	In computer room or service gallery	In computer room or service gallery	In computer room or service gallery
Rating	Continuous duty	Continuous Duty	Continuous duty	Continuous duty	Continuous duty
Short circuit tolerance	Fused or unfused short circuit protection integrated to internal circuit breakers	Fused or unfused short circuit protection integrated to internal circuit breakers	Circuit breaker protection for short circuits	Circuit breaker protection for short circuits or ability to transfer from a shorted bus	Type 3 circuit breaker protection for short circuits or ability to transfer from a shorted bus
Breaker Types	Fixed-mounted	Fixed-mounted	Fixed-mounted	Fixed-mounted	Fixed-mounted
Controls	Stand-alone	Stand-alone	Stand-alone	Stand-alone	Stand-alone
9.3.14 Computer room equipment power distribution					
Individual circuits in separate conduits or cables	Optional	Optional	Recommended	Recommended	Recommended
Receptacles labeled with individual circuit	Optional	Optional	Recommended	Recommended	Recommended
Color-coded conduit and junction boxes per upstream UPS source	Optional	Optional	Recommended	Recommended	Recommended
Twist-lock receptacles for equipment or power strips	Optional	Optional	Recommended	Recommended	Recommended
Circuits mapped to UPS plant capacity/redundancy	Yes, if UPS power system present	Recommended	Recommended	Recommended	Recommended
9.3.15 Emergency power off (EPO) systems					
Computer room EPO system					
Single Step system	Optional	Optional	Not recommended	Not recommended	Not recommended
3 state system – off/test/armed	Optional	Optional	Not recommended unless mandated by code	Not recommended unless mandated by code	Not recommended unless mandated by code

Table continues on next page

<i>System/Class</i>	<i>Class F0</i>	<i>Class F1</i>	<i>Class F2</i>	<i>Class F3</i>	<i>Class F4</i>
CCTV Camera on EPO Station	Optional	Optional	Optional	Optional	Recommended
Shutdown of UPS power receptacles in computer room area pursuant to Code	According to local jurisdiction	According to local jurisdiction	According to local jurisdiction	According to local jurisdiction	According to local jurisdiction
Shutdown of AC power for cooling equipment in room	According to local jurisdiction	According to local jurisdiction	According to local jurisdiction	According to local jurisdiction	According to local jurisdiction
Compliance with local code (e.g., separate systems for UPS and HVAC)?	According to local jurisdiction	According to local jurisdiction	According to local jurisdiction	According to local jurisdiction	According to local jurisdiction
Ability to safely turn off fire alarm connection for maintenance	Recommended	Recommended	Recommended	Recommended	Recommended
When present, automatically activate EPO when fire suppressant is released	According to local jurisdiction	According to local jurisdiction	According to local jurisdiction	According to local jurisdiction	According to local jurisdiction
Fire suppressant release for single zone system after emergency power off (EPO) shutdown	According to local jurisdiction	According to local jurisdiction	According to local jurisdiction	According to local jurisdiction	According to local jurisdiction
Second zone fire alarm system activation. Sounds pre-release on first zone with suppressant release and EPO on the second zone	Optional	Optional	Optional	Recommended	Recommended
Delay to EPO activation after button push	Optional	Optional	Optional	Optional	Optional
EPO override switch (keyed or non-keyed)	Optional	Optional	Optional	Optional	Optional
EPO activation countdown timer	Optional	Optional	Optional	Optional	Optional
Whole building EPO	According to local jurisdiction	According to local jurisdiction	According to local jurisdiction	According to local jurisdiction	According to local jurisdiction

Table continues on next page

System/Class	Class F0	Class F1	Class F2	Class F3	Class F4
9.4 Mechanical equipment support					
9.4.3.2 Chillers					
Feeds	Single	Single	Single	Single or dual, depending on mechanical plant redundancy	Single or dual, depending on mechanical plant redundancy
Source Selection	Not required	Not required	Not required	Manual or automatic	Manual or automatic
Source Mapping	N - single path	N - single path	Mapped to mechanical redundancy. Dual input will require internal or external transfer switch.	Mapped to mechanical redundancy. Dual input will require internal or external transfer switch.	Mapped to mechanical redundancy. Dual input will require internal or external transfer switch.
9.4.3.2 Cooling towers					
Feeds	Single	Single	Single	Single or dual, depending on mechanical plant redundancy	Single or dual, depending on mechanical plant redundancy
Source Selection	None	None	None	Manual or automatic	Manual or automatic
Source Mapping	N - single path	N - single path	Mapped to mechanical redundancy. Dual input will require internal or external transfer switch.	Mapped to mechanical redundancy. Dual input will require internal or external transfer switch.	Mapped to mechanical redundancy. Dual input will require internal or external transfer switch.
9.4.3.3 Pumps					
Feeds	Single	Single	Single	Single or dual, depending on mechanical plant redundancy	Single or dual, depending on mechanical plant redundancy
Source Selection	None	None	None	Manual or automatic	Manual or automatic
Source Mapping	N - single path	N - single path	Mapped to mechanical redundancy. Dual input will require internal or external transfer switch.	Mapped to mechanical redundancy. Dual input will require internal or external transfer switch.	Mapped to mechanical redundancy. Dual input will require internal or external transfer switch.

Table continues on next page

<i>System/Class</i>	<i>Class F0</i>	<i>Class F1</i>	<i>Class F2</i>	<i>Class F3</i>	<i>Class F4</i>
9.4.3.4 Air handling systems					
Feeds	Single	Single	Single	Single or dual, depending on mechanical plant redundancy	Single or dual, depending on mechanical plant redundancy
Source Selection	None	None	None	Manual or automatic	Manual or automatic
Source Mapping	N - single path	N - single path	Mapped to mechanical redundancy. Dual input will require internal or external transfer switch.	Mapped to mechanical redundancy. Dual input will require internal or external transfer switch.	Mapped to mechanical redundancy. Dual input will require internal or external transfer switch.
9.4.3.5 Humidification					
Feeds	Single	Single	Single	Single or dual, depending on mechanical plant redundancy	Single or dual, depending on mechanical plant redundancy
Source Selection	None	None	None	Manual or automatic	Manual or automatic
Source Mapping	N - single path	N - single path	Mapped to mechanical redundancy. Dual input will require internal or external transfer switch.	Mapped to mechanical redundancy. Dual input will require internal or external transfer switch.	Mapped to mechanical redundancy. Dual input will require internal or external transfer switch.
9.5 UPS					
Use of UPS	Optional	Required	Required	Required	Required
9.5.3.3.2 Static UPS					
Sizing	Either not present, or rated at <N for the connected critical load	To kW rating of the load with system designer's safety factor	To kW rating of the load with system designer's safety factor	To kW rating of the load with system designer's safety factor	To kW rating of the load with system designer's safety factor
9.5.3.3.3 and 9.5.3.3.4 Rotary and hybrid UPS					
Sizing	Either not present or rated at <N for the connected critical load	To kW rating of the load with system designer's safety factor	To kW rating of the load with system designer's safety factor	To kW rating of the load with system designer's safety factor	To kW rating of the load with system designer's safety factor
9.5.4 Paralleling and controls					
Static switch duty type	Momentary, if present	Momentary	Momentary or continuous	Continuous	Continuous
External Synch	N/A	N/A	By design	By design or active control	By design or active control

Table continues on next page

System/Class	Class F0	Class F1	Class F2	Class F3	Class F4
9.5.5 Batteries and stored energy					
Flywheel or battery	Either	Either	Either	Either	Either
Sizing	kW	kW	kW	kW	kW
Spill containment	By code	By code	By code	By code	By code
Monitoring interface with BMS	Optional	Optional	Optional	Recommended	Recommended
One or more battery strings per module	Optional	Optional	Recommended	Recommended	Recommended
Minimum full load standby time	Minimum safe time to transfer to and from generator within the capabilities of the energy storage device. Longer time optional.	Minimum safe time to transfer to and from generator within the capabilities of the energy storage device. Longer time optional.	Minimum safe time to transfer to and from generator within the capabilities of the energy storage device. Longer time optional.	Minimum safe time to transfer to and from generator within the capabilities of the energy storage device. Longer time optional.	Minimum safe time to transfer to and from generator within the capabilities of the energy storage device. Longer time optional.
Battery full load testing/inspection schedule	Every two years or as recommended by manufacturer	Every two years or as recommended by manufacturer	Every two years or as recommended by manufacturer	Every two years or as recommended by manufacturer	Every two years or as recommended by manufacturer
Batteries separate from UPS/switchgear equipment rooms	Optional, depending on battery type and size of system	Optional, depending on battery type and size of system	Optional, depending on battery type and size of system	Recommended	Recommended
Battery monitoring system	UPS self monitoring if UPS power system present	UPS self monitoring	UPS self monitoring	Recommended (ohmic readings are less reliable for large vented lead-acid batteries)	Recommended (ohmic readings are less reliable for large vented lead-acid batteries)
9.6 Standby power systems					
Generator or assured alternate power source utilized	Optional	Required	Required	Required	Required
Fuel run time	No requirement	Based on disaster plan; 8 hrs recommended	Based on disaster plan; 24 hrs recommended	Based on disaster plan; 72 hrs recommended	Based on disaster plan; 96 hrs recommended
Rating	No requirement	kW load only	kW load only	kW load only	kW load only
Load Supported	No requirement	All loads	All loads	All loads	All loads
Installation	No requirement	Outdoor or indoor	Outdoor or indoor	Recommended indoor	Recommended indoor
Redundancy	No requirement	N	N N+1 or generate tap box recommended	N+1	Greater than N+1
Bearing Sensors	No requirement	No	No	Optional	Recommended

Table continues on next page

System/Class		Class F0	Class F1	Class F2	Class F3	Class F4
9.6.2 Starting systems						
	Start time delay (maximum for 1st generator on and load transferred)	No recommended time in excess of AHJ requirements	10 second or as required by AHJ	10 second or as required by AHJ	10 second or as required by AHJ	10 second or as required by AHJ
	Maximum load assumption time (all loads)	No recommended time in excess of AHJ requirements	3 min	2 min or as required by AHJ	1 min or as required by AHJ	1 min or as required by AHJ
	Battery capacity	N	N	N	2N/independent	2N/independent
	Starter count	N	N	N	2N	2N
	Best battery selection system	Optional	Optional	Optional	Recommended	Recommended
9.6.3 Fuel systems						
Fuel filters	Grade	Standard	Standard	Standard	Marine	Marine with fuel/water separator
	100 micron	Recommended	Recommended	Recommended	Recommended	Recommended
	30 micron	Optional	Optional	Optional	Recommended	Recommended
	10 micron	Optional	Optional	Optional	Optional	Recommended
	Spin-on/off while operating	Optional	Optional	Optional	Recommended	Recommended
Fuel polish		Optional	Optional	Optional	Recommended	Recommended
Fuel additive/treatment		Optional	Optional	Optional	Recommended	Recommended
Fuel line type		Standard	Standard	Standard	Marine/Braided Steel	Marine/Braided Steel
9.6.5 Exhaust systems						
Sound rating		As required by the local jurisdiction	As required by the local jurisdiction	As required by the local jurisdiction	As required by the local jurisdiction	As required by the local jurisdiction
Air quality		As required by the local jurisdiction	As required by the local jurisdiction	As required by the local jurisdiction	As required by the local jurisdiction	As required by the local jurisdiction
Pollution abatement		As required by the local jurisdiction	As required by the local jurisdiction	As required by the local jurisdiction	As required by the local jurisdiction	As required by the local jurisdiction
Exhaust piping		Welded	Welded	Welded	Welded	Welded
Connections to engine		Steel and flexible	Steel and flexible	Steel and flexible	Steel and flexible	Steel and flexible

Table continues on next page

<i>System/Class</i>	<i>Class F0</i>	<i>Class F1</i>	<i>Class F2</i>	<i>Class F3</i>	<i>Class F4</i>
9.6.6 Cooling systems					
Rating	Match engine rating for continuous, standby or prime rating	Match engine rating for continuous, standby or prime rating	Match engine rating for continuous, standby or prime rating	Match engine rating and ASHRAE (or local equivalent) extreme temperature published for the project location	Match engine rating and ASHRAE (or local equivalent) extreme temperature published for the project location
9.6.2 – 9.6.6 Monitoring and controls					
Controls	Onboard generator	Onboard generator	Onboard generator or centralized if paralleled	Onboard generator or centralized if paralleled	Onboard generator or centralized if paralleled
Pre-Alarm Conditions Reported	No	No	Yes, summary only	Yes, by point	Yes, by point
Alarm Conditions Reported	Yes, summary only	Yes, summary only	Yes, summary only	Recommended by point	Recommended by point
Trouble Conditions Reported	Yes, summary only	Yes, summary only	Yes, summary only	Yes, by point	Yes, by point
9.6.7 Mounting					
Mounting	Pursuant to AHJ requirements	Pursuant to AHJ requirements	Pursuant to AHJ requirements	Pursuant to AHJ requirements	Pursuant to AHJ requirements
9.7 Automation and control					
9.7.2 Monitoring					
Summary alarm and trouble alerts	Optional	Optional	Recommended	Recommended	Recommended
Dynamic/real time single line	Optional	Optional	Optional	Optional	Recommended
Operations simulator	Optional	Optional	Optional	Recommended	Recommended
Utility bus/buses	Optional	Optional	Optional	Recommended	Recommended
Generator bus/buses	Recommended	Recommended	Recommended	Recommended	Recommended
Generators	Recommended	Recommended	Recommended	Recommended	Recommended
Non-critical and mechanical power systems	Optional	Optional	Optional	Recommended	Recommended
UPS output bus	Optional	Optional	Recommended	Recommended	Recommended
UPS modules	Optional	Optional	Recommended	Recommended	Recommended
Batteries/stored energy system	Optional	Optional	Recommended	Recommended	Recommended
PDU's	Optional	Optional	Recommended	Recommended	Recommended

Table continues on next page

<i>System/Class</i>	<i>Class F0</i>	<i>Class F1</i>	<i>Class F2</i>	<i>Class F3</i>	<i>Class F4</i>
Collector bus or static bypass cabinet	Optional	Optional	Recommended	Recommended	Recommended
Branch circuit distribution	Optional	Optional	Optional	Recommended	Recommended
EPO system (when present)	Optional	Optional	Recommended	Recommended	Recommended
Fire alarm system	Recommended	Recommended	Recommended	Recommended	Recommended
Power quality	Optional	Optional	Recommended on the UPS output, optional on other portions of the system	Recommended only on the utility, generators and UPS output, optional on other portions of the system	Recommended throughout
Database for alarm and trouble signals	Optional	Optional	Optional	Recommended	Recommended
Power quality monitoring	Optional	Optional	Recommended	Recommended	Recommended
Utility	Optional	Optional	Optional	Recommended	Recommended
Generator	Optional	Optional	Optional	Optional	Recommended
UPS output bus	Optional	Optional	Recommended	Recommended	Recommended
PDU	Optional	Optional	Optional	Optional	Recommended
<i>9.7.3 Power control</i>					
Controls clearly indicated and posted	Recommended, if present	Recommended, if present	Recommended	Recommended	Recommended
<i>9.7.4 System integration</i>					
Integrated electrical system monitoring	Optional	Optional	Optional	Recommended	Recommended
Electrical monitoring integrated to overall system	Optional	Optional	Optional	Recommended	Recommended
Electrical monitoring integrated to IT management system	Optional	Optional	Optional	Recommended	Recommended

Table continues on next page

System/Class	Class F0	Class F1	Class F2	Class F3	Class F4
9.8 Lighting					
9.8.3 Computer rooms					
Level	500 lux	500 lux	500 lux	500 lux	500 lux
Uniformity	>90%	>90%	>90%	>90%	>90%
Control	Local, manual or occupancy sensors	Local, manual or occupancy sensors	Local, manual or occupancy sensors	Local, manual or occupancy sensors	Local, manual or occupancy sensors
Emergency	Instant-on battery packs for safety and a minimum of 50% room coverage at 5 foot-candles	Instant-on battery packs for safety and a minimum of 50% room coverage at 5 foot-candles	Instant-on battery packs for safety and a minimum of 50% room coverage at 5 foot-candles	Instant-on battery packs for 100% room coverage at 5 foot-candles	Instant-on battery packs for 100% room coverage at 5 foot-candles
9.8.4 Support areas					
Level	As required by IES	As required by IES	As required by IES	As required by IES	As required by IES
Uniformity	>90%	>90%	>90%	>90%	>90%
Control	Local, manual or occupancy sensors	Local, manual or occupancy sensors	Local, manual or occupancy sensors	Local, manual or occupancy sensors	Local, manual or occupancy sensors
Exterior areas	Lighting sufficient for working at night and in inclement weather as well as for security	Lighting sufficient for working at night and in inclement weather as well as for security	Lighting sufficient for working at night and in inclement weather as well as for security	Lighting sufficient for working at night and in inclement weather as well as for security	Lighting sufficient for working at night and in inclement weather as well as for security
Emergency	Instant-on battery packs for safety and a minimum of 50% room coverage at 5 foot-candles	Instant-on battery packs for safety and a minimum of 50% room coverage at 5 foot-candles	Instant-on battery packs for safety and a minimum of 50% room coverage at 5 foot-candles	Instant-on battery packs for 100% room coverage at 5 foot-candles	Instant-on battery packs for 100% room coverage at 5 foot-candles
9.9 Bonding and grounding					
Grounding resistance	If 5 ohm or greater, may not conform to IEEE or BICSI	5 ohm or less, conforming to IEEE and BICSI	5 ohm or less, conforming to IEEE and BICSI. 3 ohms recommended	5 ohm or less, conforming to IEEE and BICSI. 1 ohm recommended	5 ohm or less, conforming to IEEE and BICSI. 1 ohm recommended
Electrical distribution grounding					
Lighting fixtures (277 V) neutral isolated from service entrance derived from lighting transformer for ground fault isolation	Optional	Optional	Optional	Recommended	Recommended
Building electrical main grounding busbar	Optional	Recommended	Required	Required	Required

Table continues on next page

<i>System/Class</i>	<i>Class F0</i>	<i>Class F1</i>	<i>Class F2</i>	<i>Class F3</i>	<i>Class F4</i>
Ground wires in all feeders and branch circuits (Grounding conductors shall be carried in all power system raceways)	Recommended	Recommended	Required	Required	Required
Grounding method	Solidly grounded or impedance grounded	Solidly grounded or impedance grounded	Solidly grounded or impedance grounded	Solidly grounded or impedance grounded	Solidly grounded or impedance grounded
<i>Critical power system grounding</i>					
mesh-BN, mesh-IBN, or combination thereof in computer room	Recommended	Recommended	Required	Required	Required
Lightning protection system	Based on risk analysis as per NFPA 780	Based on risk analysis as per NFPA 780	Based on risk analysis as per NFPA 780	Based on risk analysis as per NFPA 780	Based on risk analysis as per NFPA 780
Lightning detection system	Optional	Optional	Optional	Recommended for areas subject to lightning	Recommended for areas subject to lightning
Online weather system on site	Optional	Optional	Optional	For areas subject to lightning	Recommended
<i>9.9.4 Surge protective devices (SPDs)</i>					
Present	Optional	Recommended	Recommended	Recommended	Recommended
Utility entrance(s)	Recommended	Recommended	Recommended	Recommended	Recommended
Distribution panel/below source transfer or ATS	Optional	Recommended	Recommended	Recommended	Recommended
UPS input	Optional	No, unless recommended by UPS manufacturer	No, unless recommended by UPS manufacturer	No, unless recommended by UPS manufacturer	No, unless recommended by UPS manufacturer
UPS output	Optional	Optional	Optional	Recommended	Recommended
PDUs/panels	Optional	Optional	Optional	Optional	Optional
<i>9.10 Labeling and Signage</i>					
Hazard signage installed	Required	Required	Required	Required	Required
Instructions posted	Required	Required	Required	Required	Required
Safety data sheets posted or in library	Required	Required	Required	Required	Required
All equipment labeled	Required	Required	Required	Required	Required
Equipment color coded	Optional	Optional	Recommended	Recommended	Recommended

Table continues on next page

<i>System/Class</i>	<i>Class F0</i>	<i>Class F1</i>	<i>Class F2</i>	<i>Class F3</i>	<i>Class F4</i>
Single line diagrams posted	Optional	Optional	Optional	Recommended	Recommended
All electrical systems tested prior to operation	Optional	Required	Required	Required	Required
All electrical system equipment labeled with certification (from 3rd party test laboratory if available)	Optional	Required	Required	Required	Required
9.11 System Start Up and Commissioning					
Equipment subject to in-factory testing prior to project delivery – Level 1 Commissioning	Optional	Optional	Optional	Recommended	Recommended
Pre-functional start-up by manufacturer – Level 2 Commissioning	Recommended	Recommended	Recommended	Recommended	Recommended
Equipment functional testing – Level 3 Commissioning	Optional	Optional	Recommended	Recommended	Recommended
System functional – Level 4 Commissioning	Optional	Optional	Recommended	Recommended	Recommended
Electrical system testing – Level 4 Commissioning	Optional	Optional	Optional	Recommended	Recommended
Whole building testing – Level 5 Commissioning	Optional	Optional	Optional	Optional	Recommended

Table continues on next page

<i>System/Class</i>	<i>Class F0</i>	<i>Class F1</i>	<i>Class F2</i>	<i>Class F3</i>	<i>Class F4</i>
9.12 Critical Facility Operations and Maintenance					
Change control/change management	Optional/likely not present	Optional/likely not present	Present/not integrated with IT	Present/coordinate with IT	Present/integrated with IT
Work rules	Not scripted	Not scripted	Scripted	Scripted	Scripted/back check
Maintenance staff	Onsite day shift only. On call at other times	Onsite day shift only. On call at other times	Onsite day shift only. On call at other times	Onsite 24 hrs M-F, on call on weekends	Onsite 24/7
Preventative maintenance	Optional	Recommended	Recommended	Limited preventative maintenance program	Comprehensive preventative maintenance program
Facility training programs	Optional	Recommended	Recommended	Comprehensive training program	Comprehensive training program including manual operation procedures if it is necessary to bypass control system

This page intentionally left blank

10 Mechanical

10.1 Codes, References and Terminology

10.1.1 Code Compliance and Coordination

Local building codes shall be consulted in the planning and implementation of changes to the building, mechanical, electrical, and life safety systems. Codes that are commonly enforced globally include:

- *International Building Code (IBC)*
- *International Mechanical Code (IMC)*
- *International Plumbing Code (IPC)*
- *International Fuel Gas Code (IFGC)*

The IMC establishes specific requirements for ventilation rates, in coordination with ASHRAE 62.1, and specifies battery room exhaust requirements.

State and local adoption of international or uniform codes is often done by incorporation into the state building code with amendments to specific sections. As the scope of amendments may be significant, local amendments shall be checked before making decisions based on code requirements.

10.1.2 References

Within Section 10, references to the following documents are listed as follows in Table 10-1. The notation used for standards (e.g., NFPA 70) remains unchanged.

Table 10-1 Section 10 Text References

<i>Text Reference</i>	<i>Complete Document Title</i>
<i>ASHRAE Thermal Guidelines</i>	<i>ASHRAE: Thermal Guidelines for Data Processing Environments, Third Edition</i>
<i>ASHRAE Design Considerations</i>	<i>ASHRAE: Design Considerations for Datacom Equipment Centers, Second Edition</i>
<i>ASHRAE Environmental Guidelines</i>	<i>2011 ASHRAE TC 9.9, Environmental Guidelines for Datacom Equipment - Expanding the Recommended Environmental Envelope</i>

10.1.3 Terminology Differences Between Codes and Telecommunications Standards

Terminology used in building codes and by building code officials may differ from terms commonly used in the computer and telecommunications industry. For example, codes use the term “equipment room” to describe rooms housing mechanical or electrical equipment such as air handlers, pumps, chillers, transformers, and switchgear. However, *ASHRAE Thermal Guidelines* defines equipment such as servers, storage products, and PCs.

10.2 Typical Heat Rejection and Computer Room Cooling Technologies

10.2.1 Introduction

Common heat rejection and cooling systems are presented with general characteristics and illustrations.

10.2.2 Chiller Based Systems

10.2.2.1 Introduction

Any combination of the following chiller-based heat rejection systems and computer room cooling systems may be implemented within the computer room cooling design.

10.2.2.2 Heat Rejection Systems**10.2.2.2.1 Evaporative Condenser Heat Rejection System**

Heat Rejection: Evaporative cooling (cooling tower)

Primary Cooling Circuit: Water

Heat Exchanger: Indoor chiller

Secondary Cooling Circuit: Water

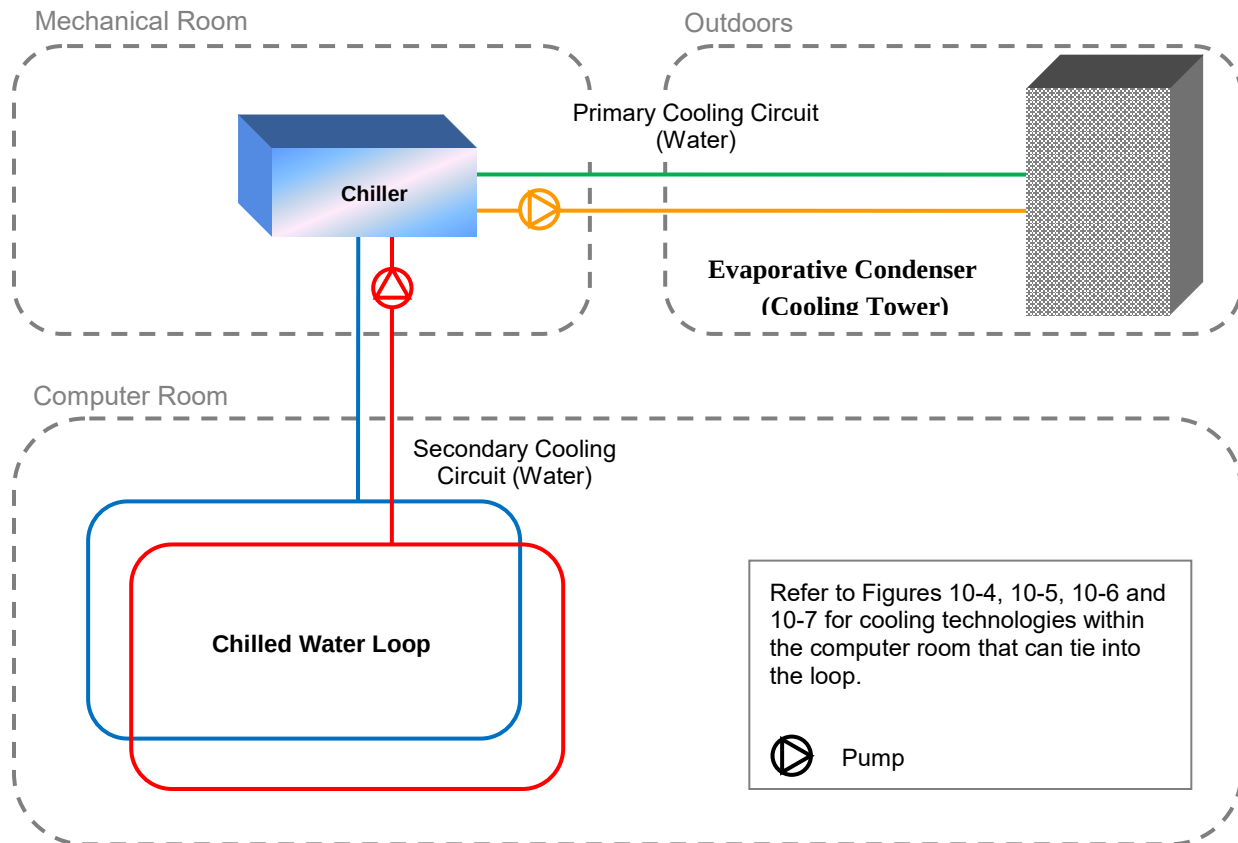


Figure 10-1
Evaporative Condenser Heat Rejection System

10.2.2.2.2 Air-Cooled Condenser Heat Rejection System

Heat Rejection: Air-cooled condenser (dry-cooler)

Primary Cooling Circuit: Glycol

Heat Exchanger: Indoor chiller

Secondary Cooling Circuit: Glycol

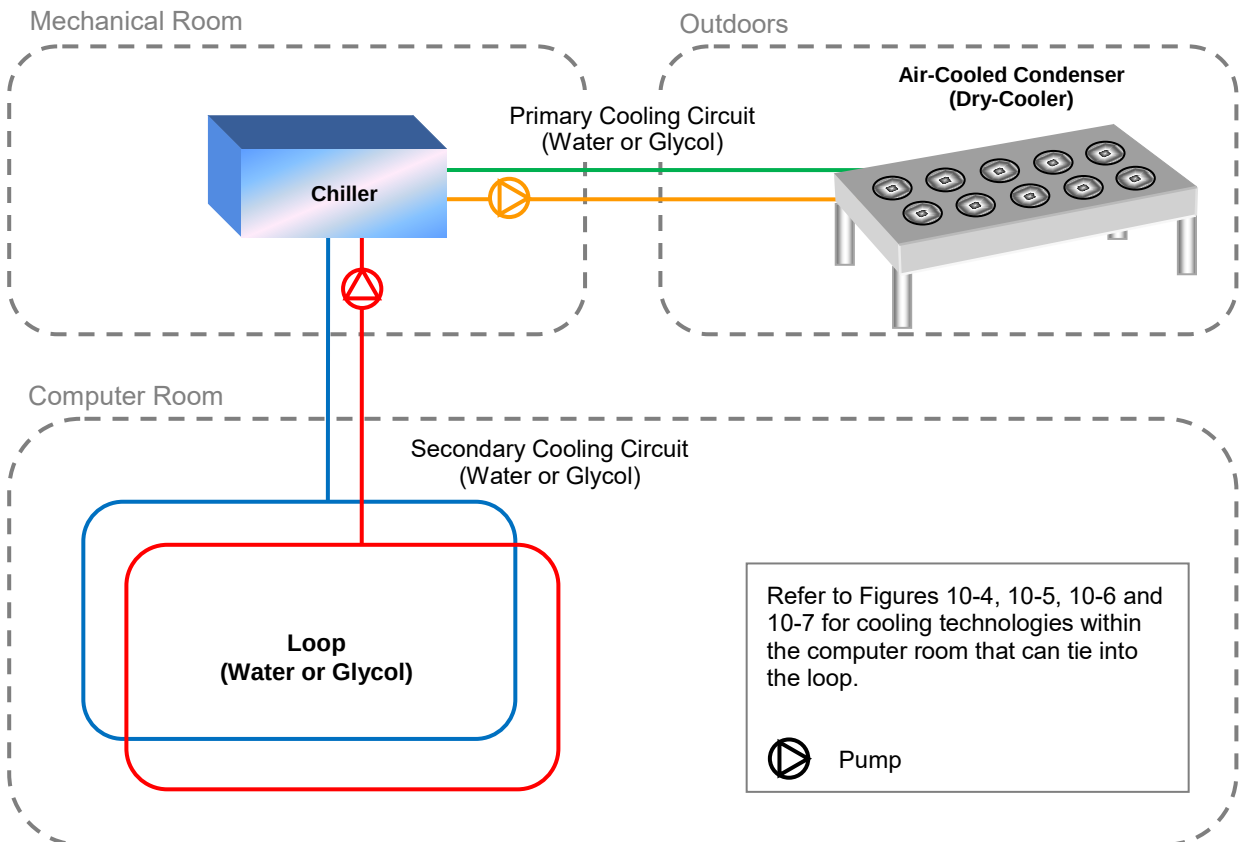


Figure 10-2
Air-Cooled Condenser Heat Rejection System

10.2.2.2.3 Air-Cooled Chiller Heat Rejection System

Heat Rejection:	Air-Cooled
Primary Cooling Circuit:	Integral to packaged outdoor chiller
Heat Exchanger:	Packaged outdoor air-cooled chiller
Secondary Cooling Circuit:	Glycol

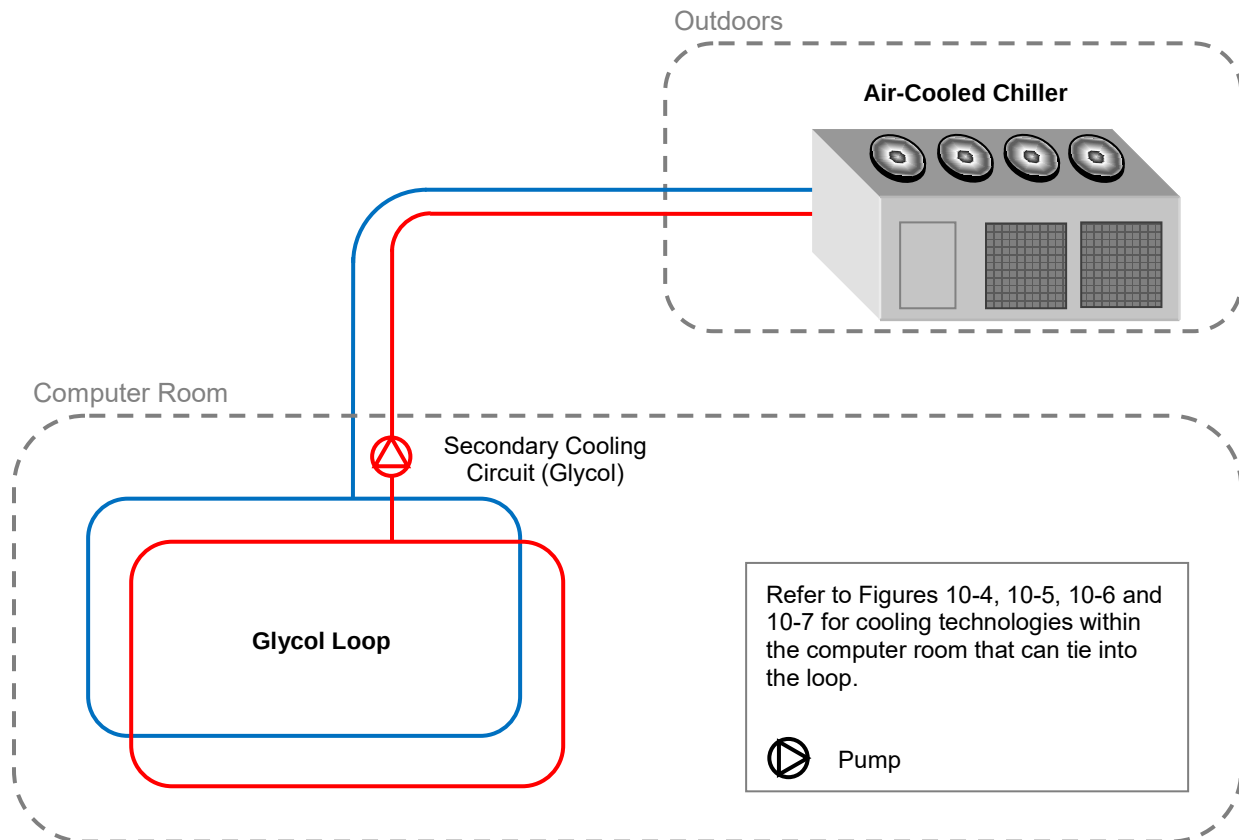


Figure 10-3
Air-Cooled Chiller Heat Rejection System

10.2.2.3 Computer Room Cooling Systems

10.2.2.3.1 Computer Room Air Handler Cooling System

Secondary Cooling Circuit:	Water for chiller utilizing evaporative cooling Glycol for outdoor chiller or chiller utilizing air-cooled condenser
Cooling Circuit:	CRAH
ITE Cooling Circuit	Air Distribution with underfloor supply and open room return, ducted supply, ducted return, or vertical heat collars above cabinets up to plenum return
ITE Heat Rejection:	Air cooled heat sink

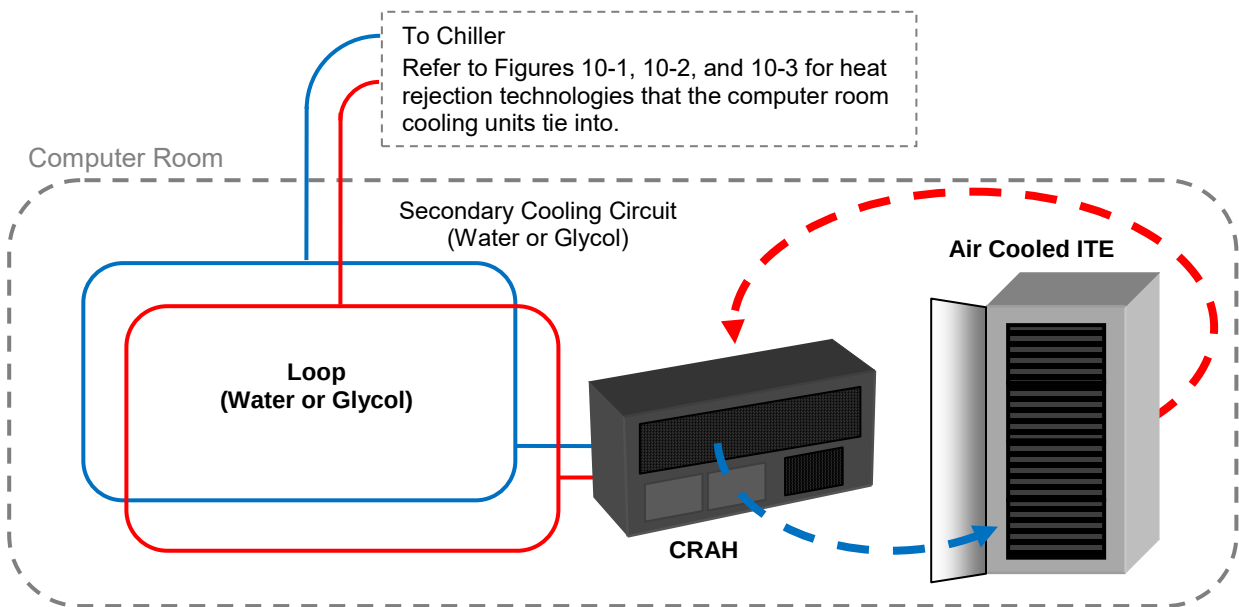


Figure 10-4
Computer Room Air Handler Cooling System

10.2.2.3.2 Liquid Cooling ITE Cooling System

Secondary Cooling Circuit:	Water for chiller utilizing evaporative cooling Glycol for outdoor chiller or chiller utilizing air-cooled condenser
Cooling Circuit:	Integrated with ITE
ITE Cooling Circuit	Not applicable
ITE Heat Rejection:	Liquid cooling (liquid-to-air or liquid-to-liquid exchange)

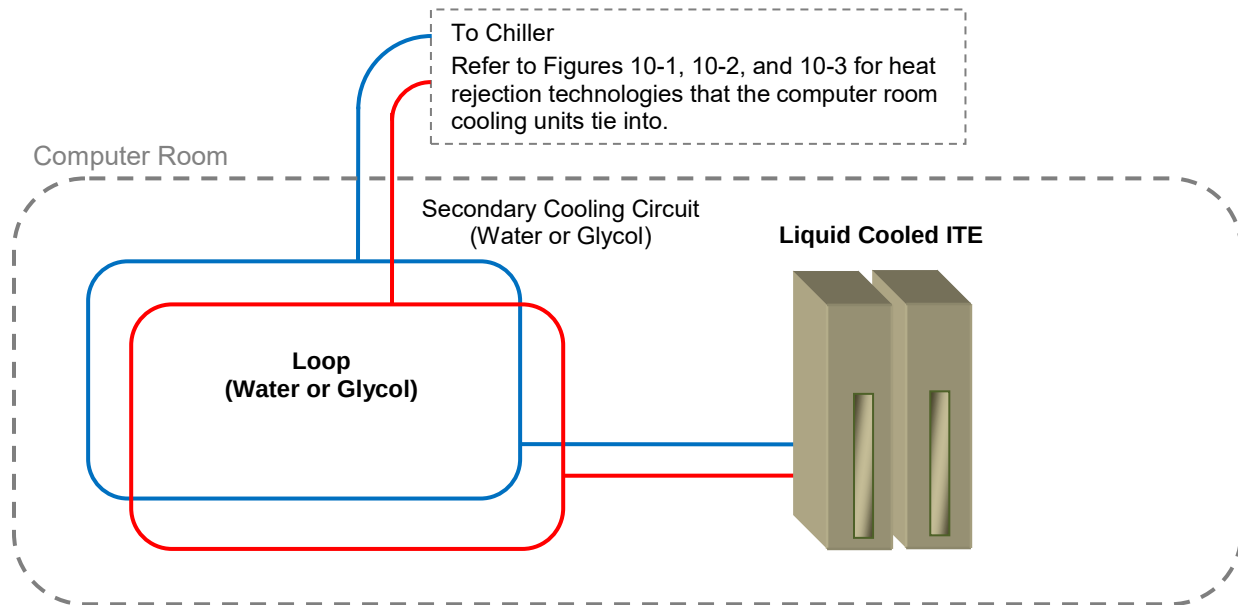


Figure 10-5
Liquid Cooling ITE Cooling System

10.2.2.3.3 Closed Cabinet Cooling System

Secondary Cooling Circuit:	Water for chiller utilizing evaporative cooling Glycol for outdoor chiller or chiller utilizing air-cooled condenser
Cooling Circuit:	Compressor integrated within closed cabinet
ITE Cooling Circuit	Air distribution contained within closed cabinet
ITE Heat Rejection:	Air cooled heat sink

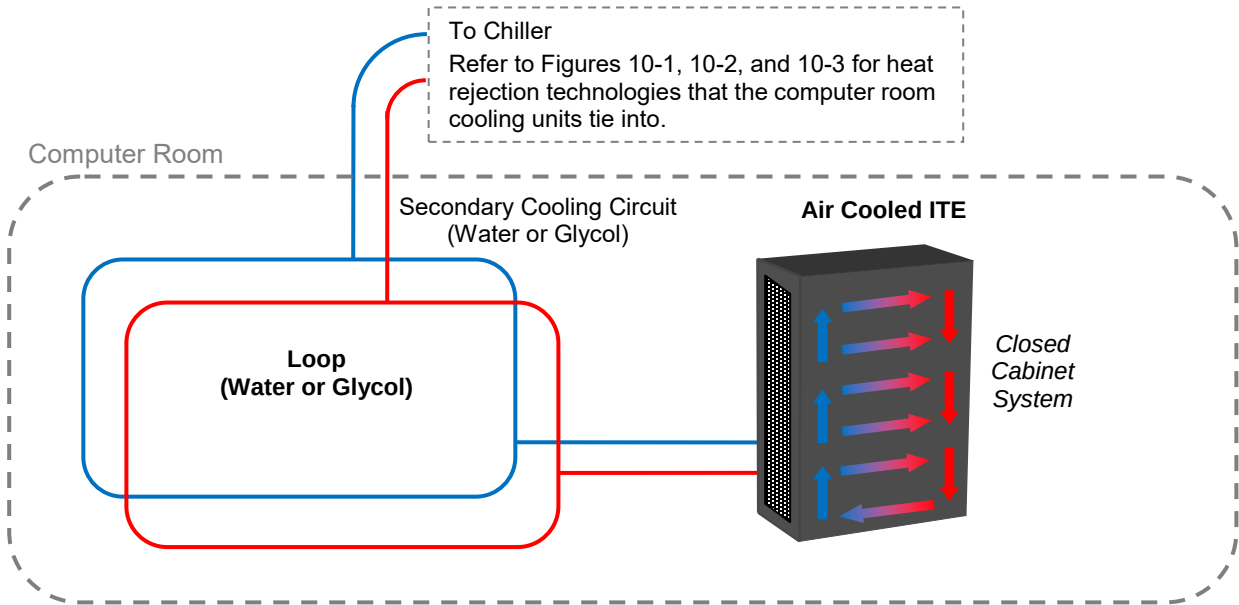


Figure 10-6
Closed Cabinet Cooling System

10.2.2.3.4 Row Integrated Cooling Systems

Secondary Cooling Circuit:	Water for chiller utilizing evaporative cooling Glycol for outdoor chiller or chiller utilizing air-cooled condenser
Cooling Circuit:	Above-row/in-row refrigerant sub-system
ITE Cooling Circuit	Air distribution
ITE Heat Rejection:	Air cooled heat sink

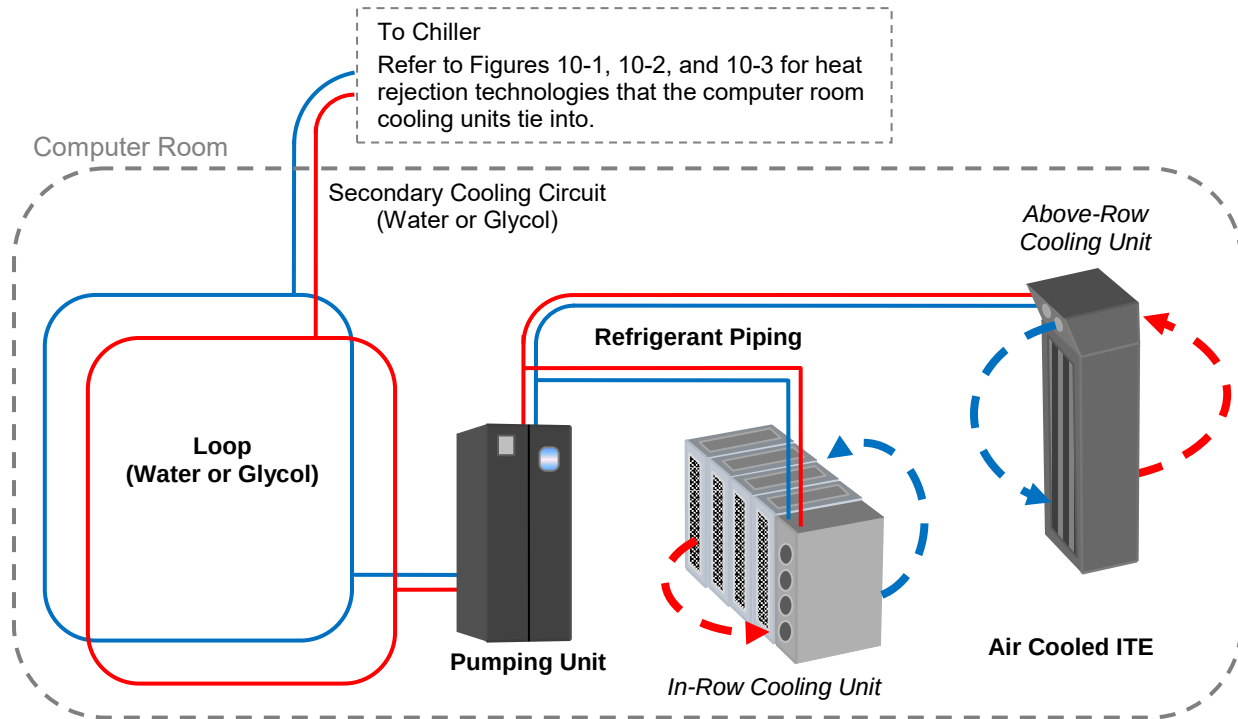


Figure 10-7
Row Integrated Cooling Systems

10.2.3 Direct Expansion Cooling Systems

10.2.3.1 Introduction

Direct expansion systems for cooling avoid the use of a chiller. Information and illustrations on common direct expansion cooling systems are presented below.

10.2.3.2 Computer Room Air Handler Cooling System

Heat Rejection:	Air cooled condenser (1 condenser for each CRAC)
Primary Cooling Circuit:	Refrigerant
Heat Exchanger:	Integrated within computer room air conditioner (CRAC)
Secondary Cooling Circuit:	Internal to CRAC
Cooling System:	CRAC with compressor
ITE Cooling Circuit:	Air distribution with underfloor supply and open room return, ducted supply, ducted return, or vertical heat collars above cabinets up to plenum return
ITE Heat Rejection:	Air cooled heat sink

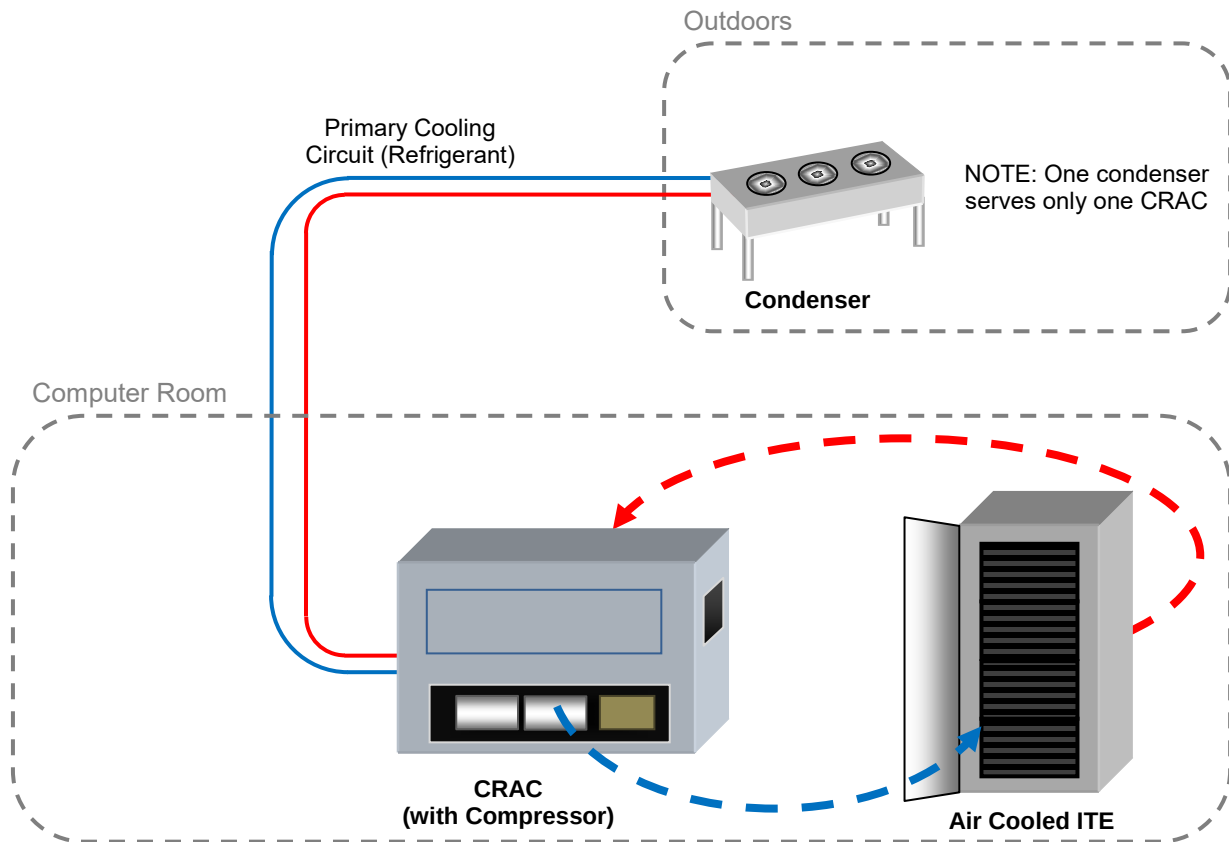


Figure 10-8
Direct Expansion Computer Room Air Handler Cooling System

10.2.3.3 Integrated Cooling System

Heat Rejection:	Air cooled condenser (1 condenser for each DX module)
Primary Cooling Circuit:	Refrigerant
Heat Exchanger:	Direct expansion module
Secondary Cooling Circuit:	Refrigerant
Cooling System:	Above-row or in-row cooling units
ITE Cooling Circuit:	Air distribution
ITE Heat Rejection:	Air cooled heat sink

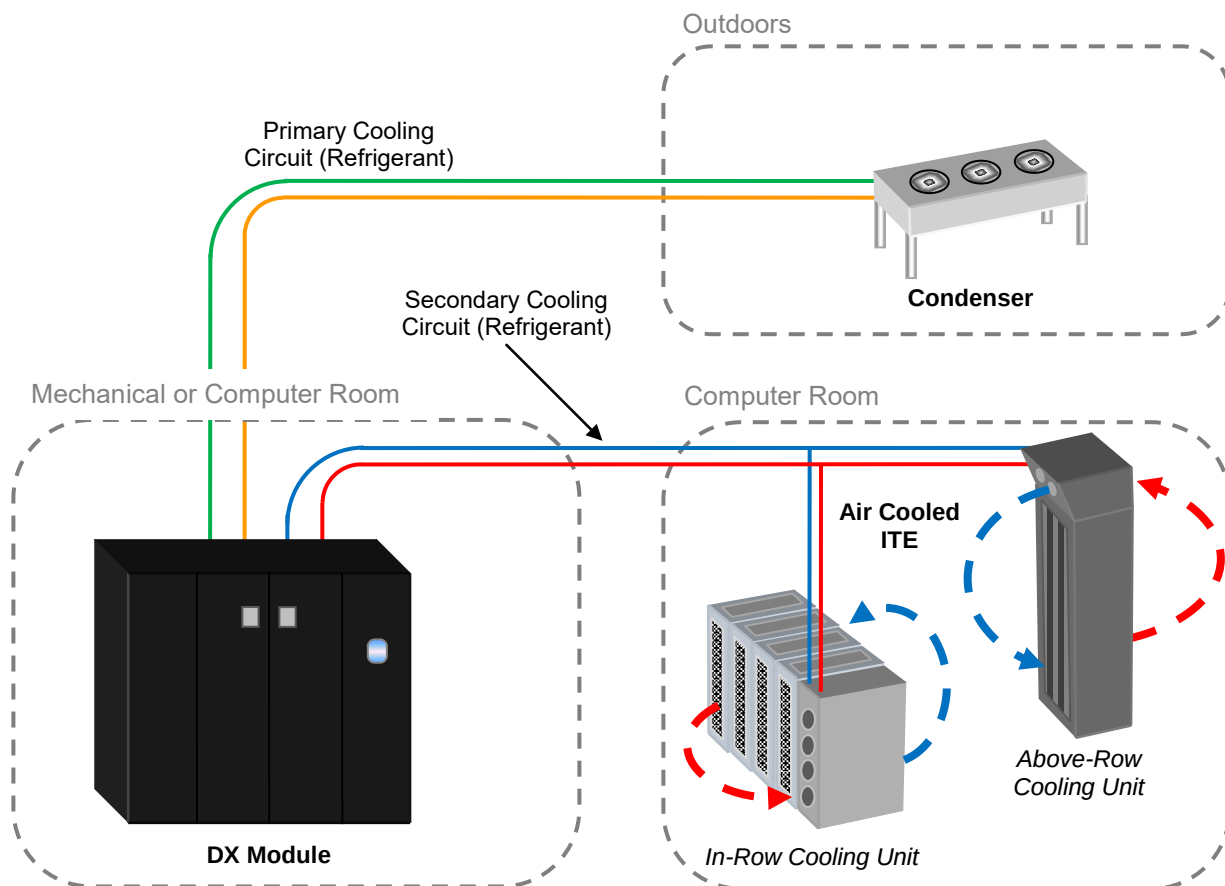


Figure 10-9
Direct Expansion Integrated Cooling System

10.2.3.4 Closed Cabinet Cooling System

Heat Rejection:	Air cooled condenser (1 condenser for each cabinet)
Primary Cooling Circuit:	Refrigerant
Heat Exchanger:	Direct expansion integrated within closed cabinet
Secondary Cooling Circuit:	Internal to cabinet
Cooling System:	Compressor integrated within closed cabinet
ITE Cooling Circuit:	Air distribution
ITE Heat Rejection:	Air cooled heat sink

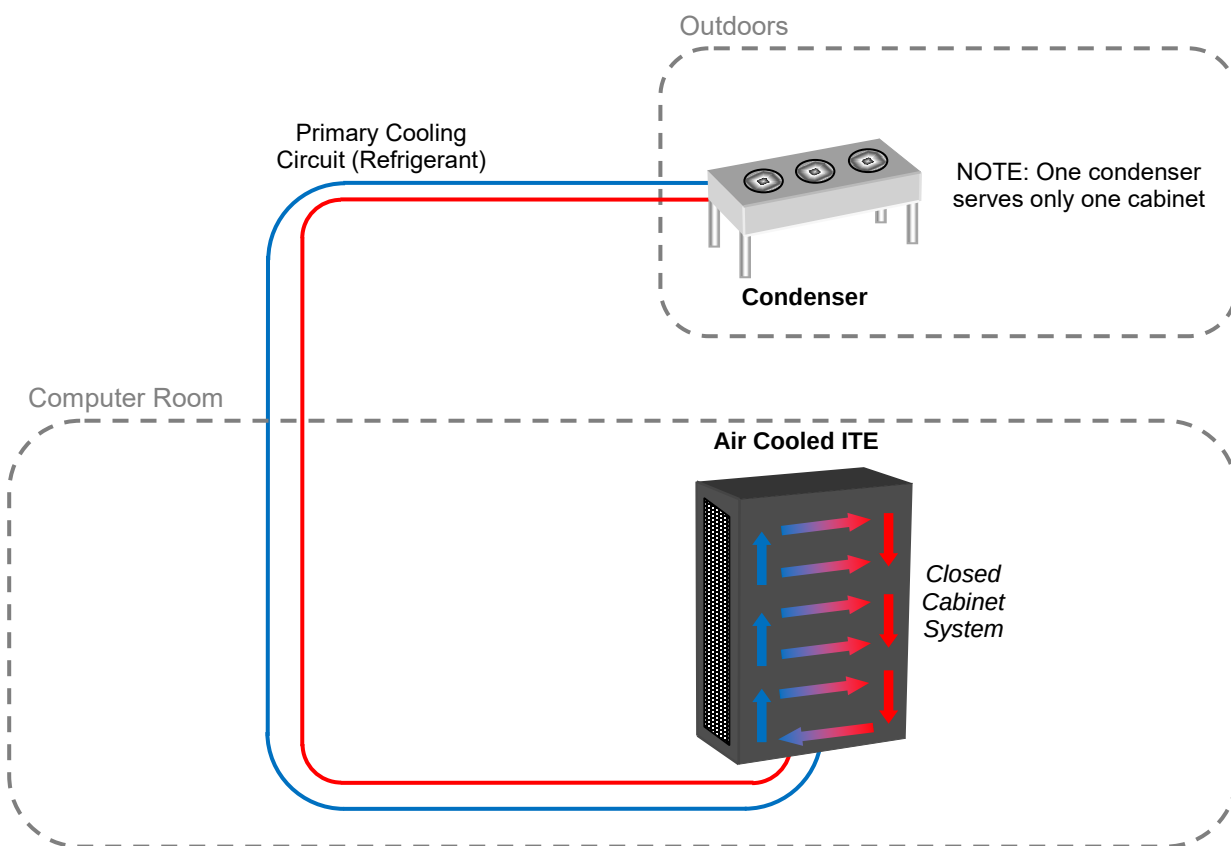


Figure 10-10
Direct Expansion Closed Cabinet Cooling System

10.2.4 Dual Coil Cooling Solution

In mechanical solutions that have dual coils with one coil utilizing a water-based heat rejection system and the other coil utilizing a DX heat rejection system, the water-based coil may be used in the unit to provide an energy efficient mode of operation (compressor-less). The water-based system would only need to be an “N” solution as each of the air handlers would have a dedicated condensing unit. The redundancy provided by the quantity of air handlers and their associated condensing units would need to match the level of redundancy required for the Class of the data center.

10.3 Mechanical Class Ratings

10.3.1 Introduction

This section expands upon the data center facility availability classes described in Appendix B and provides specific design information of the mechanical systems for achieving each Class. The standard includes five Classes relating to various levels of reliability of the data center facility infrastructure. The Classes are completely performance related.

The five Classes are:

- Class F0 and F1—The Single Path Data Center
- Class F2—The Single Path Data Center with Redundant Components
- Class F3—The Concurrently Maintainable and Operable Data Center
- Class F4—The Fault Tolerant Data Center

10.3.2 Class F0 and F1 Description

The mechanical systems cannot be maintained while operating. A failure of any element in the mechanical systems will likely result in the loss of cooling capability for the load. Single points of failure are common throughout the system. Any downtime, whether planned or unplanned, will result in cooling interruption.

Table 10-2 Class F0 and F1 Mechanical System Overview

Industry Description:	Single Path
Component Redundancy:	None
System Redundancy:	None
System Controls:	Single system
Power Feed:	All power feeds from common upstream distribution
Ability to be maintained under load:	No
Ability to recover from failures	No

Some representations of a Class F0 and F1 topology are shown in Figure 10-11 and Figure 10-12.

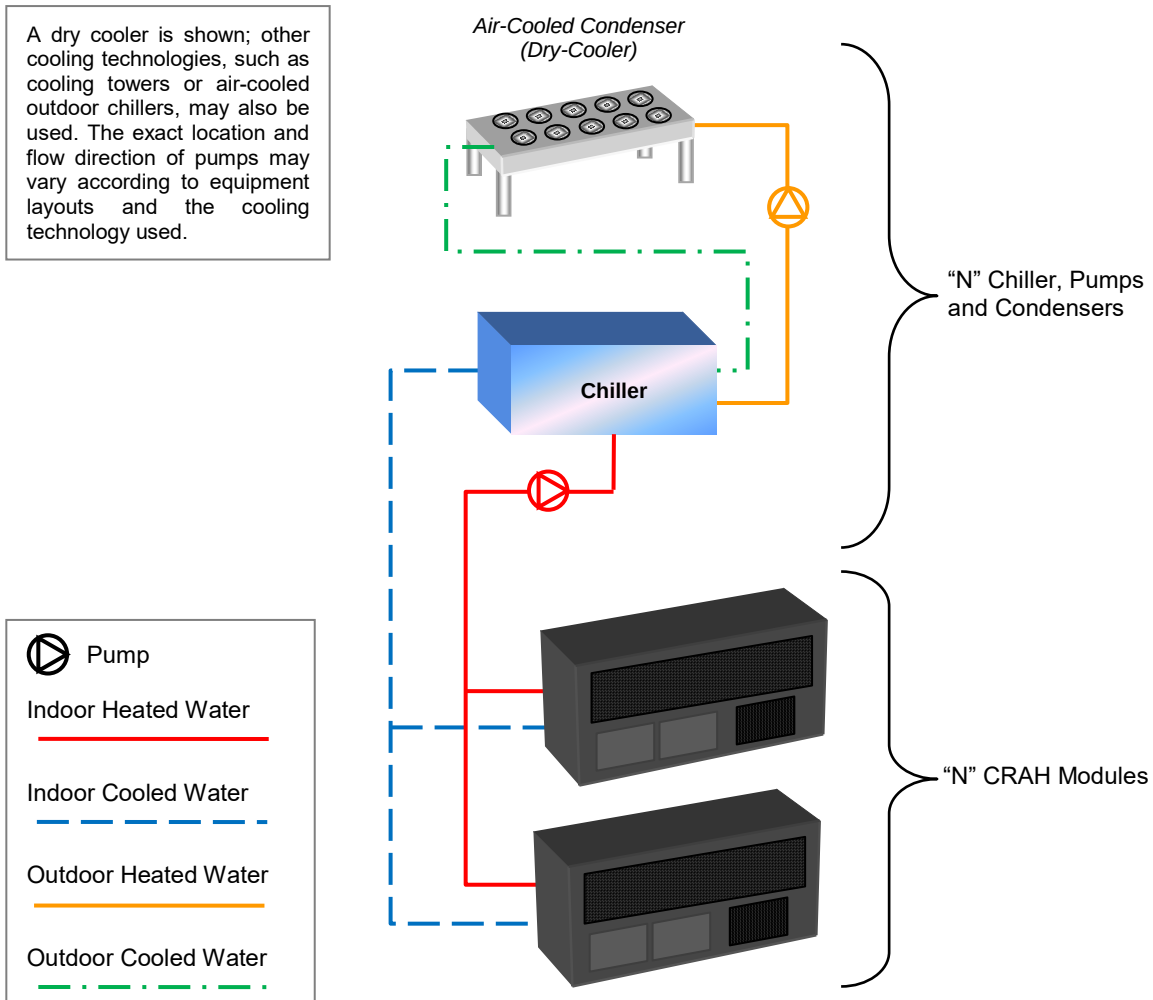


Figure 10-11
Class F0 and F1 Chiller System Example

The configuration shown in Figure 10-11 represents only one method of providing the level of redundancy required. Any solution that meets the performance requirements specified in Section 10.3.2 satisfies the reliability requirements.

Chiller piping and valve redundancy are not required for Class F0 and F1.

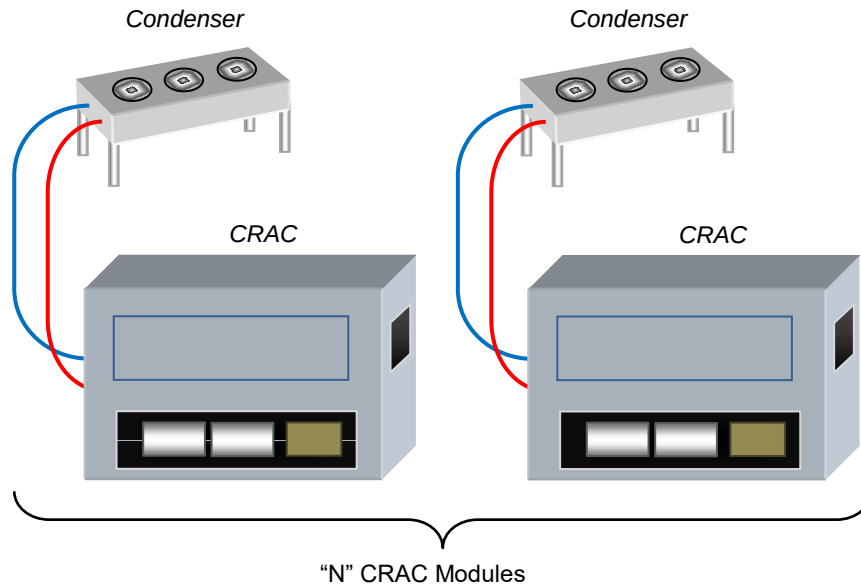


Figure 10-12
Class F0 and F1 Direct Expansion System Example

10.3.3 Class F2 Description

The mechanical systems possess some component redundancy but do not have any system redundancy. The mechanical components with redundancy can be maintained while operating. A failure of any element in the mechanical systems without component redundancy will likely result in the loss of cooling capability for the load. Single points of failure often exist within the overall cooling system. A minimum of $N+1$ components shall be provided for components with high failure rates, more than $N+1$ is recommended as the number of modules required to meet "N" increases.

Table 10-3 Class F2 Mechanical System Overview

Industry Description:	Single path with redundant components
Component Redundancy:	Yes for components with high failure rates
System Redundancy:	None
System Controls:	Single system
Power Feed:	All power feeds from common upstream distribution
Ability to be maintained under load:	For components with redundancy only
Ability to recover from failures	No

Some representations of a Class F2 topology are shown in Figure 10-13 and Figure 10-14.

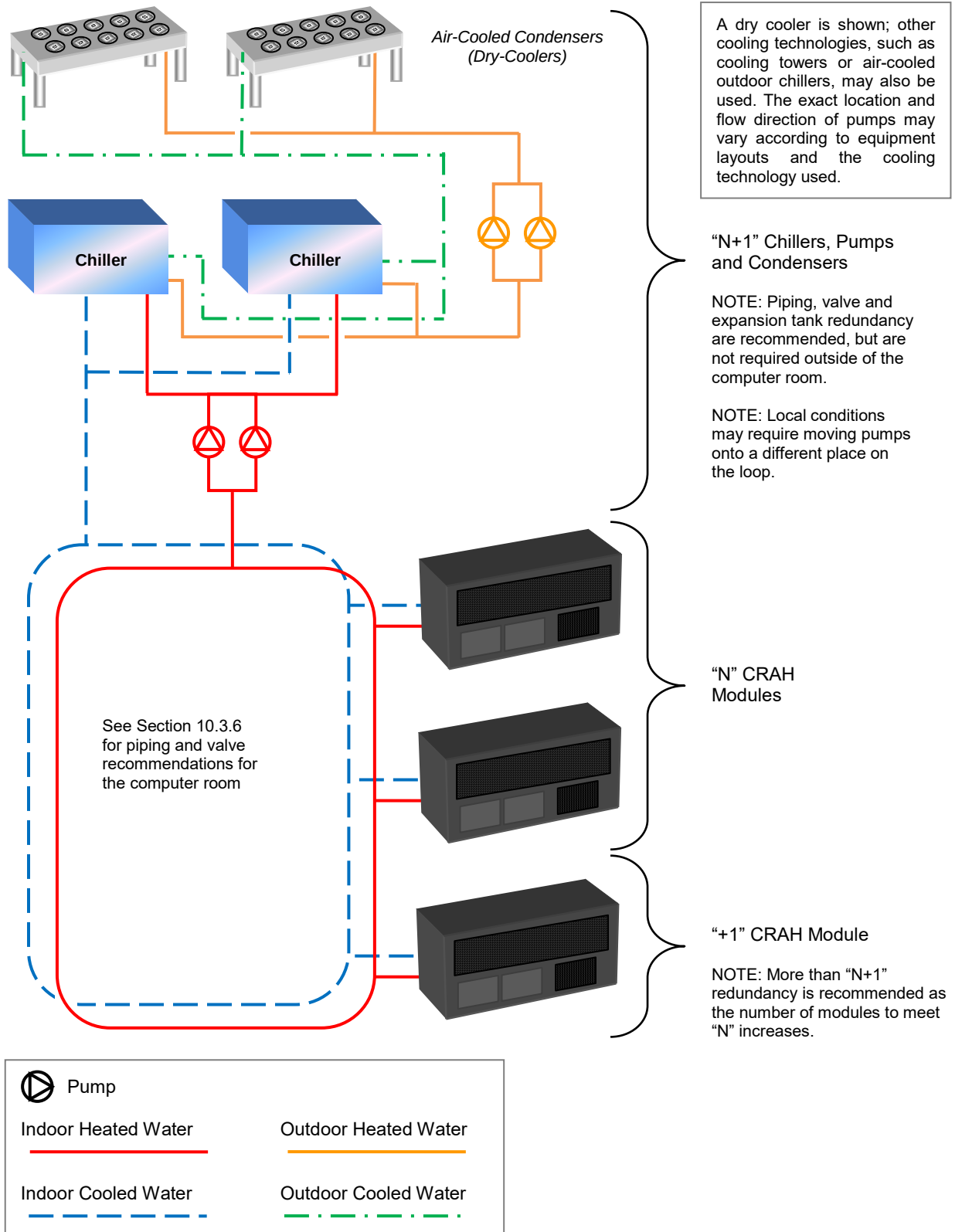


Figure 10-13
Class F2 Chiller System Example

The configuration shown in Figure 10-13 represents only one method of providing the level of redundancy required. Any solution that meets the performance requirements specified in Section 10.3.3 satisfies the reliability requirements for Class F2.

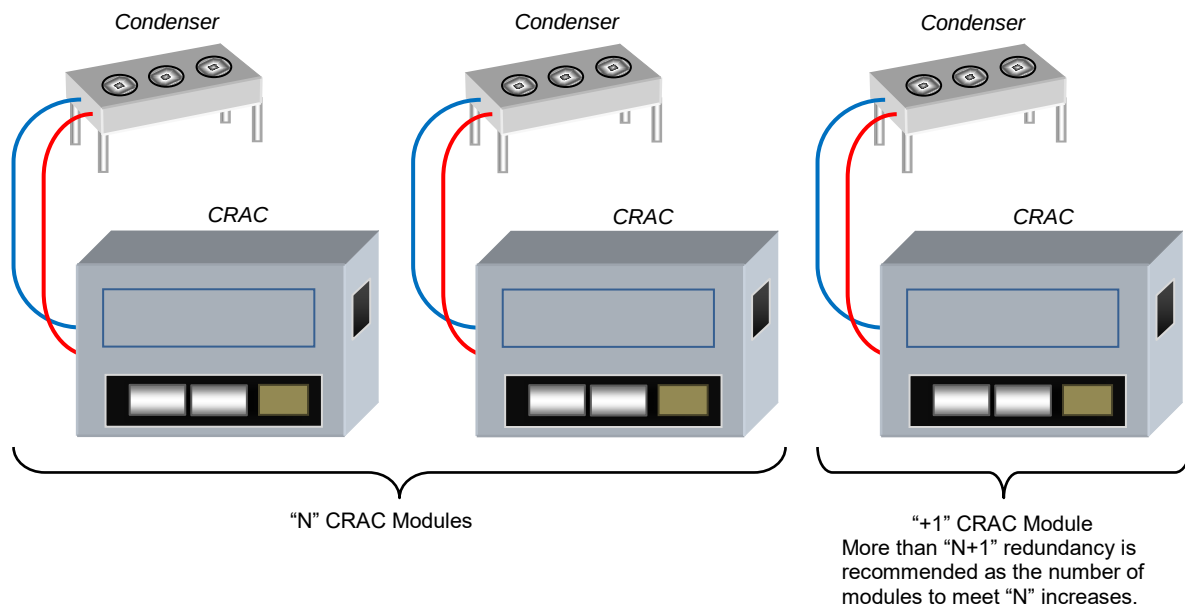


Figure 10-14
Class F2 Direct Expansion System Example

10.3.4 Class F3 Description

The mechanical systems possess redundancy so that any system or component may be taken off-line without impacting the system's ability to meet the "N" cooling capacity required. The level of redundancy required will be either at a system level or at a component level in order to ensure that all mechanical components can be maintained without impacting IT operations. A failure of any element in the mechanical systems will not result in the loss of cooling capability for the load. Single points of failure shall not exist within the overall cooling system. A minimum of N+1 components shall be provided for components with high failure rates; more than N+1 is recommended as the number of modules required to meet "N" increases.

Table 10-4 Class F3 Mechanical System Overview

Industry Description:	Concurrently maintainable and operable
Component Redundancy:	Yes for all components not included within a redundant system
System Redundancy:	Yes for all systems whose combination of components cannot be concurrently maintained by simply providing component redundancy
System Controls:	Redundant components or systems to ensure concurrent maintainability of cooling system
Power Feed:	Mechanical equipment and controls with redundant systems shall have the "A" systems feed from upstream "A" electrical distribution and "B" systems feed from upstream "B" electrical distribution. Mechanical equipment and controls that are limited to redundant components shall be feed from the electrical distribution in such a way as to ensure that the cooling capacity does not drop below "N" upon taking any mechanical component or upstream electrical distribution offline for maintenance, which is accomplished with the implementation of mechanical equipment with dual power feeds or ATS upstream on the power circuits feeding the mechanical equipment.
Ability to be maintained under load:	Yes without reducing cooling capacity to less than "N"
Ability to recover from failures	Yes at the system or component level without reducing the cooling capacity to less than "N"

Some representations of a Class F3 topology are shown in Figure 10-15 and Figure 10-16.

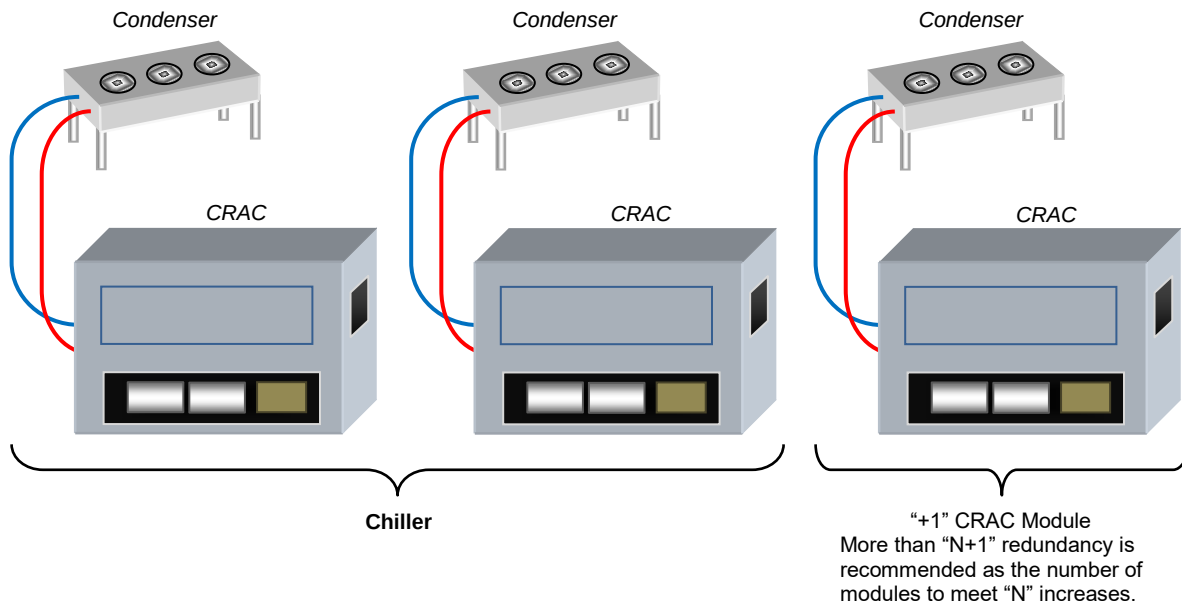


Figure 10-15
Class F3 Direct Expansion System Example

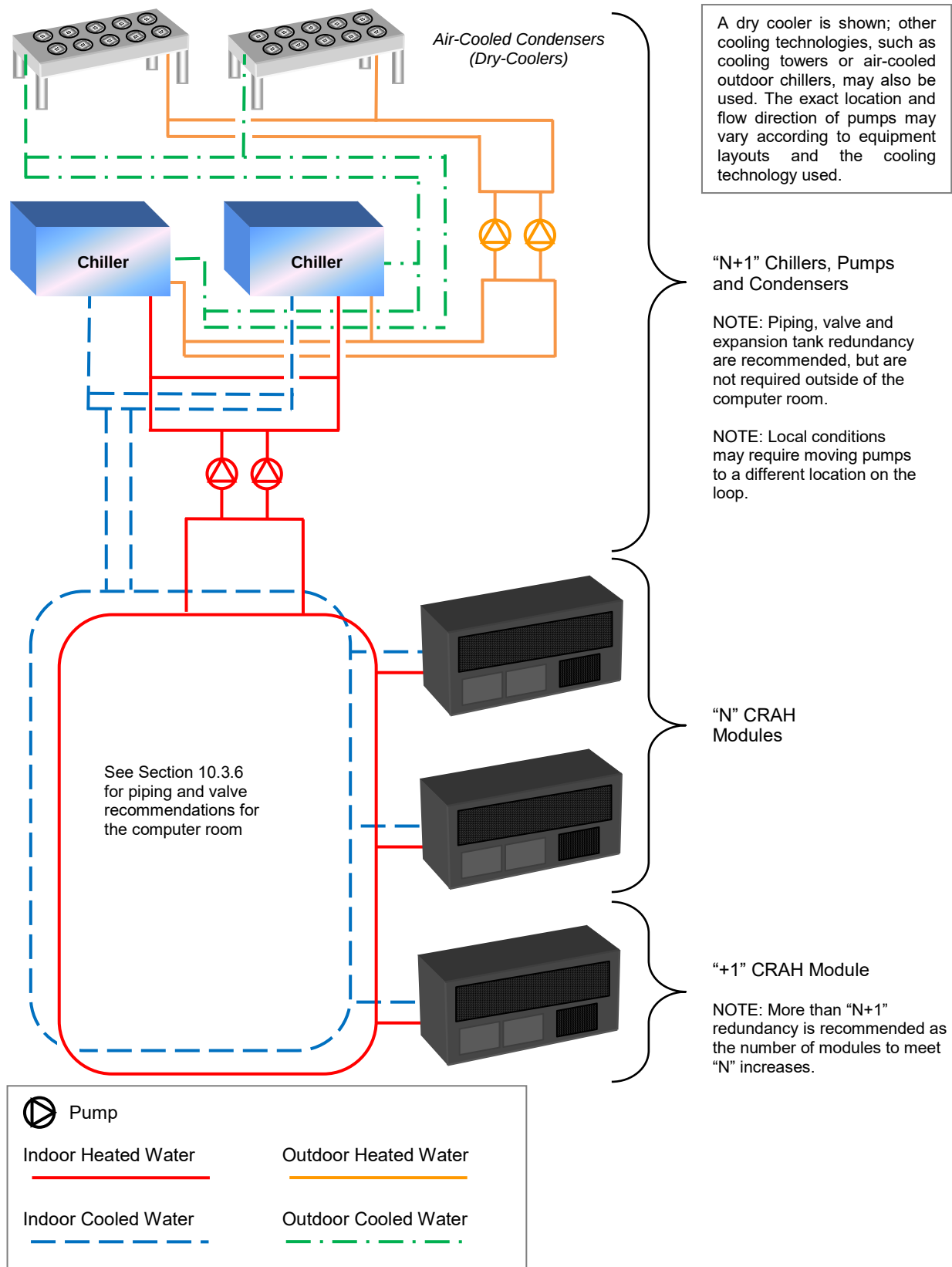


Figure 10-16
Class F3 Chiller System Example

The configuration shown in Figure 10-16 represents only one method of providing the level of redundancy required. Any solution that meets the performance requirements specified in Section 10.3.4 satisfies the reliability requirements for Class F3.

10.3.5 Class F4 Description

The mechanical systems possess redundancy so that any system or component may be taken off-line without impacting the system's ability to meet the "N+1" cooling capacity required. The level of redundancy required will be either at a system level or at a component level in order to ensure that a mechanical component can experience a fault while maintaining any other mechanical component or system without impacting IT operations. A failure of any element in the mechanical systems will not result in the loss of cooling capability for the load. Single points of failure shall not exist within the overall cooling system. A minimum of N+2 components shall be provided for components with high failure rates; more than N+2 is recommended as the number of modules required to meet "N" increases.

Table 10-5 Class F4 Mechanical System Overview

Industry Description:	Fault tolerant
Component Redundancy:	Yes, "N+1" for all components within a redundant system, and "N+2" for all components not within a redundant system.
System Redundancy:	Yes for all systems whose combination of components cannot be fault tolerant by simply providing "N+2" component redundancy
System Controls:	Redundant systems to ensure fault tolerance of cooling system
Power Feed:	Mechanical equipment and controls with redundant systems shall have the "A" systems feed from upstream "A" electrical distribution and "B" systems feed from upstream "B" electrical distribution. Mechanical equipment and controls that are limited to redundant components shall be feed from the electrical distribution in such a way as to ensure that the cooling capacity does not drop below "N+1" upon taking any mechanical component or upstream electrical distribution offline for maintenance, which is accomplished with the implementation of mechanical equipment with dual power feeds or ATS upstream on the power circuits feeding the mechanical equipment.
Ability to be maintained under load:	Yes without reducing cooling capacity to less than "N+1"
Ability to recover from failures	Yes, at the system or component level without reducing the cooling capacity to less than "N+1"

Some representations of a Class F4 topology are shown in Figure 10-17 and Figure 10-19.

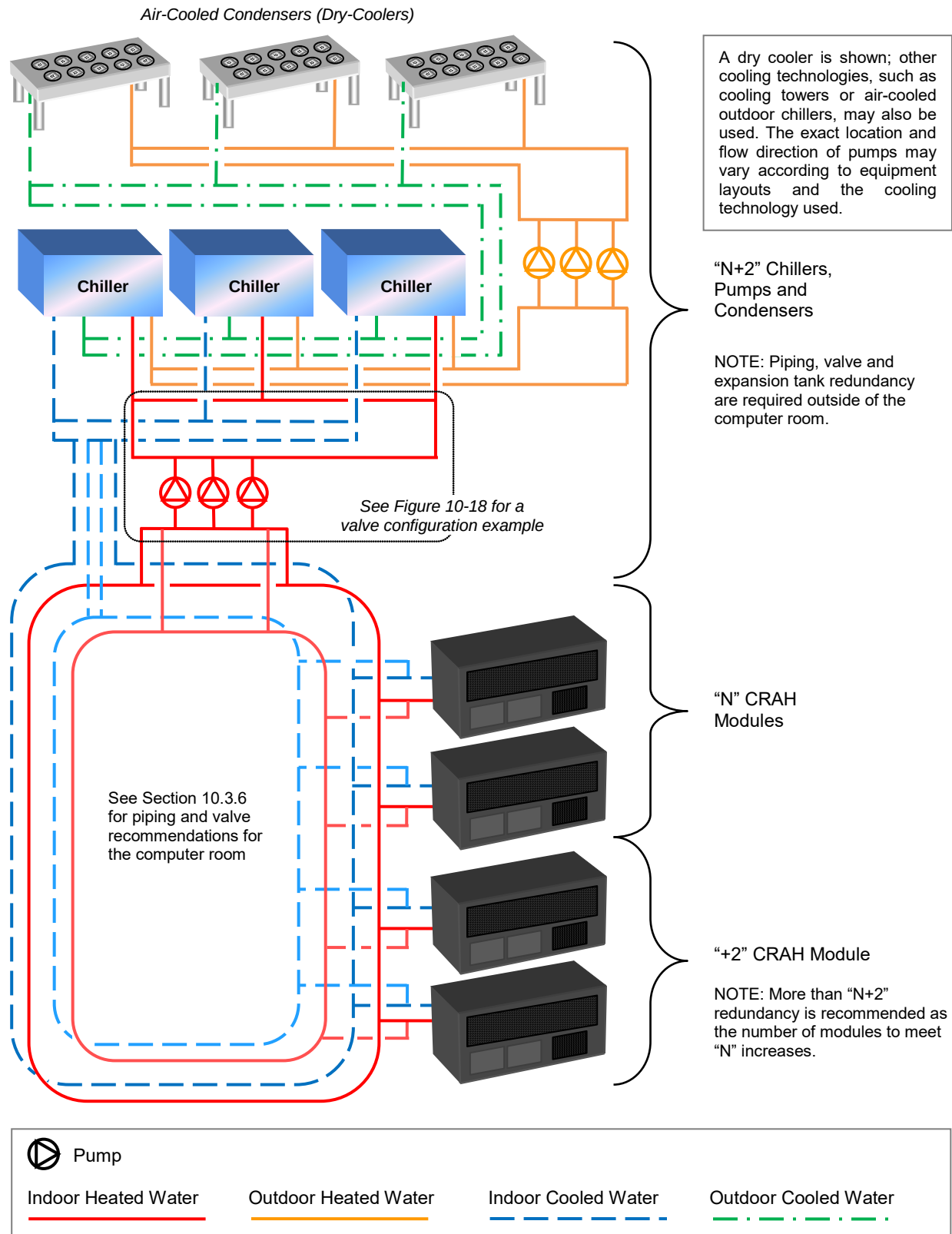


Figure 10-17
Class F4 Chiller System Example

The configuration shown in Figure 10-17 represents only one method of providing the level of redundancy required. Any solution that meets the performance requirements specified in Section 10.3.5 satisfies the reliability requirements for Class F4.

Figure 10-17 also shows the supply and return piping from two piping loops, with interlocks to avoid loop mixing. A dual coil CRH or 2N CRAH solution that separates the loops are also options.

Figure 10-18 shows an example valve layout that facilitates concurrent maintainability of the pumps and piping in an N+1 pump redundant layout.

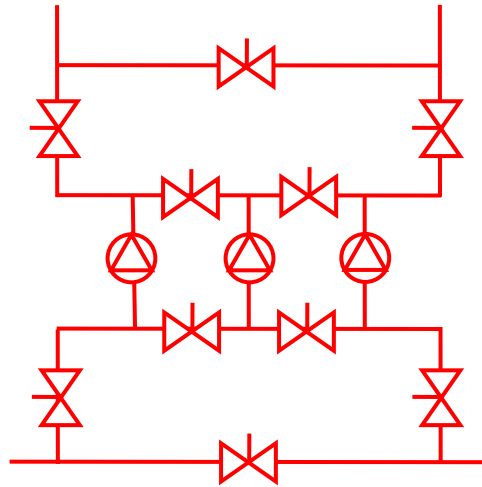


Figure 10-18
Valve Configuration Example for Pumps in Class F4 System (Figure 10-17)

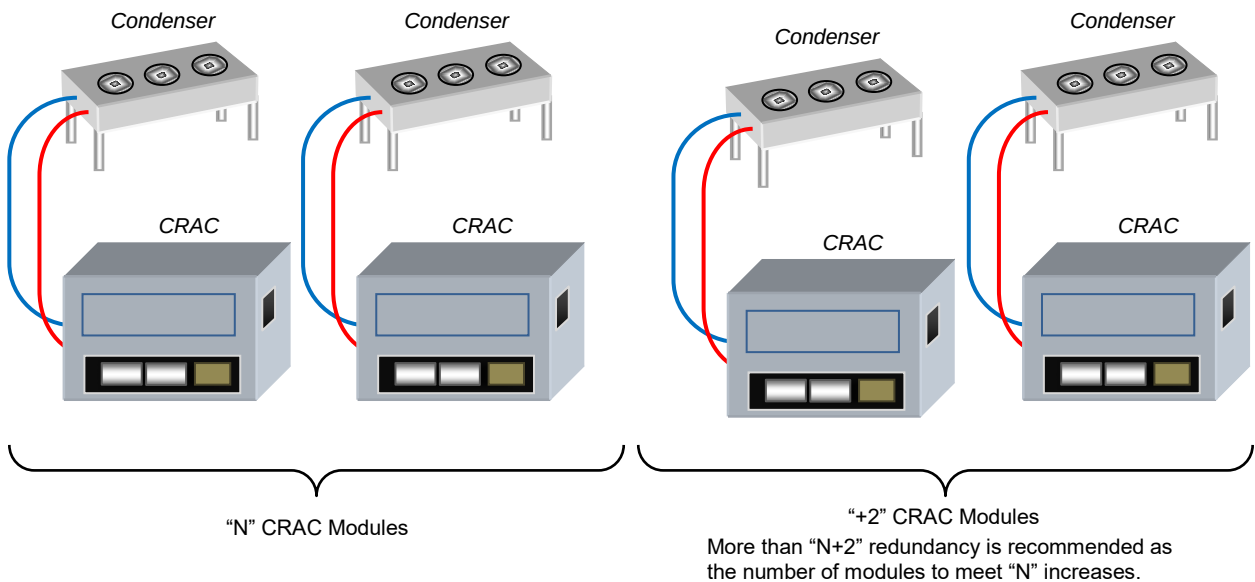


Figure 10-19
Class F4 Direct Expansion System Example

10.3.6 Chiller Piping and Valve Redundancy

For higher class data centers, redundancy in chiller piping systems and valve components is a complex balance between providing concurrent maintainability or fault tolerance and simplicity. The standard provides the performance requirements and some concept-level examples to facilitate the discussions and decisions that will need to be made regarding piping and valve redundancy, maintainability, and operations.

10.3.6.1 Class F0 and F1 Requirements

Class F0 and F1 data centers do not require piping or valve redundancy.

10.3.6.2 Class F2 Requirements

Class F2 data centers shall have piping redundancy within the computer room, which is typically accomplished with a looped piping system. Piping redundancy outside the computer room is not required. Valve redundancy is not required.

10.3.6.3 Class F3 Requirements

10.3.6.3.1 Introduction

See Figure 10-20 for an example Class F3 piping and valve redundancy.

CRAH:

Each CRAH unit shown represents a single CRAH or group of CRAHs connected to the computer room piping loop in between loop isolation valves.

Isolation Valves:

The quantity of CRAHs connected between isolation valves shall be coordinated so that the quantity of CRAH units taken off-line during valve or pipe maintenance does not reduce the cooling system to below "N" capacity for specified computer room conditions. During maintenance modes, ASHRAE environmental condition ranges A1, A2 or higher may be acceptable.

Valves in Series:

Double isolation valves in series may not be required if alternate methods of isolation are achievable to accommodate valve and pipe maintenance.

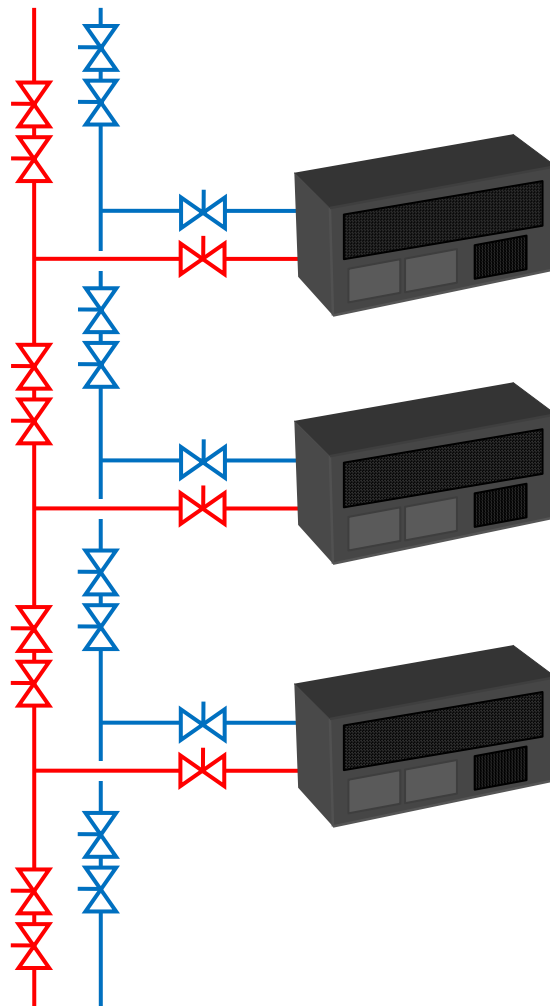


Figure 10-20
Class F3 Piping and Valve Redundancy Example

10.3.6.3.2 Requirements

Class F3 data centers shall have piping redundancy within the computer room, which is typically accomplished with a looped piping system.

In a Class F3, the quantity of CRAHs or similar units connected between isolation valves shall be coordinated so that the quantity of units taken off-line during valve or pipe maintenance does not reduce the cooling system to below “N” capacity. Depending on computer room design conditions, room conditions at ASHRAE allowable A1, A2, or higher environmental conditions may be acceptable during maintenance modes.

Double isolation valves may not be required if alternate methods of isolation are achievable to accommodate valve and pipe maintenance.

10.3.6.3.3 Recommendations

Valve redundancy within the computer room is not required, but it is recommended. Piping and valve redundancy outside the computer room is not required, but it is recommended. Valve maintenance may be achievable without valve redundancy through other manual maintenance options, such as freezing the pipe in the area to be maintained.

10.3.6.4 Class F4 Requirements

10.3.6.4.1 Introduction

See Figure 10-21 for an example Class F4 piping and valve redundancy.

10.3.6.4.2 Requirements

Class F4 data centers shall have fault tolerant piping redundancy within the computer room, which is typically accomplished with a double looped piping system. Valve redundancy within the computer room is required.

In a Class F4, the quantity of CRAHs or similar units connected between isolation valves shall be coordinated so that the quantity of units taken off-line during valve or pipe maintenance does not reduce the cooling system to below “N+1” capacity. Depending on computer room design conditions, room conditions at ASHRAE allowable A1, A2, or higher environmental conditions may be acceptable during maintenance modes.

Double isolation valves may not be required if alternate methods of isolation are achievable to accommodate valve and pipe maintenance.

10.3.6.4.3 Recommendations

Piping and valve redundancy outside the computer room is not required, but recommended. Valve maintenance may be achievable without valve redundancy through other manual maintenance options such as freezing the pipe in the area to be maintained.

10.4 Environmental Conditions

10.4.1 Introduction

Telcordia GR-3028-CORE includes a discussion of the differences between machine and human requirements. Generally, modern data centers are not designed to provide human comfort conditions. Temperatures, air velocities, and noise levels often exceed acceptable human conditions. High processing power is moving data centers toward an industrial environment.

10.4.2 Normal Operation Versus Loss of Environmental Control

Normal operating conditions exist when the HVAC system provides the necessary air conditioning to maintain the computer room within specifications. Designed properly, very high densities can be cooled adequately. However, even in computer rooms with moderate densities, loss of the HVAC system (whether through loss of power or cooling equipment failure) can result in steep temperature gradients and subsequently high space and equipment inlet temperatures.

10.4.3 Environmental Class Definitions

10.4.3.1 ASHRAE Thermal Guidelines

The environmental class recommended within *ASHRAE Thermal Guidelines* that is the most significant for the day-to-day operation of a typical data center is Class 1: Equipment in Operation. The recommended environmental limits are:

- 18.3 to 26.7 °C (64.4 to 80.6 °F)
- 60% maximum relative humidity (RH)
- Maximum dew point of 15 °C (59 °F)
- Minimum dew point (lower moisture limit) of 5.5 °C (42 °F)

CRAH:

Each CRAH unit shown represents a single CRAH or group of CRAHs connected to the computer room piping loop in between loop isolation valves.

Isolation Valves:

The quantity of CRAHs connected between isolation valves shall be coordinated so that the quantity of CRAH units taken off-line during valve or pipe maintenance does not reduce the cooling system to below "N+1" capacity for specified computer room conditions. During maintenance modes, ASHRAE environmental condition ranges A1, A2, or higher may be acceptable.

Valves in Series:

Double isolation valves in series may not be required if alternate methods of isolation are achievable to accommodate valve and pipe maintenance.

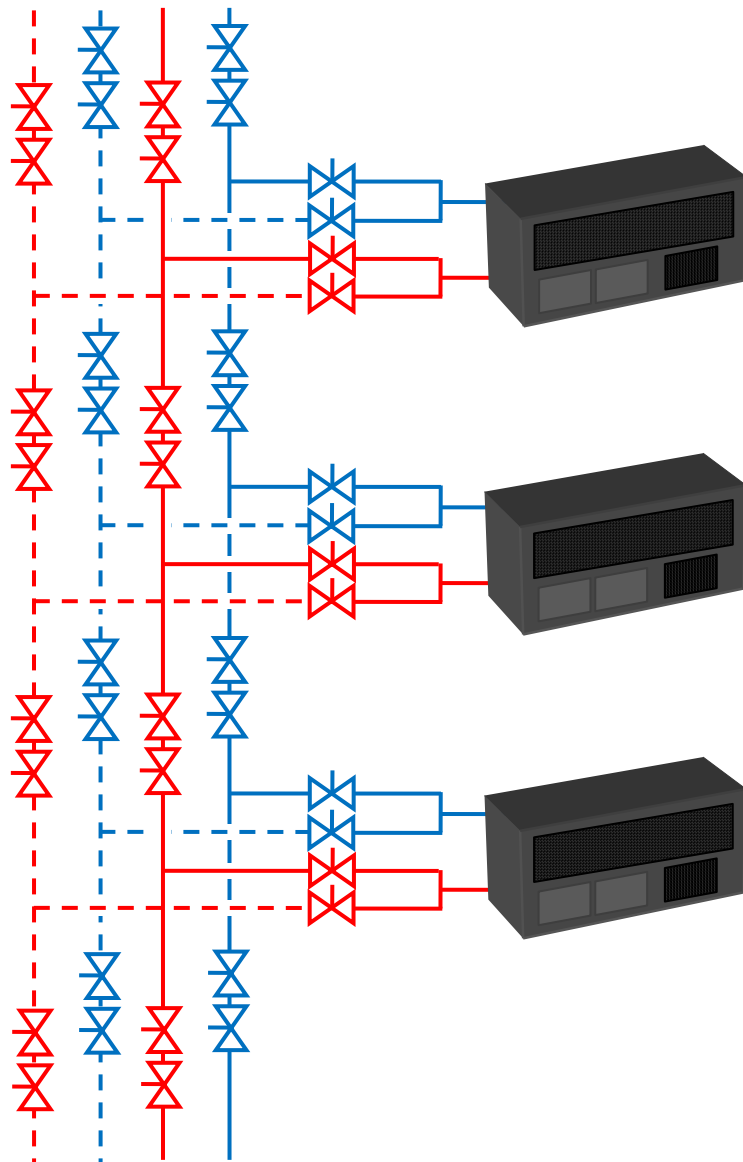


Figure 10-21
Class F4 Piping and Valve Redundancy Example

Dew point of 5.5 °C corresponds to approximately 44% RH at 18 °C (64 °F) and 25% RH at 27 °C (81 °F). The lower moisture limit is used to control electrostatic discharge (ESD).

The preceding conditions are stated at sea level. The recommended maximum dry-bulb temperature is derated by 1 °C/300 m above 1800 m (1.8 °F/1000 ft above 6000 ft).

These recommended temperature and humidity conditions are measured at the equipment inlet. Compliance with these thermal guidelines can be demonstrated by using the Rack Cooling Index (RCI) listed in Section 10.4.4.3.

NOTE: Refer to *ASHRAE Thermal Guidelines* for definitions of the other environmental classes.

10.4.3.2 NEBS GR-3028-CORE

The recommended limits for environments are 18.3 to 26.7 °C (64.4 to 80.6 °F) and maximum 55% relative humidity.

10.4.4 Air Conditioning

10.4.4.1 Introduction

Control of environmental conditions within the data processing areas, as well as the supporting areas, such as UPS rooms, is critical to the functioning of computer equipment. Data processing areas have unique needs associated with heat generation, gaseous contaminants, air impurities, and variations in humidity and temperature.

10.4.4.2 Recommendations

HVAC design should consider and provide for:

- Controls for temperature and humidity at the computer equipment inlet
- Adequate filtration and ventilation
- Special needs of direct cooled equipment
- Airflow patterns for heat dissipation within the room
- Avoidance of recirculation of hot air
- Redundant cooling systems as determined necessary by the user
- Architectural features such as a tight vapor barrier

Control of temperature and humidity is achieved when conditions at the equipment air inlet are maintained within the limits established by *ASHRAE Environmental Guidelines* or GR-3028-CORE. Limits include both high and low values of temperature, humidity, and rate of change for temperature. Because relative humidity varies with temperature without the addition or removal of moisture, it is a moving target, and therefore, not a good indicator of stable environmental conditions. A much more effective parameter is dew point. Whenever possible, space environmental controls should seek to achieve a stable dew point over the acceptable temperature range. This strategy will improve the stability of both temperature and humidity in the computer room.

It is recommended that consideration be given to further improve of the cooling system performance by using modular CRAC units, cold or hot aisle containment, or a combination of the two techniques. Such measures will stop hot air contaminating the expensive processed cold air and improve the environment for the remainder of the computer room space. However, a hot air return plenum may require the use of cabinet exhaust chimneys and greater cabinet depth.

10.4.4.3 Additional Information

The Rack Cooling Index (RCI) is a best practice performance metric designed to gauge the compliance with the thermal guidelines of ASHRAE and NEBS for a given data center. The RCI is a measure of how effectively equipment racks are cooled and maintained within industry thermal guidelines and standards. As such, the Index can help engineers and architects to design well-functioning data centers, and the Index can be used to specify the level of compliance required as part of a basis-of-design document (Herrlin, M. K. 2005. *Rack Cooling Effectiveness in Data Centers and Telecommunications Central Offices: The Rack Cooling Index (RCI)*. ASHRAE Transactions, Volume 111, Part 2, American Society of Heating, Refrigerating and Air-conditioning Engineers, Inc., Atlanta, GA).

The computer room air distribution method may be vertical, such as overhead or underfloor, or may be horizontal such as a flooded supply or with cooling units in the rows of equipment. Overhead distribution is sometimes chosen when no access floor is used or when central air handling equipment is used versus CRAC units. Be aware that overhead distribution may introduce more limitations than underfloor distribution and may limit the choice of HVAC equipment. Horizontal distribution methods can also be used without an access floor. Flooded supply from an upflow or downflow cooling unit can be used while placing cooling units among the racks is one method to close-couple the heat load to the cooling, minimizing mixing of hot and cold air. The selection of air distribution method involves many factors that are specific to a particular project. The method of air distribution should not be selected before a thorough review of the project requirements, including but not limited to physical limitations of the building, fire suppression systems, location of power and communications cabling, and budget. Refer to *ASHRAE Design Considerations and Datacom Equipment Power Trends and Cooling Applications* for additional guidelines regarding HVAC design.

10.4.5 Ventilation (Outside Air)

10.4.5.1 Equipment Rooms

10.4.5.1.1 Introduction

Human occupancy in data centers is typically low. However, removal of internally generated pollutants and maintaining a positive pressure in the computer room and entrance space should be considered when determining a ventilation rate. Maintaining a positive pressure in the computer room and entrance room spaces relative to adjacent spaces is important as contaminants or dirt could migrate into the data center. It is especially important when the adjacent space is outdoors as wind effects can create pressure differentials that will exceed the space pressurization, resulting in increased outdoor air infiltration.

10.4.5.1.2 Recommendations

GR-3028-CORE recommends 0.25 air changes per hour for removal of internally generated contaminants, which equals the code requirement when the total ceiling heights and access floor height is 3.7 m (12 ft) and exceeds the code requirement when this dimension is greater than 3.7 m (12 ft).

Absence or presence of vapor barriers must be considered to ensure acceptable environmental control and to prevent mold growth.

10.4.5.1.3 Additional Information

Ventilation is defined by ASHRAE as air supplied to or removed from a space for the purpose of controlling air contaminant levels, humidity, or temperature. It is typically interpreted as the portion of the supply air that is “fresh” outdoor air that has not been recirculated or transferred from any other space.

Ventilation rates prescribed by codes (*International Mechanical Code* or other mechanical codes adopted by the local or state jurisdiction) and by ASHRAE 62.1 are concerned with meeting the needs of occupants. Meeting the requirements of ASHRAE 62.1 may not provide sufficient ventilation for adequate space pressurization, but code compliance must always be documented in the design process.

As ventilation rates increase, the potential for introducing contaminants into the computer room may also increase. This is because typical filter holding frames provided by the manufacturers of air handling units allow for some bypass around the filters. As the volume of outdoor air supplied to the computer room increases, the volume of unfiltered bypass air will also increase. Filter frame leakage efficiency is addressed in Section 10.4.6.

10.4.5.2 Battery Rooms

NOTE: Additional information can be found in the *IMC* and *NFPA 70E*.

10.4.5.2.1 Requirements

When mechanical ventilation is provided, the minimum required exhaust flow is 0.3 m³/min per m² of room area (1 ft³/min per ft² of room area) with hydrogen concentration limited to 1% of the total room volume. Conservative HVAC engineers often design the battery room exhaust system for 0.6 m³/min per m² of room area (2 ft³/min per ft² of room area).

Ventilation is required for both VRLA and flooded cell batteries.

10.4.5.2.2 Recommendations

Battery rooms (or enclosures) should limit the concentration of hydrogen gas to less than 1% concentration.

In most cases, a dedicated exhaust system is provided to remove hydrogen gas that may accumulate.

Battery ventilation is a code-required safety system and is independent of Class. Redundant exhaust fans are not required by codes but should be provided for Class F3 and Class F4 data centers to be consistent with the reliability goals of such facilities along with an alternate source of makeup air in the event of a makeup air system failure. Exhaust fan operation/status should be monitored.

If hydrogen detection systems are provided, they should be monitored by the central security monitoring or building automation/management system.

10.4.5.3 Computer Room Pressurization

10.4.5.3.1 Recommendations

TIA-942-A specifies a positive pressure differential with respect to surrounding areas. A typical range for the pressure differential between the computer room and any adjacent rooms is 3 to 12 Pa (0.012 to 0.05 in WC).

Controlling room pressure differential with a building control system and a system of dampers or variable speed fans is often complicated, with limited effectiveness, especially if doors are frequently opened and closed.

Generally, manual balancing to achieve the desired pressure differential is sufficient. Room pressure differential should be monitored.

Loose or leaky construction (such as oversized, unsealed openings created for piping, conduit, or cabling, abandoned openings, and poor construction methods) that may exist in older buildings will significantly increase the volume of makeup air required for pressurization. Care should be taken during construction to seal cracks and openings that prevent adequate pressurization.

10.4.6 Airborne Contaminants (Gases and Particles)

10.4.6.1 Indoor Limits

See TIA-942-A, *Gaseous and Particulate Contamination Guidelines for Data Centers*, or applicable local codes or standards for a list of contaminants levels.

10.4.6.2 Recommendations

Particulates in the air degrade computer operations. Good operating practices will limit or prohibit the most common sources of particulate contamination from the computer room (i.e., cardboard and storage of paper). Maintaining a controllable positive pressure in the computer room with respect to adjacent spaces will aid in reducing infiltration of particulates and humid/dry air. However, excess positive pressurization can be detrimental.

The air-handling unit supplying outdoor air should be equipped with filters to at least MERV 13 (ASHRAE 80% to 90%) to ensure a clean air supply. When this is not possible, the air supplied to the computer room for pressurization should be filtered to this level before it is supplied to the space.

Air handling units supplying outdoor air should be equipped with low-leakage filter holding frames to limit bypass to less than 1% at 0.7 kPa (3 in WC) differential pressure.

Users should not replace “standard” efficiency filters in their existing packaged computer room air conditioners with high-efficiency filters without first consulting the manufacturer of the equipment to assess the impact of this change as reduced airflow and cooling capacity could result.

10.4.6.3 Additional Information

Pressurization of the computer room with air supplied from outside the space is the most effective means of controlling infiltration of particulate that could migrate from surrounding spaces.

Particulate contamination originating from the building’s construction should be addressed, where possible, by thoroughly cleaning of the space before it is occupied. It is important to understand that increasing the filtration level at the air handlers has only a marginal benefit compared to the additional energy expended by the fan systems.

The standard filters furnished with packaged computer room air conditioning equipment have either 20% or 30% ASHRAE efficiency ratings. Higher efficiency filters at CRAC units will not provide significant improvements in air quality and will result in higher energy costs. See the *ASHRAE Handbook* or ASHRAE 52.2 regarding minimum efficiency reporting value (MERV) ratings of filters.

Manufacturers offer optional high-efficiency filters, usually up to 85% ASHRAE efficiency (some equipment offered in Europe is available with near-HEPA filter quality filters). Selecting high-efficiency filters will require a higher static pressure blower and correspondingly higher horsepower motors.

10.4.7 Environmental Limits

10.4.7.1 Recommended Operational

TIA-942-A: dry bulb temperature is 20 °C (68 °F) to 25 °C (77 °F).

NEBS: dry bulb temperature is 18 °C (65 °F) to 27 °C (80 °F) per GR-3028-CORE.

ASHRAE: dry bulb temperature 18.3 °C (64.4 F) to 26.7 °C (80.6 F).

10.4.7.2 Rate of Change Operational

TIA-942-A: maximum rate of change is 5 °C (9 °F) per hour.

NEBS: maximum rate of change is 30 °C (54 °F) per hour.

ASHRAE: maximum rate of change is 5 °C (9 °F) per hour.

10.4.7.3 Additional Information

ASHRAE *Thermal Guidelines* specifies allowable and recommended environmental limits for four classes of environments and NEBS in both “product operation” and “power off” modes. For a typical operating computer room, the ASHRAE Class 1 recommended conditions apply and are noted below. See Table 2.1 in *ASHRAE Thermal Guidelines* for all other conditions. Of note, TIA guidelines correspond to the ASHRAE Class F1 Recommended conditions.

ASHRAE *Environmental Guidelines* specifies that the recommended maximum dry-bulb temperature should be derated by 1 °C/300 m above 1800 m (1.8 °F/1000 ft above 6000 ft).

10.4.8 Humidity Control

10.4.8.1 Recommended Operational Relative Humidity

TIA-942-A: 40% to 55%

NEBS: Maximum 55%, a generally accepted telecommunications practice, and no NEBS requirements exist

ASHRAE: 60% maximum relative humidity; dew point (absolute humidity) is between 5.5 °C (42 °F) and 15 °C (59 °F)

10.4.9 Temperature And Humidity Control—Tape Media

ASHRAE: *ASHRAE Thermal Guidelines* notes that environments for tape products are more critical than computer equipment. This footnote sets ASHRAE Environmental Class A1 as the standard and includes limits for humidity rate of change.

10.4.10 Maximum Dew Point

10.4.10.1 Recommendations

One of the more practical considerations regarding dew point temperature limits in a computer room is to avoid cold surfaces in the computer room. If equipment is brought into the room when its surface temperature is below the room dew point, condensation on that cold surface will occur. The same is true for building components; insufficient insulation of an exterior wall or roof assembly could result in a surface temperature below the room dew point with condensation resulting.

10.4.10.2 Maximum Dew Point

TIA-942-A: 21 °C (69.8 °F)

NEBS: 28 °C (82 °F)

ASHRAE: 15 °C (59 °F)

Dew point temperature, dry bulb temperature, and relative humidity are interrelated conditions; any two of these parameters defines the third.

10.4.11 Altitude

10.4.11.1 Maximum Altitude

NEBS: 4000 m (13,000 ft)

ASHRAE: 3050 m (10,000 ft)

Maximum altitude is specified to account for the limitations of HVAC equipment.

10.4.12 Noise Levels

Room air distribution noise level should follow guidelines as established by ASHRAE and be at or below the maximum level of NC-45 using the Beranek Noise Criteria (NC) Method.

10.4.13 Leak Detection

Leak detection should be provided at any location where water can exist or at the very least where water is most likely to exist. The most common sources of water are leakage from piping or valves and condensation on cooling coils in HVAC equipment. Whenever possible, install leak detection in drip pans below the areas that have the highest leak potential. Drip pans can minimize the amount of leak detection equipment required and provide some degree of containment.

In piping systems, leakage will most likely occur at screwed or flanged connections, at valve stems, or at unions. Welded or soldered joints in piping have a much lower leak potential. However, especially in insulated piping systems, water can “travel” along a sloped pipe and drip off many feet from the source of the leak. A continuous drip pan below piping, with either spot or continuous detection, is desirable.

If drip pans are not feasible, the piping should be equipped with leak detection cables installed directly within the thermal insulation to provide for early leak detection. Additional leak detection cables should be installed below the piping on the floor in areas with screwed or flanged connections or valves.

Air handling units should be provided with drip pans below with spot detection in the drip pan. If drip pans are not feasible, a loop of leak detection cable around the unit will detect but not contain a leak. The most common failure modes in air handlers that result in leaks are:

- Failed condensate pump. Gravity drainage is always preferable to a pump.
- Overflow of condensate drain pan. This happens either because of plugging of the outlet with biological material growing in the pan, or the result of an improperly configured drain trap.
- Leaking coil connection.

10.5 Thermal Management

10.5.1 Introduction

Effective heat removal from computer equipment requires attention to the direction of airflow. An important part of thermal management of air-cooled electronic equipment is air management. Selection of the appropriate HVAC system and equipment are made based on many factors. There is no single HVAC solution that is appropriate for all data centers, and some systems may be inappropriate for a particular combination of factors. Each of the factors noted below, either individually or in combination, can have a significant impact on the selection of the appropriate system and cooling equipment:

- Room size
- Overall cooling density (watts per square meter or watts per square foot), which is established by the maximum kW load for the computer equipment used in the electrical design. Cooling load should match actual operating load as opposed to nameplate load
- kW per cabinet or module
- Number and capacity of HVAC units required to meet load and redundancy criteria and their location in the space relative to computer equipment layout
- Room location relative to mechanical support spaces
- Room location in the building relative to outdoors
- Ceiling height
- Absence or presence of access floor
- Access floor height
- Future expansion needs
- Reliability requirements
- Available maintenance personnel
- Local climate

As the cooling load and power density increase, selection of the appropriate HVAC system becomes more and more critical. Refer to GR-3028-CORE for a definition of Room Cooling (RC) and Supplemental Cooling (SC) Classes for equipment environments.

Datacom Equipment Power Trends and Cooling Applications and *ASHRAE Design Considerations* provide in-depth descriptions of data center HVAC systems and equipment.

10.5.2 Use Of Operating Rather Than Nameplate Load

ITE manufacturers now provide heat release data to allow more effective planning of cooling system capacity. Using this data will result in significantly more accurate estimates of the heat release than by applying a derating factor to nameplate electrical ratings. *ASHRAE Thermal Guidelines* provides a template for ITE manufacturers to use in reporting heat release and airflow (volumetric flow rate and configuration). Data is provided for Minimum, Full, and Typical configurations, and some manufacturers also have configuration tools available to allow for more accurate estimation of specific hardware configurations.

10.5.3 Current Equipment Heat Release and Trends

Datacom Equipment Power Trends and Cooling Applications provides estimates of power and cooling trends through the year 2020 for various hardware platforms. In all cases, these densities are well in excess of the cooling ability of most existing data center HVAC systems. The value of the trend charts is for forecasting a data center life capacity plan based on an actual baseline starting point, regardless of the year designation on the trend lines. Based on some anticipated number of technology refreshes and associated application proliferation over the life of the data center, the trend line slopes provide valuable planning thresholds.

10.5.4 Equipment Heat Release Specifications

10.5.4.1 Recommendations

Whenever possible, power and cooling requirements for electronic equipment should be determined based on the manufacturer's actual published data for the specific configuration in question. GR-3028-CORE and *ASHRAE Thermal Guidelines* propose a standardized template for equipment manufactured to report power and cooling requirements for use by both end users and the designers of power and cooling infrastructure.

In the absence of the data noted above, refer to *Datacom Equipment Power Trends and Cooling Applications* to estimate power and cooling requirements. Within this document is a method for planning a data center based on equipment, applications, and space and both historical data and future trends for equipment power and cooling requirements for the typical data center platforms.

10.5.4.2 Additional Information

ASHRAE Thermal Guidelines includes an example of a Thermal Report. In this example, the Nominal Airflow column is where the manufacturer will report the air volume moved through the electronics by the internal server fans. For any particular row of racks, the total of all server airflows in that row represents the total airflow through the racks from the cold aisle to the hot aisle. This is not the same as the volume of air that must be supplied to the cold aisle by the HVAC system. The HVAC system must supply more air since the temperature difference produced by the HVAC equipment will generally be lower than the temperature rise through the electronics equipment, because of bypass air waste and related mixing of supply air and return air.

10.5.5 Electronic Equipment Cooling

10.5.5.1 Recommendations

TIA-942-A: Equipment that utilizes front-to-rear cooling schemes should be used in conformance to TIA-942-A and *ASHRAE Thermal Guideline*, so as not to disrupt the functioning of hot and cold aisles.

Also refer to NEBS GR-3028-CORE: Airflow Protocol Syntax (EC-Class).

Equipment cabinet air inlet temperature measurement points should be selected in accordance with *ASHRAE Thermal Guidelines*.

10.5.6 Humidification and Dehumidification Equipment

10.5.6.1 Location of Humidification and Dehumidification

Humidification and dehumidification may be located at either the CRAC units or the central air handlers.

10.5.6.2 Additional Information

A study of local environmental conditions in conjunction with building construction will determine requirements for humidification/dehumidification. If ultrasonic humidifiers are used, deionized water should be provided to prevent formation of dust from dissolved solids in the water. If availability of deionized water over the life of the data center is uncertain, ultrasonic type humidifiers should be avoided.

The integrity and construction of the building envelope, use of vapor barriers, pressurization of the computer room relative to adjacent spaces, and the conditioning of outdoor air supplied to the space must be considered in the context of local environmental conditions when selecting a humidity control scheme. If a central steam boiler used for building heating is also used for direct steam humidification, the type of boiler water chemicals should be considered. Generally, steam generating humidifiers (using electricity, natural gas, or steam as the energy source) have a lower life cycle cost than ultrasonic humidifiers, which need deionized water in the ultrasonics. Evaporative humidifiers can be very effective and save energy when air from the hot aisle is used to evaporate water. Refer to the *ASHRAE Handbook* for design considerations.

Humidifiers and reheat coils can be included in individual CRAC units. However, when two or more CRAC units are in a space, care should be taken to ensure that the controls and sensors are calibrated so that individual units do not fight each other (e.g., some humidifying while others are dehumidifying). It may be beneficial to use a centralized humidification system to avoid this issue as well as for ease of maintenance. Refer to *ASHRAE Design Considerations* for information on different types of humidification systems.

10.5.7 Air-side Economizer Systems

Air-side economizer systems are gaining acceptance as data center cooling solutions, in part, as a result of the potential of significant cooling energy savings. These systems will require a thorough, engineered evaluation because of site specific conditions that can have an important impact on their viability. Additionally, computational fluid dynamic modeling (CFD) should be considered to help evaluate operation over an expanded range of thermal conditions. An air-side economizer system brings filtered outside air directly into the data center for distribution to the servers. The heated exhaust air from the servers is simply directed outside instead of being cooled and re-circulated. When the outside air is particularly cold, the economizer may mix it with the heated exhaust air so that its temperature and humidity fall within the desired range for the server equipment. The air-side economizer can be either a specially designed component or an integrated operation in a large central air handling system with ducting for both intake and exhaust air. In either case, air filters reduce the amount of particulate matter, or contaminants, that are brought into the data center. Outdoor contaminate risk will always need to be considered, however. When data centers must be cooled 24/7, 365 days per year, air-side economizers may be economically feasible even in hot climates where they can take advantage of cooler evening or winter air temperatures.

10.5.7.1 Recommendations

Displacement ventilation can be an effective method of cooling data center equipment as long as the equipment configuration is taken into account. Vertical displacement should be considered in rooms with multiple rows of racks, allowing the heat plume to rise in the same direction as the ventilation.

Horizontal displacement system design should avoid return air path crossing through cold aisles.

10.5.7.2 Additional Information

Horizontal displacement systems will be limited by the maximum cooling density, physical configuration of the room, and the size range of commercially available CRAC units that are designed for displacement applications.

10.5.8 Supplemental Cooling

Supplemental cooling systems are any method of heat management that is added to an existing data center to supplement the primary or original cooling system, either by mitigating local hot spots or by adding cooling capacity. *Design Considerations* lists five common approaches to supplemental cooling. Each of these approaches is aimed at increasing the local cooling effect by one of the following means:

- Improving or regulating air circulation either at the inlet or discharge of the ITE cabinet or rack
- More closely coupling cooling equipment with the ITE
- Isolating hot and cool airstreams from one another to reduce recirculation or mixing
- Directing cool air from the cooling equipment discharge into the ITE inlets
- Directing hot air from the ITE discharge into the return air path to the cooling equipment

Well-designed airflow management brings significant performance and efficiency benefits. Every opportunity to improve air circulation and isolate the hot and cold airstream should be considered in the design of primary cooling systems for new data centers. These techniques can also be applied to correct hot spots or when expansion of the primary system is too costly or disruptive to correct the problem at hand.

The choice of supplemental cooling systems depends partially on whether the problem is a shortfall of cooling capacity, or lack of cooling effectiveness. A capacity shortfall can only be addressed by systems that provide heat rejection to the outdoors or to an existing system such as chilled water. System effectiveness problems are most likely the result of airflow deficiencies, which may be improved by airflow solutions.

10.5.8.1 In-Room

Supplemental chilled water room cooling units may be used to cool room hot spots when floor space and chilled water are available in accordance with the system descriptions of GR-3028-CORE.

10.5.8.2 In-Frame

Supplemental in-frame chilled water-cooling may be used where water can be introduced into the computer room and where a solution does not exceed the standard cabinet floor utilization specifications to deliver the cooling benefits described in GR-3028-CORE.

10.5.8.3 Direct Return

Direct return air systems may increase the cooling capacity of the supply duct system when equipment is located per GR-3028-CORE and has an acceptable interface between the equipment exhaust and the ductwork.

One method of direct return is to install rack-mounted fan air-removal units to capture 100% of the exhaust air from each rack and direct the hot air to an overhead return air plenum. This solution works well as a solution for isolated hot spots or for new installations. Because it requires unique ducting on every rack, some of the benefits can be offset by the cost and reduced flexibility.

Another method of direct return is to install barriers that will channel 100% of the hot exhaust air from a rack into an adjacent row-integrated cooling unit. This solution is very effective for extreme high-density applications.

A third method of direct return is to use row-integrated air conditioning units and a totally enclosed hot aisle. The hot aisle becomes the return duct to all cooling units installed on either side of the hot aisle. This method is effective when there are many high-density racks in close proximity, thereby creating a high-density zone within the computer room. Provisions must be provided to comply with local codes for smoke detection and fire suppression within the enclosed aisle.

A weakness of direct ducting is that the delta temperature (ΔT) will typically exceed the range of DX cooling units with one possible result being a resultant increase in the supply air temperature. This can be addressed by specifying standard water-cooled units or special DX cooling units that operate efficiently at wider ΔT s.

Loosely coupled direct ducting in the ceiling plenum space provides opportunities for “conditioning” the return air with ceiling grates that would allow for some mixing with bypass make-up air. In addition, in environments where there might be reason for mixing ducted exhaust cabinets with standard cabinets, the ceiling grills would be required to move the free-space return air from the room and introduce it into the return air path in the plenum. This could occur where there were high-density cabinets mixed in a room with low- or moderate-density.

A fully deployed ducted exhaust system also greatly reduces the detail management of air delivery to just setting the overall room temperature and ensuring it is pressurized just above the consumption rate of the room’s cumulative load. This eliminates the negative effects of low-pressure vortices formed under the floor by cycling between air handlers for service and maintenance.

10.6 Computer Room Cooling

10.6.1 General Considerations

HVAC systems and cooling equipment must always be selected using a holistic approach. The choice of air distribution method should never be considered without evaluating other significant factors, such as whether or not an access floor is used, the return air path, location of CRAC units or air handling equipment relative to server racks, orientation of hot/cold aisles, ceiling height, methods for humidity control, and provisions for future expansion, to name just a few. Each choice affects the others, and the overall performance of the data center cooling system will be dictated by the entire package of decisions. *Datacom Equipment Power Trends and Cooling Applications* and *ASHRAE Design Considerations* provide general descriptions of the various air delivery methods and some of the cooling system technologies available, but they do not provide hard and fast rules for selection since there are so many combinations of the factors noted above. A knowledgeable and experienced data center HVAC engineer/consultant is essential to achieve a successful outcome.

10.6.2 Access Floor Versus No Access Floor

The necessity or use of an access floor for any particular data center depends on a number of factors. As with the selection of an HVAC system, access floor decisions should be made as part of a larger consideration of needs and requirements, many of which are unrelated to the mechanical system.

Advantages of access floor with underfloor air distribution:

- Allows great flexibility in location of load to CRAC unit
- Imposes fewer limits on locating CRAC units in the space
- Piping services may be concealed below the access floor

<List continues on next page>

- More compatible with gravity condensate drainage from cooling coils and humidifiers
- No overhead supply ductwork to obstruct the return air path or to interfere with lighting, sprinkler heads, or overhead power/cable distribution systems
- Permits the use of nearly any cooling technology, regardless of air supply/return configuration

Disadvantages of access floor for HVAC:

- The underfloor space is an air distribution plenum—all cable must be listed for data processing or plenum rated for flame spread and smoke developed characteristics or installed in conduit, (See Section 14.7 for considerations of overhead versus under-floor cable routing).
- Poor planning of underfloor utilities can result in blocked airflow and poor cooling performance.
- Poor management of cable openings can result in reduced airflow at perforated tiles, supply air grilles, or other supply air openings.
- Recent research suggests that overhead cooling delivery may be capable of producing more favorable rack cooling efficiency than underfloor cooling. (Herrlin, M. K. and Belady, C. 2006. *Gravity-Assisted Air Mixing in Data Centers and How it Affects the Rack Cooling Effectiveness*. ITherm 2006, San Diego, CA, May 30–June 2, 2006)

Access floors have traditionally been the first choice for medium to large rooms with higher power/cooling densities. A factor in this has been the commercial availability of specialized data center HVAC equipment.

Several HVAC equipment manufacturers now offer equipment capable of cooling very high-density loads with localized overhead or horizontal air distribution. This equipment is sometimes suited to specific heat rejection technologies and may not be appropriate for all buildings.

Access floors offer fewer air distribution advantages for small data centers. Smaller HVAC equipment can perform very well in small spaces where the electronic equipment is in close proximity to the HVAC unit.

10.6.3 Hot Aisle/Cold Aisle Concept

10.6.3.1 Recommendations

NOTE: See *ASHRAE Thermal Guidelines* for a more in-depth discussion of hot and cold aisles.

The hot aisle/cold aisle concept for arrangement of computer equipment in the computer room should be used, regardless of whether air distribution is overhead or supplied from an access floor plenum.

10.6.3.2 Additional Information

Conventional wisdom regarding data center supply air considers recirculation of return air from hot aisles to cold aisles as a condition to avoid. The following example illustrates this and also why controlling environmental conditions based on relative humidity is difficult:

With the ASHRAE Class 1 recommended equipment inlet conditions of 18 to 27 °C (64.4 to 80.6 °F) (dry bulb temperature) and a relative humidity range of 40% to 55%, server exit conditions are very often close to 38 °C (100 °F) and 20% RH. The typical CRAC unit supplies air between 13 and 16 °C (55 and 60 °F) and close to 90% RH; clearly conditions that are outside the range required by the typical server manufacturer. To achieve 18° to 27 °C (64.4° to 80.6 °F) at the server inlet, mixing between hot and cold airstreams must occur in the proper proportion, and the resultant air should be uniformly distributed along the entire server rack, top to bottom, unless supply air and return air can be completely isolated from each other and the supply air can then be delivered within the required use parameters. Since server fans generally vary the airflow to maintain a balance between temperature and power consumption, the airflow through the server cabinets is not constant.

The temperature and relative humidity displayed on the CRAC unit control panel is measured at the inlet to the CRAC unit. This temperature represents the mixed condition of all the air that makes it back to the CRAC unit. In most data centers, the CRAC unit temperature set point is set between 20 to 25 °C (68 to 77 °F), and the CRAC unit operates to maintain this temperature. This tells the data center manager/operator that enough hot aisle air has mixed with enough cold aisle air in the space between the CRAC unit and server racks to ensure that the right conditions exist at the CRAC unit inlet, but it tells nothing of the conditions that are most important—the actual temperature at the server inlets. For the condition described above to exist, the air temperature at the server inlets will be well below the temperature range recommended by ASHRAE with a corresponding elevation of relative humidity.

Airflow in the typical data center consists of two flow loops:

- CRAC units (a few big fans) circulate air within the entire room.
- Servers (many little fans) circulate air between cold and hot aisles.

These loops are “decoupled;” they do not depend on each other, and one will continue to operate if the other is shut off, or if the flow rates do not balance. Hot air is buoyant and will tend to rise, and all air will take the path of least resistance relative to the room pressure gradients. Air will tend to flow back toward the CRAC unit inlets, but the greater the distance from the CRAC unit, the less momentum the air mass has to overcome turbulence.

Each of the two airflow loops described above operates with a different temperature difference between inlet and supply. However, the energy must balance between the two; all of the heat rejected from the servers must be further rejected in the CRAC unit. Therefore, the relative airflow rates of the two loops will be proportional to the temperature difference of each loop. The air temperature rise through servers is not constant since most servers use variable speed fans to balance CPU temperature, power consumption, and noise, but 11 to 17 °C (20 to 30 °F) is common. CRAC units typically will operate at a constant volume, and varying temperature rise based on load, depending on the type of cooling technology employed. A typical CRAC unit temperature difference is 8 to 11°C (15 to 20 °F) (depending on whether the CRACs are chilled water units or are air/glycol cooled). The CRAC unit loop can circulate 50% more air than the sum of all the server fans.

The “ideal” data center HVAC design would supply air at the server inlet at the desired inlet temperature and at a volume that matches the server fans. All hot aisle air would be returned to the air-handling units with no mixing or recirculation between hot and cold aisles. When such isolation cannot be achieved, careful attention must be paid to monitoring server intake supply air to be sure the proper calibration is maintained of the mix of source air and return air.

10.6.4 Access Floor

10.6.4.1 Recommendations

The type of air delivery method through an access flooring system should be consistent. Do not mix perforated tiles with supply air grilles as the differences in flow/pressure drop characteristics will result in inconsistent and unpredictable performance. Similarly, large, relatively unobstructed openings in the access floor can have significant adverse effects on the underfloor pressurization and should be avoided as the larger the opening, the smaller the pressure drop corresponding to a particular cubic meters or feet per minute. Since air takes the path of least resistance, large openings will starve the perforated floor tiles. *Large* means any opening that is large relative to a single perforation in an access floor tile. Many (relatively) small openings can begin to look to the HVAC system like a few very large openings.

Cable penetrations into the bottom of cabinets should be filled to minimize the flow of air directly into the cabinet from below. The area of the unobstructed portion of a cable opening looks to the HVAC system like a large opening. It is not uncommon for unprotected cable cutouts to allow up to half of the total CRAC unit airflow capacity to bypass the perforated tiles.

An access floor system provides a flexible method of delivering cooling to data centers, allowing for numerous configurations. Perforated panels can readily be moved to accommodate high heat load areas. Floor height should be selected based on the combined needs for airflow, power distribution, network/communications cabling, and chilled water distribution, if used. Access floor heights greater than 900 mm (36 in) introduce additional cost to the flooring system, may require special considerations for access and safety, and do not significantly enhance the uniformity of air distribution below power densities of 1350 W/m² (125 W/f²). For data centers with power densities in the 1610 to 2150 W/m² (150 to 200 W/f²) range, a 1060 mm (42 in) access floor depth should be considered.

Chilled air should always be delivered into the cold aisle in front of the cabinets and not be delivered directly into the bottom of the cabinet. There are three main reasons for this:

- 1) Openings provided below the racks for this purpose will generally be large compared to the tile perforations.
- 2) Some of the air will bypass out through the back of the rack into the hot aisle.
- 3) Air supplied directly into the bottom of a cabinet may be significantly below the minimum temperature prescribed in *ASHRAE Thermal Guidelines* or GR-3028-CORE. CRAC unit discharge air temperatures are typically in the 13 to 16 °C (55 to 60 °F) range, and 80% to 90% RH at that temperature. With underfloor distribution, the air coming out of the perforated tiles will usually be below 20 °C (68 °F).

Room temperature measurement points should be selected in conformance to *ASHRAE Thermal Guidelines*:

- Temperature measurement sensors should be regularly calibrated.
- A significant difficulty with temperature and humidity measurement point locations is the physical installation in meaningful locations. Sensors typically must be mounted on a fixed surface, making the mid-aisle 1500 mm (60 in) above floor locations impractical for permanently installed devices. Temperature and humidity sensors furnished with CRAC units are factory installed in the units at their inlet and do not indicate the conditions of the air at the computer equipment inlets.
- Temperature-measuring points should ideally mimic the equipment inlet conditions since these conditions define the equipment comfort.

Floor plenums should be as airtight as possible relative to adjacent spaces and cleaned prior to being put into use.

10.6.5 Overhead Air Distribution

Overhead air distribution can be used effectively, although it will generally not be as flexible for future equipment placement as underfloor supply. Fixed diffuser locations limit reconfiguration.

Overhead ductwork must be closely coordinated with lighting, sprinklers, and power or network cabling in data centers where these utilities are not located below an access floor. Overhead ducts wider than 1200 mm (48 in) will require sprinkler heads to be located below the ductwork.

Supply air should be placed in the cold aisles only.

Outlet airflow should be 0.38 to 0.47 m³/sec (800-1000 CFM) per GR-3028-CORE, which is based upon the *ASHRAE Handbook* for system specifications of vertical overhead delivery.

10.6.6 Row-Integrated Cooling

For ITE that takes cool air in the front and discharges hot exhaust air out the back, cooling units can be applied within the rows of equipment racks. The cooling units should be designed for row integration with an airflow pattern from back to front. These types of units, which can be refrigerant or chilled water based, are designed to capture the hot air being exhausted out the back of the equipment into the hot aisle and to discharge cool supply air into the cold aisle in front of the racks. By placing the cooling units very close to the heat source (ITE), the path that the hot air must take to return to an air conditioner can be greatly reduced, thereby minimizing the potential for mixing of hot and cold air streams. Fan power can be lower, and capacity and efficiency can be higher because of the higher return air temperatures to the cooling units. The high return air temperatures also lead to a very high sensible heat ratio, minimizing the amount of unnecessary dehumidification (and a subsequent need for rehumidification to maintain constant humidity levels).

This type of configuration can work well for low- to medium-density loads. For higher densities, it is possible to install a containment barrier around the entire hot aisle to ensure that all of the hot exhaust air is directed into a cooling unit, thereby eliminating any mixing of hot exhaust air with the cool supply air.

10.6.7 Equipment Layout

Printers and other potential contamination sources should not be located in the computer room.

Cabinets and racks shall be arranged in rows with fronts of cabinets/racks facing each other in a row to create hot and cold aisles. Equipment should be placed in cabinets and racks with cold air intake at the front of the cabinet or rack and hot air exhaust out the back, top, or both. However, reversing the equipment in the rack will disrupt the proper functioning of hot and cold aisles. Blank panels should be installed in unused cabinet and rack spaces to improve the functioning of hot and cold aisles.

When placed on an access floor, cabinets and racks shall be arranged to permit tiles in the front and rear of the cabinets and racks to be lifted. Cabinets should be aligned with either the front or rear edge along the edge of the floor tile per TIA-942-A.

Cabinet size, location for air entry, location for cable entries, and access to front and rear should be planned for consistency according to ETSI EN 300-019.

CRAC units should be located in the hot aisle path when the return air path is the free space in the room (e.g., not ducted to the CRAC unit inlet).

10.6.8 Supply Air Layout

When underfloor cooling is used, perforated access floor tiles should be located in the cold aisles only to support the functioning of the hot and cold aisles. For an overhead air distribution system, the supply diffusers should be placed above the cold aisles only.

10.6.9 Return Air Layout

Return air should be positioned to capture the highest heat concentration such as return air intakes directly over the hot aisles or directly over equipment producing the highest heat. Capturing the heat with return grilles and not entraining it in the supply air should be the goal of return and supply layouts. When using a return air system to reduce recirculation, supply air temperature must be controlled to very near the lowest acceptable equipment inlet temperature.

A ceiling height of at least 3 m (10 ft) above the access floor will allow for an effective hot air area above cabinets and racks and optimize the return air path. Rooms with high-density cooling loads should consider ceilings higher than 3 m (10 ft).

10.6.10 Cable Management

The cold aisle plenum space should remain unobstructed by raceways in conformance to TIA-942-A.

Floor tile cutouts for cable egress to cabinets and damping around cables should conform to TIA-942-A.

When overhead cable systems are used in lieu of or in addition to underfloor cabling, placement and grouping of cable should be planned to minimize the effects on return air. Obstructions in the return air path could contribute to higher levels of hot air recirculation to the cold aisles, depending on the configuration of the cable system relative to the rack layout (refer to Section 14.7 for additional considerations of overhead versus under-floor cable routing).

Telecommunications cabling under the access floor should run parallel to CRAC air delivery path in accordance with applicable standards (e.g., BSRIA BG 5/2003). Where the cable pathways cross the front of the air delivery system care should be taken to reduce the impact on the air flow.

Cables shall not be left abandoned under access floor, in overhead raceways, or above suspended ceilings. Inactive cables shall be removed or terminated on at least one end and marked “for future use”.

10.7 Mechanical Equipment (Design and Operation)

10.7.1 General Recommendations

Most of the following recommendations and topics are also addressed in more detail in the *Design Considerations for Data and Communications Equipment Centers*.

HVAC availability and redundant power access should conform to the requirements of the Class that best satisfies the reliability goals of the enterprise. The Class chosen will then drive selection and configuration of the HVAC systems and equipment selected. For example, providing CRAC units and other mechanical cooling equipment with dual power sources to ensure continuous operation if one source of power is lost is to be considered for Class F3 and Class F4 but is not mandatory under the requirements of this standard and is not required for Class F2 or lower facilities. Mechanical equipment, including specialized mission-critical equipment, such as CRACs, is not offered by manufacturers with provisions for dual power sources as a “standard option.” Specifying this feature for mechanical systems should be done only after careful consideration of the costs and complexities involved compared to alternative approaches to achieve the same or similar result.

Use mechanical equipment that is designed for mission-critical installations.

Air ducts, water pipes, and drain pipes not associated with the data center equipment should not be routed through or within the data center spaces.

Electrical power for mechanical systems should be on generator backup.

There should be two independent sources of water for the HVAC systems or one source and on-site storage.

Air filters in air conditioning equipment should have a Class F1 rating. Class F1 filters are less able to support combustion than Class F2 filters.

Duct coverings and insulation should have flame spread ratings less than 25 and smoke developed ratings less than 50.

In areas where there is no equipment to cool, replace perforated tiles with solid tiles and close air ducts.

Mechanical equipment should be anchored to the elements that support them. Equipment that vibrates should be mounted on vibration isolators. The vibration characteristics of the floor should be carefully reviewed.

10.7.2 Computer Room Air Conditioning (CRAC) Units

10.7.2.1 Recommendations

At minimum, each computer room in a Class 2 or higher data center should have one redundant CRAC/CRAH although analysis-using tools, such as computational fluid dynamics modeling, may determine that more than one redundant CRAC/CRAH may be required to maintain adequate airflow to all areas of the room.

Set points for CRAC and CRAH units should not be set lower than necessary to keep temperature at the equipment air intakes (in the cold aisles) between 18 to 27 °C (64.4 to 80.6 °F). The temperature in the hot aisles is not a concern if the temperature at equipment air intakes is within these temperature ranges and does not exceed the safe operating limit for wiring and equipment in the hot aisle.

Set points for CRAC and CRAH units should not be any higher (or lower) than required to keep relative humidity below 60% and a dew point between 5.5 to 15 °C (42 to 59 °F). Do not unnecessarily humidify or dehumidify air. Additionally, to prevent CRACs/CRAHs from working against each other to control humidity, set all CRACs/CRAHs to the same humidity settings and use a 5% dead-band on humidity set points.

Arrange CRACs/CRAHs and air ducts to enhance the proper functioning of hot and cold aisles. If CRACs/CRAHs are not fully ducted for both air intake and discharge, they should be arranged perpendicular to rows of equipment. Any air intake ducts should be placed in hot aisles. Perforated tiles and tiles with supply grilles should be placed in cold aisles. Overhead supply should be designed to direct air downward into the cold aisle, not laterally, or into hot aisles.

Return ducts for CRACs/CRAHs placed on the room perimeter should be placed as high up in the ceiling as possible and be aligned with hot aisles.

In computer rooms with an access floor, CRAC units located in the room should be supported independently such that they do not transmit vibration to the access floor system.

10.7.3 Central Air Handlers

Central air handlers are preferred over CRAC units when a ducted supply or return air system is used. CRAC units are packaged systems that do not offer the designer the flexibility to tailor the fan selection to match the duct system performance.

Central air handlers can allow the use of air-side economizers for improved energy efficiency when the physical configuration of the building and geographical location (e.g., local climatic conditions) are favorable.

A central air handler designed system can also be located outside the IT server room, which may be an advantage in some cases such as security or space needs.

10.7.4 Supplemental Cooling Systems

Supplemental cooling is typically used to mitigate thermal issues that cannot be effectively resolved by existing cooling system design alone. These auxiliary methods may include:

- Spot cooling
- Cooled cabinets
- Rear door heat exchangers
- In-row cooling

The following types of redundancy for supplemental cooling may be required in addition to redundancy for power to support them:

- Backup supplemental systems
- Generator feed for supplemental cooling systems
- Dual power feeds for supplemental cooling systems

10.7.5 Chilled Water Systems

Systems using chillers as the primary cooling source (with either chilled water CRAC units or built-up air handling systems) can be more energy efficient than systems using air-cooled packaged CRAC units. Packaged air-cooled machines can be less efficient than straight air-cooled CRACs, but offer benefits other than efficiency. Chilled water systems overcome distance limitations on air-cooled CRAC refrigerant piping, allow free-cooling in many climates, and enable thermal storage. Chillers are not as cost effective for smaller systems. There is no strict load that defines smaller, but in general, critical loads below 300–400 kW may be too small to provide economic justification for installation of a chilled water system unless the load is expected to grow significantly over the life of the facility. Each project must be evaluated to determine the suitability of chilled water compared to other cooling solutions.

The entire chilled water system consists of chillers, pumps, cooling towers, controls systems, water treatment, and chilled water distribution piping. Many configurations are possible to achieve alignment with the reliability goals established for the data center.

If dual power paths are provided to the individual components in a chilled water system, the use of transfer switches, either manual or automatic, must be provided at each system component.

10.7.6 Chillers

The chiller technology chosen can depend on the size of the load served and the availability of space indoors in a dedicated equipment room. Chillers located outdoors will be packaged, air-cooled units with capacity limited to approximately 500 tons each. If larger chillers are desired, indoor units must be used. Equipment located indoors is better protected from physical and environmental hazards and may receive better service from maintenance personnel.

10.7.7 Cooling Towers

10.7.7.1 Introduction

Dry cooling towers operate by heat transfer through a surface that separates the working fluid from ambient air, such as in a tube to air heat exchanger, utilizing convective heat transfer. They do not use evaporation.

Wet cooling towers or open circuit cooling towers operate on the principle of evaporative cooling. The working fluid and the evaporated fluid (usually water) are one and the same.

Fluid coolers or closed circuit cooling towers are hybrids that pass the working fluid through a tube bundle, upon which clean water is sprayed and a fan-induced draft applied. The resulting heat transfer performance is much closer to that of a wet cooling tower with the advantage provided by a dry cooler of protecting the working fluid from environmental exposure and contamination.

10.7.7.2 Recommendations

For Class F3 and Class F4 facilities, a reliable backup source of water or water storage must be provided.

10.7.7.3 Additional Information

Evaporative cooling towers are generally the most maintenance intensive part of the chilled water system. When evaporative towers are used, installation and maintenance of a condenser water treatment system is essential. Evaporative towers are dependent on a steady source of makeup water (typically domestic, potable water) to provide heat rejection of the building load. Interruption of this water supply will result in a complete cooling system shutdown.

10.7.8 Thermal Storage

10.7.8.1 Recommendations

The thermal storage system should be designed for the simplest operation with the minimum number of components that must operate and start.

10.7.8.2 Additional Information

Goals for thermal storage as a concept must be clearly defined and understood by all parties and coordinated with the electrical system design. The purpose and function of the thermal storage system will define the scope and design of the system. Site considerations are important as some sites do not have adequate space for thermal storage.

Thermal storage systems for data centers are used to provide chiller load leveling and short-term cooling at times such as during a chiller short-cycle lockout. In this case, the energy stored in the thermal storage tank may be required to be available at the point of use in less than two minutes.

10.7.9 Piping And Pumps

10.7.9.1 Recommendations

The most effective way (e.g., practical, cost effective) to accomplish “dual path” supply in a chilled water system is to provide a looped piping system, allowing both ends of the loop to be supplied from the chiller plant. Dual piping systems are not practical for most data centers as they introduce significant cost and complexity.

A piping loop may be installed below the access floor on its perimeter, or preferably, outside the room. Sectionalizing valves installed at intervals in the loop will permit isolation of one or more CRAC units or air handlers for servicing a leaking isolation valve at the unit inlet. If a sectionalizing valve is installed between each CRAC unit branch pipe, then two adjacent CRAC units would need to be shut down to isolate a single leaking sectionalizing valve. An alternative method for valve servicing is to freeze the pipe.

10.7.9.2 Additional Information

Circulating pumps, dry coolers, and close-circuit fluid coolers (where used) are subject to the same restrictions regarding dual power as chillers—automatic or manual transfer switches must be installed as part of the electrical design.

Piping itself is very reliable, especially when care is taken in the design and water quality is maintained. Catastrophic failure of piping is rare when compared to other failure modes such as slow leaks from threaded joints or valve stems and end connections. These concepts should be kept in mind when evaluating designs to achieve high reliability.

Thoughtful design and layout coordinated with the reliability goals of the data center are essential. For example, adding more valves for isolation is not a solution by itself as installing more valves may only increase the likelihood of failures. Instead, the use of very high quality valves (industrial quality versus commercial quality) can be a cost effective way to achieve higher reliability levels. In the vast majority of data centers of all Classes, commercial quality valves are or will be installed.

10.7.10 Plumbing

10.7.10.1 Additional Information

The following additional items should be considered when planning plumbing for data centers:

- Domestic water
- Tempered water—safety shower/eyewash equipment
- Sanitary sewer
- Storm drainage system

10.8 Materials and Finishes

10.8.1 Introduction

Problems can arise if the materials used are of an improper size, strength, or spacing. Finishes must be suitable and not cause danger to persons or equipment.

10.8.2 Materials in Air Plenums

10.8.2.1 Requirements

Materials, such as wire and cable jacketing, plastic piping, and insulation jacketing shall meet all code and Listing requirements (e.g., flame spread and smoke developed characteristics) as per the AHJ. Additionally, all materials installed in air plenums shall meet installation requirements of the AHJ.

PVC piping shall not be used within air plenums.

10.8.2.2 Additional Information

Many AHJs have additional requirements for telecommunication, BAS, or other non-electrical cabling located within access flooring. An example is that plenum-rated or LSZH cable may be the minimum performance required concerning flame spread and smoke development.

CPVC piping with an appropriate rating is available and may be used within plenums if allowed by the AHJ.

This page intentionally left blank

11 Fire Protection

11.1 Introduction

Because fire protection regulations differ between countries and jurisdictions, the designer must use the appropriate local codes and standards. The following section describes the best practices in the United States and can be used for guidance in other locations as although the codes and standards may differ, the safety philosophy and best practices employed will be similar.

11.2 Basic Design Elements

The basic design elements of fire protection are:

- Fire suppression—extinguishing systems to protect the data processing equipment.
- Fire detection—smoke, heat, and early warning detectors connected to an alarm and monitoring panel.
- Fire alarm system—a system, including the fire detection systems, with a means to automatically send alarm, supervisory and trouble signals to a central station, security center, fire department, or other approved, constantly attended location, and warn occupants of the presence of smoke, heat, or fire through the use of audible or visual alarms.

11.3 General Requirements and Recommendations

11.3.1 Requirements

The computer room shall be separated from other areas or occupancies within the building by fire-resistance-rated construction. Refer to Section 7.5.7 for minimum fire rating of spaces.

The computer room shall have a fire protection system. If the computer room is located in a sprinklered building, the computer room shall be likewise protected with a sprinkler system. If the data center is a standalone facility (not part of a larger building) or is located in a nonsprinklered building, the computer room shall be protected with a sprinkler system, a gaseous clean agent system, or both a sprinkler system and a gaseous clean agent system.

The basic fire suppression system in a computer room shall be a fire sprinkler pre-action system. The sprinkler system for a computer room shall be valved separately from other sprinkler systems. Valves controlling water to the computer room sprinkler system shall be labeled and easily identified as separate from valves controlling sprinkler water to the rest of the building.

Sprinkler heads shall be flush-mount pendant type if there is a suspended ceiling. The sprinklers shall be installed per applicable local codes, standards, and regulations. If there is no suspended ceiling, sprinkler heads shall be covered with a wire cage to prevent accidental impact and discharge.

Halocarbon clean agent systems, including Halon 1301, shall not be used to protect under an access floor unless the space above the access floor is likewise protected by the same halocarbon gaseous fire suppression system.

Any furniture in the computer room shall be constructed of metal or nonflammable materials. However, chairs may have seat cushions made of flame-retardant material.

Tapes and records shall be in a separate room with a fire suppression system and with fire-rated construction separating these rooms from the rest of the computer room and from any adjacent occupancies that are not part of the computer room. See Table 7-1 in Section 7.5.7 for further information regarding fire-resistant construction.

Automated tape libraries or other types of automated information storage system (AISS) units shall have a gaseous agent fire suppression systems installed within each unit if there are more than 0.76 m³ (27 ft³) of tapes or other combustible media.

Combustible materials shall not be stored in the computer room.

11.3.2 Recommendations

The fire detection system should include an early warning smoke detection system and a water leak protection system.

When practical, the sprinkler system should have an alternate water source to prevent a single point of failure and to allow maintenance.

Local codes may sometimes require that the suppression agent used below the access floor must be identical to the method used above the floor for the rest of the space or building.

Where it is critical to protect electronic equipment in the computer room, a gaseous, clean agent system dedicated exclusively to the computer room should be considered in addition to any required fire sprinkler system and, when used, it should be configured as the system that is activated first. While overhead water sprinklers provide excellent protection for the building structure, water from sprinklers will not reach fire located within ITE cabinets. Gaseous agent extinguishing systems provide “three dimensional” protection of spaces within equipment enclosures and are capable of suppressing fire in circuit boards and internal components.

If the entire facility is not protected with a gaseous clean agent system, it is a best practice to protect space under access floors with a dedicated inert gas clean agent system or a carbon dioxide total flooding system when the under-floor space contains combustible material (such as non-plenum rated cable). Carbon dioxide should normally not be used above the access floor in computer rooms.

Computer rooms should not have any trash receptacles. All unpacking should occur outside the computer room, and any trash in the computer room should be promptly removed.

Data center personnel should be trained on the use and function of the fire detection and extinguishing systems of the computer room.

Paper should be stored outside the computer room with a fire suppression system separate from the one used by the computer room.

11.4 Walls, Floors, and Ceilings

11.4.1 Requirements

NFPA 75 provides minimum requirements for the construction of the walls, floors and ceilings of the computer room.

Penetrations through the walls and floor of the room shall be sealed with a fire resistant material that provides a fire rating at least equal to the rating of the wall and floor. Air ducts shall be provided with automatic fire and smoke dampers where the ducts pass through fire-rated structure. If pass-throughs or windows are provided in the fire-rated walls of a computer room, then such openings shall be provided with a fire-rated shutter or fire-rated window of rating equal to the wall.

Some clean agents such as the inert gas agents will require vents in the enclosure that open during the discharge of clean agent to prevent excessive pressure build up as a result of the influx of gas in the room. Consult NFPA 2001, ISO 14520, and the system manufacturer for guidance.

11.5 Aisle Containment

11.5.1 Introduction

Aisle containment is rapidly becoming a standard feature in data centers in order to minimize air exchanges between hot and cold aisles and to maximize cooling efficiency (See Section 6.6.3.4). Additional volume spaces may be created by hot aisle containment or cold aisle containment structures and barriers such as ceilings above the aisles, doors and door swings at the ends of aisles, and barriers strategically placed to manage the direction of air flow. Aisle containment introduces challenges for fire prevention, detection, and suppression, especially in existing buildings.

11.5.2 Aisle Containment Construction and Materials

11.5.2.1 Requirements

The objective of fire prevention in data centers is to minimize or eliminate the use of combustible materials. Containment aisles or “hot collars” (e.g., equipment cabinet chimneys, vertical exhaust ducts) shall not be considered to be plenums. Materials used to construct containment structures or barriers shall meet the requirements of the AHJ. For locations where the AHJ does not have requirements, materials used shall have a maximum flame spread index of 50 and a maximum smoke development index of 450 as measured by UL 723 (See Section 6.6.3.4).

NOTE: Standards for combustibility include ASTM E84, Standard Test Method for Surface Burning Characteristics of Building Materials and UL 723, Standard for Test for Surface Burning Characteristics of Building Materials.

Hinged doors used in hot aisles shall open in the direction of egress. Sliding doors and hinged doors shall meet the requirements of the AHJ and be operable from the inside without the use of hands (e.g., “panic hardware”) as allowed by the AHJ.

Doors shall meet one of the following criteria:

- Not lockable from the outside
- Designed for lock-out/tag-out (LOTO) to prevent locking a worker inside the space
- Designed to lock from the outside but open from the inside without a key

Releasing devices, if used to remove ceilings or other obstructions, shall be listed for the application.

11.5.3 Detection Systems In Contained Spaces

Containment systems, by their very nature, modify and obstruct the natural air flow in a data center, creating challenges for detection systems. The objective of data center detection systems is to identify the precise source of incipient fire conditions (i.e., smoke and rising heat) before a condition turns into actual fire. Contained spaces can increase air temperature, contain high air velocity, increase air turbulence, and redirect air flow away from room smoke detectors, thereby making such precision more difficult. For example, temperatures in a hot aisle or hot collar can be as high as 60 °C (140 °F). The typical air exchange rate in a building is a maximum of 60 air changes per hour (ACH), but in data centers—and especially in contained aisles—the exchange rate can be as high as 500 to 1000 ACH, and air velocities can range from 15 m/min (50 ft/min) to as high as 1500 m/min (5000 ft/min).

11.5.3.1 Requirements

Detectors shall be required within the contained space and shall comply with local regulations.

Detectors shall be listed for use in high volume air flow.

When installed in contained hot aisles or hot collars, detectors that respond to high temperatures shall be able to compensate for the high temperatures normally present in such spaces. Typical temperatures in a contained hot aisle frequently range from over 38 °C (100 °F) to as high as 60 °C (140 °F).

11.5.3.2 Recommendations

Spacing of detectors within a confined aisle or hot collar should be based on best engineering judgment to meet site-specific conditions. Sensor spacing will depend upon the type of smoke detectors being used and manufacturer's recommendations for the conditions of use.

If smoke detectors are used to trigger automatic actions, such as closing dampers or activating power shutdown, multiple sensors should be required to verify a condition. Very early warning fire detector (VEWFD) systems can be sensitive to conditions that could lead to false alarms in the turbulent conditions of a contained space. Cross-zone smoke detection might require two types of detection.

11.5.4 Suppression Systems In Contained Spaces

11.5.4.1 Requirements

Suppression systems used within a contained aisle shall meet or exceed the minimum requirements for suppression systems used in the surrounding space and shall comply with local regulations.

Where containment is introduced into existing data centers, fire suppression systems shall be modified when necessary to meet prevailing codes and standards. For example, sprinkler head placement shall meet local code requirement for clearances to walls or other obstructions to dispersal. The system may have to be retested to verify compliance.

Sprinkler or clean agent system dispersal modification requirements may be waived if:

- 1) Obstructions are removable prior to an emergency dispersal event,
- 2) Obstruction can be removed without compromising means of egress, and
- 3) Removal is initiated by an automatic means of smoke detection.

Fusible links, shrinking panels or other heat-responsive triggers shall not be used as a means for triggering removal of barriers to code-required clearances for suppression systems.

Automatic barrier removal, if used, shall remove all obstructions for the entire suppression zone.

For gaseous fire suppression systems:

- Any additional volumetric space constructed for contained closed loop return air shall be added to the calculated total volume requirement for gaseous agent.
- The concentration of gaseous agent, when released, shall not be less inside a contained space than it is in the area outside the contained space.

11.5.4.2 Recommendations

Sprinkler piping should be centered at ceiling level within the contained aisle (not above cabinets). Sprinkler heads should be high enough that spray can reach the top of the cabinets on either side of the aisle.

Clean agent nozzles that are too close to a wall or other obstruction can result in “frosting”, thereby reducing the effectiveness of the agent, before the agent has a chance to atomize. Placement of 1.2 – 1.8 m (4 – 6 ft) from the nearest obstruction is recommended.

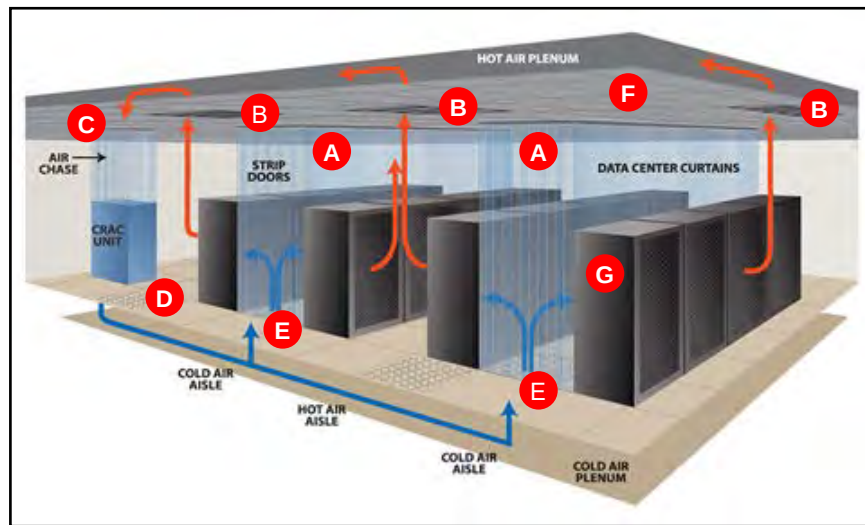
11.5.5 Additional Information

In a new construction, fire suppression sprinkler pipes on eight foot centers grids can be arrayed to meet clearance requirements of most local codes for hot aisle containment and cabinet hot collar containment. Rows will fall on an eight tile pitch from the center of cold aisle to the center of the adjacent cold aisle. (See Figure 6-4 in Section 6.6.3)

Most fires in data centers are presumed to be electrical in nature. Smoke, not heat, is the main cause of damage or injury. Therefore, devices that require heat for activation (e.g., fusible links in sprinkler heads or in drop-down curtains, shrink-activated drop-down ceilings, etc.) are ineffective. If drop-down ceilings and partitions are used, they should be mechanically activated from a smoke detector or other means.

Containment systems can reduce the amount of smoke dilution in a computer room but, at the same time, can increase the smoke dilution within a contained aisle, thereby making it difficult to isolate the specific source of the smoke. Reduction in spacing of detectors based on air change rates within a contained space is typically necessary.

Figure 11-1 illustrates variations in air flow in contained spaces. Note that Figure 11-1 illustrates cold-aisle containment; it is not meant to illustrate all of the many different variations of aisle containment.



(Illustration courtesy of Tiesche Engineered systems)

Figure 11-1
Variations of Air Flow in a Data Center with Aisle Containment

The following notations in Figure 11-1 indicate the different places where fire detection might be installed:

- A. Area monitoring within containment
- B. Monitoring at transfer grilles to plenum
- C. Monitoring in plenum at return air collection point and prior to entry into HVAC system
- D. Monitoring at HVAC supply
- E. Monitoring at supply plenum exit points into containment
- F. Area monitoring at ceiling
- G. In-cabinet monitoring

11.6 Handheld Fire Extinguishers

11.6.1 Requirements

Fire extinguishers shall be clearly visible. Each fire extinguisher shall be labeled to describe clearly the type of fire on which it should be used.

11.6.2 Recommendations

Hand-held, clean agent fire extinguishers are recommended and may be required by the AHJ

Extinguishers that use dry chemical agents are not recommended because they can damage electronic equipment. Switchgear rooms should have clean agent handheld fire extinguishers similar to those used in the computer room.

11.7 Fire Protection

11.7.1 Water Sprinkler System

11.7.1.1 Wet System

11.7.1.1.1 Introduction

The wet sprinkler system is a method of fixed fire protection using piping filled with pressurized water, supplied from a dependable source. Closed heat sensitive automatic sprinklers spaced and located in accordance with recognized installation standards are used to detect a fire. Upon operation, the sprinklers distribute the water over a specific area to control or extinguish the fire. Wet systems are applied to the noncritical areas of the data center (see Table 11-1). This system is usually required as a minimum to protect people and property.

As with pre-action sprinkler systems, the wet system may require additional water supplies or fire pumps if there is not enough water pressure available from the utility serving the site (e.g., from the city).

Table 11-1 Recommended Sprinkler Systems for Data Center Spaces

<i>Area</i>	<i>Sprinkler System</i>
Computer room	Pre-action sprinkler system
Network operations center	Pre-action sprinkler system
Entrance room	Pre-action sprinkler system
Office	Wet sprinkler system
Electrical switchgear	Pre-action sprinkler system
Battery and UPS rooms	Pre-action sprinkler system
Generator rooms	Pre-action sprinkler system
Chiller room	Wet sprinkler system
Other spaces not listed above	Wet sprinkler system

NOTE: AHJ requirements may supersede these recommendations.

11.7.1.2 Pre-action Sprinkler System

11.7.1.2.1 Recommendations

The best practice for critical areas is to install a pre-action sprinkler system. This type of sprinkler system provides some safeguard against water damage to the data processing equipment because of an accidental discharge.

11.7.1.2.2 Additional Information

The pre-action sprinkler piping system is similar to the wet system except the piping in the critical areas does not contain water until there is a fire event.

Two events are required before the deluge valve will open and allow water to flow into the sprinkler piping. A single interlock system requires a detection system to operate a valve to flood the fire sprinkler system piping with water. A double interlock system admits water (by opening the deluge valve) in the sprinkler piping upon operation of both detection and a loss of pressure in the sprinkler piping. Both systems have sprinkler heads, requiring a heat rise to open the sprinkler head allowing the water to flow. The interlock system's designs are intended to prevent accidental water flow in sensitive areas caused by events such as the accidental operation of a sprinkler head or leaks that may develop in the sprinkler piping. Applicable codes and standards require review prior to the application of either of the interlock systems. Types of detection systems include smoke, heat, or other automatic fire detectors such as air sampling detectors or flame detectors.

It is important to note that pendant systems will typically have a column of water in the sprinkler pipe drop from the branch main. The sprinklers should be removed and the pipes drained after system trip testing.

11.7.1.3 Dry Sprinkler Systems

11.7.1.3.1 Introduction

Dry sprinkler systems are similar to pre-action systems in that no water is in the piping until there is a fire event, but their activation system is simpler. The primary difference is that the piping is filled with nitrogen or dehydrated air below the water supply pressure. To prevent the water supply pressure from forcing water into the piping, the design of the dry pipe valve creates a greater force on top of the check valve, where the air is, than under the valve, where the water is. When one or more of the sprinklers heads opens, the air in the piping vents from that sprinkler head(s), reducing the pressure above the valve.

Dry pipe systems are installed in spaces in which the ambient temperature may be cold enough to freeze the water in a wet pipe system. Dry pipe systems are typically not used unless the range of ambient temperatures reaches below 4 °C (40 °F).

11.7.1.3.2 Requirements

Dry sprinkler systems shall not be used in computer room or generator areas of a data center.

11.7.1.3.3 Recommendations

Dry sprinkler systems should be used only in spaces that do not have HVAC and are exposed to ambient temperatures. Dry sprinkler systems are recommended for areas such as outdoor loading docks, parking garages, and unheated storage sheds.

11.7.1.4 Fire Protection Interfaces

11.7.1.4.1 Additional Information

Interfaces to the fire protection system include:

- Fire detection/control/alarm (Section 11.7)
- Building automation system (BAS) (Section 13.2)
- Security/guard station (Section 12)
- Electrical power control and monitor system (Section 9.7)
- EPO (emergency power off) system (Section 9.3.15)

11.7.2 Gaseous Fire Suppression

11.7.2.1 Clean Agent Gaseous System

11.7.2.1.1 Introduction

Because of the expense involved with replacing the data center equipment and the difficulty of water from overhead sprinklers to reach fire within ITE cabinets, building owners may consider a gaseous fire suppression system. Fire suppression is achieved by developing an extinguishing concentration of a “clean agent” in the fire zone. Clean agents are stored in pressurized cylinders in or near the computer room to keep pipe lengths short, and most systems are designed to fully discharge within 10 to 60 seconds from initiation.

11.7.2.1.2 Requirements

Where clean agent gaseous fire suppression systems are used, the extinguishing concentration shall be maintained long enough for the materials that have been heated by the fire to cool sufficiently so that the fire will not reignite. Standards, such as NFPA 2001, require that 85% of the design concentration be maintained at the highest level of combustibles in the protected space for at least 10 minutes or for a time period long enough to allow for response by trained personnel.

Protection shall extend to all areas of the computer room within the fire-rated envelope. If a separate gaseous agent system is provided for protection of the space under an access floor, it shall be arranged to discharge simultaneously with the gaseous agent system protecting above the access floor.

Subject to the approval of the AHJ, gaseous agent systems may be provided to discharge gas within specific ITE enclosures. Such protection is typically used for automated information storage systems such as automated tape libraries.

Halon 1301 systems shall not be installed in new data centers and not introduced or expanded within existing data centers.

NOTE: Existing Halon 1301 systems may continue in usage unless prohibited by local laws.

11.7.2.1.3 Recommendations

Noise in excess of 120 dB may cause disk drives to fail, so some type of noise suppression is recommended for computer rooms with disk drives inside.

11.7.2.1.4 Additional Information

The air sampling pipe network is a system of pipes installed above or below the access floor with strategically placed air sampling ports. Sample piping material must be approved for use in air plenums when installed in return air ceilings or under raised floors in accordance with the requirements of the AHJ.

11.7.2.2 System Controls

11.7.2.2.1 Introduction

In a gaseous fire suppression system, an automatic fire detection system activates the release of the gas. Two-detector actuations are used to minimize false discharges.

11.7.2.2.2 Requirements

Upon initiation of a stage 2 alarm, system controls shall activate an adjustable time delay prior to activation of the actual release of the suppression gas to allow personnel time to evacuate the area. An abort station for the system shall be located within the computer room and provide the ability to temporarily halt the release of the suppression gas. Halting of the release of the system shall require a continuing manual action (e.g., holding a button/switch). At least one manual release control station and abort control station shall be present in a computer room and located at the exit doors.

11.7.2.2.3 Recommendations

Actuation of one detector should initiate a stage 1 alarm, consisting of audible alarms and automatic notification to the central station or fire/security monitoring system.

Actuation of a second detector should initiate a stage 2 alarm, consisting of an audible alarm that is distinct from the first stage alarm. Discharge commences after a time delay of no greater than 30 seconds, subject to approval by the AHJ.

The abort station should not restart the discharge delay sequence.

A land-line telephone and fire extinguisher should also be located at each exit and emergency station. A land line is an analog line served directly by the service provider and that bypasses the owner’s PBX, voice gateways, or other voice systems.

11.8 Fire Detection

11.8.1 Area Requirements

Table 11-2 lists recommended detection systems for differing data center spaces.

Table 11-2 Recommended Detection Systems for Data Center Spaces

<i>Area</i>	<i>Detection System</i>
Computer room	Incipient or early warning intelligent
Network operations center	Incipient or early warning intelligent
Entrance room	Incipient or early warning intelligent
Office	Ionization/photoelectric
Access floors	Photoelectric (where allowed by code)
Electrical switchgear	Ionization/photoelectric
Battery and UPS rooms	Ionization/photoelectric
Generator rooms	Thermal or flame detectors
Chiller room	Ionization/photoelectric
Other spaces not listed above	Ionization/photoelectric

NOTE: AHJ requirements may supersede these recommendations.

11.8.2 Detector Technology

11.8.2.1 Addressable Systems

11.8.2.1.1 Recommendations

Provide an addressable, multiplexed, microprocessor-based, electrically supervised fire alarm system for the facility. Design the system to comply with regulatory and code requirements.

11.8.2.2 Design Considerations

11.8.2.2.1 Requirements

The smoke detection system shall be designed to automatically control air supply and exhaust systems and shall be interfaced with the building automation system. Where required, duct-type smoke detectors shall be provided in all ventilation systems.

Smoke detector spacing shall comply with regulatory and code requirements and NFPA 72 or ISO 7420.

11.8.2.2.2 Additional Information

The air velocity of the HVAC system should be considered as high velocity or turbulent air may require a reduction in smoke detector spacing below normal requirements.

Ionization type detectors are designed to be installed in areas of low air velocity and are not recommended for computer rooms.

Photoelectric type detectors are designed to be installed in areas of higher air velocity. Smoke detectors located in ducts and air plenums should be rated and clearly labeled for use in high air velocity applications.

Incipient air sampling systems are not normally affected by the air velocities found in a typical computer room. Incipient stage fire detection located at the CRAC return air grills provides the most reliable detection. Sample points can be provided in the exhaust air stream from critical pieces of equipment to provide very early warning of equipment overheating.

In many cases, the CRAC can be provided with supplemental built-in smoke detectors intended strictly for internal CRAC system controls. These can be connected to the fire alarm system or BAS.

11.8.2.3 Addressable System, Non-Data Floor Conditions

11.8.2.3.1 Requirements

The system shall provide:

- Smoke detectors in all unoccupied spaces
- Audiovisual notification appliances to meet local code requirements
- Manual pull stations at all exit doors
- Connections from flow/tamper switches to the fire alarm system
- Required interface(s) with the security system. Upon activation, the fire alarm system shall release all security doors
- Monitoring of the fire pump and generators, if provided.

Smoke detectors can sometimes give false alarms. Also, deactivation of HVAC may result in greater hazard than continued air flow, depending upon the design. Where operations are critical and when acceptable to the AHJ, a procedure to control the cessation of air circulation within a room or zone upon activation of smoke detectors shall be permitted.

Fixed temperature heat detectors or flame detectors shall be provided in generator rooms. Temperature set points shall be coordinated with the sprinkler system operation parameters so that the heat detectors will actuate first.

Smoke detectors shall be provided in conjunction with magnetic door holders, where applicable.

Firefighters' control panel, graphic smoke control panel (if required), printer, and annunciator shall be located at the main security office.

Photoelectric and ionization-type smoke detectors shall be provided in UPS equipment and battery rooms.

11.8.2.4 Addressable System Data Floor Conditions

11.8.2.4.1 Requirements

Cross-zoned smoke detectors shall work in conjunction with the pre-action sprinkler system and the clean-agent fire suppression system.

11.8.2.4.2 Additional Information

When an access floor is present in the computer room, photoelectric type detectors may be installed below the floor where permitted by the AHJ.

11.8.3 Early Warning Detection Systems

11.8.3.1 Incipient (Air Sampling) Systems

11.8.3.1.1 Recommendations

In areas where maximum fire protection is required, early warning or incipient type systems should be installed at selected computer room and entrance room locations.

11.8.3.1.2 Additional Information

Early warning or incipient-type systems can be up to 2000 times more sensitive than conventional spot-type detectors.

Consideration needs to be given regarding the level at which incipient systems are used with these systems as premature activation should be avoided.

Incipient control panels may be installed at several locations and connected to the fire alarm control panel.

The air sampling pipe network is a system of copper or PVC pipes installed above or below the access floor with strategically placed air sampling ports. When mounted under an access floor, the pipes are mounted with nonconductive supports to the floor support pedestals midway between data and power raceways.

If added protection is desired, sampling pipes may be run above the ceiling or surface mounted to structures where no ceiling is provided.

11.8.3.2 Early Warning Intelligent Detectors (Alternative To Incipient)

11.8.3.2.1 Additional Information

A class of (spot) detectors provided by several manufacturers is able to detect conditions at the early stages of a fire. The early warning detectors use a combination of laser, infrared, or thermal technology.

The detectors are addressable, which allows for multiple detector protection for pre-action sprinkler and gaseous suppression systems.

The detectors use a processing capability to both learn and automatically compensate for actual conditions.

The detectors should be installed according to codes and manufacturer's recommendations for air velocity and other conditions.

11.9 Labeling and Signage

11.9.1 Requirements

All devices shall be labeled with the fire alarm circuit, zone, or address.

Junction boxes shall be painted red or as required by AHJ.

11.9.2 Recommendations

| Labeling and signage practices for the fire protection system should include the following:

- Emergency procedures should be posted on all fire alarm control panels and annunciator panels.
- Fire alarm manual stations should be clearly labeled to avoid any confusion. Where permitted, install a cover over these manual stations to avoid accidental triggering.

11.10 Testing and Quality Assurance

11.10.1 Requirements

Startup and commissioning for the fire protection system shall follow those required by applicable standards, regulations, and the AHJ.

11.10.2 Recommendations

Pre-action sprinkler systems should be trip tested at least once every three years.

11.11 Ongoing Operations

11.11.1 Requirements

Site operations and maintenance procedures for the fire protection system shall follow as a minimum those required by applicable standards, regulations, and the AHJ.

11.11.2 Recommendations

| Clean agent systems should be maintained in accordance with manufacturer's instructions and either NFPA 2001 or ISO 14520.

•

12 Security

12.1 General

12.1.1 Introduction

The purpose of this section is to define the physical security practices and countermeasures necessary to protect the confidentiality, integrity, and availability of the data center.

12.1.2 Requirements

The requirements in this standard shall apply to all existing data centers; all new construction, renovation, alterations, remodeling, or expansion of any site, building shell, data center, or computer room.

12.2 Physical Security Plan

The physical security plan is a document providing the framework, policies, and procedures to establish security for data center staff, contractors, and visitors along with the ITE, network technology, telecommunications assets, and the sites and buildings that house them. A physical security plan shall be created and followed for the data center and the entire building or campus where it is located.

12.2.1 Recommendations

During construction on any existing data center, enhanced temporary security measures should be put in place.

12.2.2 Additional Information

There is no guarantee of security implied; however, compliance with the requirements listed in this section should provide an acceptable level of security.

No single countermeasure provides effective security. All architectural, operational, and physical security measures (see Figure 12-1) are intended to do one or more of the following individually and collectively:

- Delay
- Deter
- Detect
- Decide
- Act

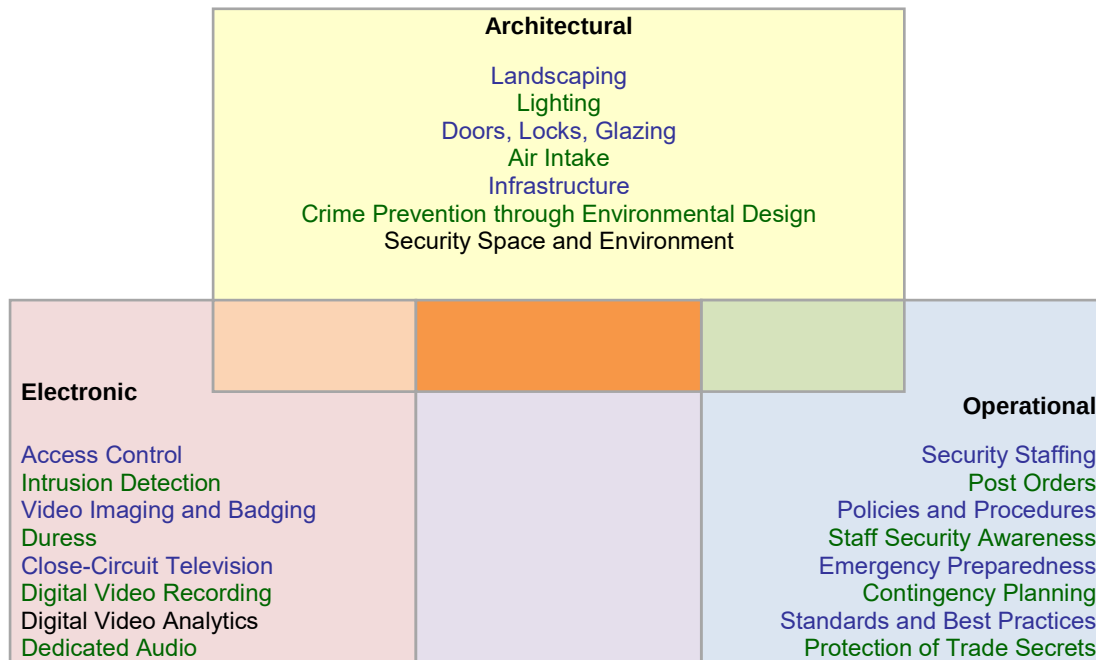


Figure 12-1
Security Measures

12.2.2.2 Physical Security in Data Centers

Modern data centers are composed of layers of technical, administrative support, and end user space supporting a single or multiple computer room(s) with various amounts of data processing and storage capabilities. Depending on the number and types of potential threats, providing physical security for the data center can encompass the full range of security needs for the site, zones, buildings, rooms, and areas, including:

- Access control devices
- Architectural design
- Barriers
- Detection and alarms
- Guard services
- Surveillance

12.2.2.3 Physical and IT Security

Historically, the policies, design, practices, technology, and personnel utilized to protect physical assets have been separate from those used to protect ITE and its data. The increasing use and importance of devices that create data, when combined with the increasing sophistication of the attacks and frequency of attempts to capture or compromise that data, requires a move toward a more holistic type of security. Such security will require the data center operator to consider both physical and IT countermeasures.

12.2.2.4 Cyber/IT Security Plan

The cyber security plan provides security for data at rest and data in motion and protects it from attempts to defeat its confidentiality, integrity or availability through electronic means. Cyber security plans are beyond the scope of this section.

12.3 Risk and Threat Assessment

12.3.1 Definitions

Definitions that apply specifically to risk and threat assessment follow below and only apply to the security section of this standard:

- Asset—an employee, contractor, or any physical, technological or intellectual possession.
- Countermeasures—the procedures, technologies, devices or organisms (dogs, humans) put into place to deter, delay or detect damage from a threat.
- Risk—the likelihood that a threat agent will exploit a vulnerability creating physical or technological damage.
- Secured environment—an area defined within the data center or within the site facilities that has security measures to control physical access to in-scope systems.
- Threats—the agents by which damage, injury, loss or death can occur; threats are commonly classified as originating from temperature extremes, liquids, gases, projectiles, organisms, movement or energy anomalies.
- Vulnerability—a physical, procedural or technical weakness that creates opportunity for injury, death or loss of an asset.

12.3.2 Recommendations

12.3.2.1 Security Survey/Analysis

Every data center should have a complete security survey or analysis during the preplanning and planning stages of construction, after data center operations commence and repeated annually. The security consultant, architect, and engineer team should assess the following metrics and provide written recommendations:

- Identification of assets
- Identification of natural, technological, and human threats
- Probability of risk
- Past and potential future losses to the content of the complex or building
- Potential impact of losses and risk
- Possible countermeasures
- Cost/benefit analysis of proposed countermeasures

12.4 Regulatory and Insurance Requirements

12.4.1 Recommendations

The data center security plan (Section 12.5) should include topics regarding applicable regulatory, insurance, and best practices issues leading to compliance to such requirements and recommendations.

The physical and cyber security plans should contain requirements that support compliance.

12.4.2 Additional Information

Various entities require the protection of sensitive data and the computer equipment in which such data is stored or by which it is processed or transported. Depending on the size of company and IT dependence, compliance with government, finance, and insurance entities' regulations should have a positive impact on document management, storage management, and the establishment of record retention schedules.

12.4.2.1 Regulations or Laws Affecting Security

The regulatory, financial, and other legal requirements affecting the operation of a data center will vary widely between countries, regions, localities, and business sectors inhabiting the facility. The data center owner and operator should be familiar with all legal and regulatory requirements concerning privacy, purposeful or accidental disclosure of financial, medical, or personal data, and national security. Some examples of regulatory and legal documents affecting the operation of the data center include:

- Sarbanes-Oxley
- Industry-specific standards
- US Patriot Act
- Federal Information Processing Standards (FIPS)
- Health Insurance Portability and Accountability Act (HIPAA)
- Gramm-Leach-Bliley (GLB)
- National Association of Security Dealers Conduct Rules 3010, 3013, and 3110
- European Privacy Standards
- NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*
- Statement on Standards for Attestation Engagements (SSAE) No. 16, *Reporting on Controls at a Service Organization*

The primary purpose of these rules and regulations are to protect investors, shareholders, employees, and the public from a variety of violations, ranging from accidental disclosure of personal information through the pending collapse of the corporation.

Data center operators, security architects, and designers should avoid viewing these laws and regulations mechanistically, or as a checklist. They should be viewed and approached as a top-down risk assessment.

12.5 Data Center Security Plan

12.5.1 Recommendations

12.5.1.1 General

The data center security plan should be comprehensive, but easy to read and understand.

The data center security plan should be reviewed and updated as follows:

- Once annually
- Following any major construction or remodeling project of the data center and related spaces
- Following any site-based major construction or remodeling when the data center is located in a multitenant building or campus
- Following any major breach of security or disaster event
- Following notification of changes/revisions of applicable regulations, policies, or externally imposed requirements
- When a change in local, regional, or national security events warrant

Prior to creation of a data center security plan, the data center operator, security architect, or designer should conduct a thorough risk assessment of the existing or future site, buildings and demographics of the data center.

The data center security plan should address all areas of potential risk identified during security survey.

The data center security plan should address departmental responsibility for both each element of the security plan and the implementation of that element, including:

- Administration
- Cyber security
- Facilities
- Finance
- Human resources
- Information technology
- Physical/plant security
- Purchasing
- Operations

Additionally, the data center plan should detail what countermeasures should be selected and deployed for each of the previously listed elements, utilizing the following criteria:

- Protection of the life and safety of occupants
- Protection of physical assets
- Protection of electronic assets

The data center should, at a minimum, employ the following protective measures:

- Access control with retention of at least thirty days of access control logs
- Video surveillance system (VSS) with at least thirty days retention of archived footage
- Intrusion detection systems with at least thirty days retention of alarm logs
- Implementing visitor entry control procedures with at least one year retention of visitor records
- Securing offices, rooms, and facilities
- Protecting against external and environmental threats
- Controlling all access points, including delivery and loading areas

The data center security plan should detail the roles and responsibilities that IT operations and network security can play in supporting the physical security procedures.

All employees should receive training on all relevant aspects of the security plan. This training should be done during orientation and annually refreshed during their employment. Training should be interactive, containing learning checkpoints. Training should include penalties for failure to follow the security plan.

12.5.1.2 Access Control Policy and Procedures

The control of access to the data center should be addressed in detail by the security plan. Questions answered by the security plan include:

- Who has access to the data center, during what hours and for what reasons.
- If the data center occupies the entire building, how is the security for public areas, loading docks, utility areas, offices, vendor/visitor areas and meeting areas addressed.
- If the data center occupies only a part of the building, how is security to be addressed for common areas with other tenants, elevators, storage areas, risers, normal/emergency pathways, and common telecommunications areas.
- How is access granted, controlled, reviewed and removed.
- How are visitors and contractors managed.
- How are breaches in security policy dealt with.
- Is there a space programming standard that specifies recommendations or a template for each type of space.
- Do some areas, such as the computer room, prohibit sole occupancy by an employee or contractor.
- What levels of authentication are required for access to computer and critical facility rooms.
- How are service providers monitored when working in the facility.
- If access control procedures change during non-business hours.

<List continues on next page>

- What types of doors and locks are used for each type of area:
 - Public
 - Semipublic
 - Semiprivate
 - Private
 - Critical facilities, including the computer room floor
- How are keys and badges managed.
- What are the emergency (e.g., fire alarm) event access procedures.

Every six months, per standards such as ISO 27001, a review should be executed of those individuals that have been authorized to access the data center or confidential information contained therein and verify both whether the individual still requires access and the individual's present access level.

Access restrictions and organizational measures should be taken to ensure that printed or other materials containing confidential information cannot be viewed or removed by unauthorized individuals.

Regular (monthly or more frequently as necessary) reports of access should be generated from the physical access control devices in place and provided to the data center management and/or customer corresponding to the change control ticket associated with the need to access the secured environment. In addition, any irregularity should be reported immediately according to the established escalation procedures.

12.5.1.3 Badging Policy and Procedures

The security plan should require the use and display of badges for all employees at all times.

The security plan should require the use and display of temporary identification badges for all visitors, contractors, and delivery personnel at all times.

All temporary identification badges should have some visible method by which employees, security, and law enforcement personnel can easily determine whether the badge has expired. Possible methods for ensuring that expired badges are not reused include:

- A rotating color scheme
- The expiration date printed on the badge
- The day of the week printed on the badge
- Use of self-adhesive tokens that gradually expire over a predetermined period, typically one day
- Use of badges that gradually expire over a given period, gradually displaying bars or some other visually distinctive method

The security plan should specify how the visitor, contractor, or delivery person should wear or display the identification badge.

If identification badges are used, badges for employees should be different from those for visitors, contractors, delivery persons, or other non-employees.

The security plan should address how identification badges will identify those visitors, contractors, and delivery personnel who must be escorted.

12.5.1.4 Signage and Display Policy and Procedures

The security plan should identify the wording, readability, and location of signage and displays intended to control pedestrian and vehicular traffic from straying into unauthorized areas.

The plan should address methods of signage and other methods of announcement or reminders to all regarding the observation of non-permanent individuals for compliance with the plan's policies and procedures.

12.5.1.5 Fire Prevention, Detection, and Suppression

The security plan should contain policy on the type and location of fire suppression equipment.

The security plan should contain policy on what type of protective containers should be used for sensitive material. This may include the reference to or specification of fire-resistance standards.

The security plan should contain policy on the storage of combustible chemicals and materials.

The security plan should contain policy and procedure for the fire rating of any containers found in sensitive areas such as trash receptacles.

12.5.1.6 Monitoring and Alarms Policy and Procedures

The data center should have written guidelines for evaluating emergency responses to all alarms.

The security plan should specify what types of alarms or monitoring systems are used for controlling access to certain areas or devices. Areas of particular concern should be:

- Common cross-connect spaces
- Common riser closets
- Computer room
- Critical facilities rooms/areas
- Elevators and stairwells
- Entrance facilities
- Administrative, HR, and finance departments
- Offices
- Plenum and ceiling spaces
- Telecommunications spaces
- Utility rooms and closets
- Vehicular and pedestrian gates

The security plan should address who has access to alarm codes and keys to turn off or bypass systems.

The security plan should state the policy and procedures regarding code changes because of terminated employees, contractors, or contract personnel, such as janitorial.

The security plan should address the issuance of unique codes or groups of codes to employees, contractors, or contract personnel. Such procedures should include the use, expiration, control, on-going review, and authorization of such codes.

The security plan should coordinate with the cyber/IT plan how live data and telephone jacks in public or semipublic areas are monitored and secured against unauthorized access. This would include common building areas such as riser closets, common cross-connect areas, entrance facilities and service provider areas.

When applicable, the security plan should coordinate with the cyber/IT security plan, the policy for alarming, and monitoring of computers cases, server cases, and cabinets against the unauthorized access to or removal of discreet components or equipment.

Alarm company and security service providers should be monitored when working on surveillance and alarm systems. The security plan should detail policy and procedure to ensure that only authorized service is performed on alarm and surveillance equipment by requiring 24 hour advance notice of the employee's name and other identification information or similar.

12.5.1.7 Material Control and Loss Prevention

The security plan should address:

- All aspects of material control and loss prevention both in and out of the data center site, campus, buildings, parking garages, and office areas
- Which materials, including ITE, employees are authorized to bring into and take out of the data center and inspection procedures
- Which materials, including ITE, visitors and contractors are authorized to bring into and take out of the data center and inspection procedures
- Description and control of use for all bring your own device (BYOD) equipment to include electronic emissions and connection to hard and wireless networking
- The inspection and receiving procedures for all deliveries, including authorized points of unloading and personnel authorized to receive deliveries
- Approved methods for disposal of printed materials and magnetic or other media

The security plan should state the policy, inspection procedures, and penalties for unauthorized transport or use of removable media such as thumb drives, tapes, optical disks, or removable hard drives. This should be complimentary to any existing cyber/IT security policy.

The security plan should specify when property tags, electronic tags, and other identification systems should be affixed to data center equipment and assets.

12.5.1.8 Surveillance Policy and Procedure

The data center should have written guidelines for evaluating emergency responses to all VSS alarms or incidents.

The security plan should detail:

- Policy for the location and placement of surveillance equipment, including special circumstances noted during the risk/threat assessment.
- Policy and procedure for the protection and secure placement of surveillance devices within offices, work areas, elevators, loading docks, lobbies, parking garages, and exterior areas of the data center.
- Personnel able to authorize special surveillance, covert surveillance, or placement of new VSS equipment.
- The secure placement, storage, and disposal of surveillance tapes and recorded media (servers, storage, and DVR).
- Locations that work may occur outside the range of the VSS with any supervision requirements by or of data center personnel for these locations.

12.5.1.9 Disaster Recovery

Definitions as defined by NFPA 1600, the Standard on Disaster/Emergency Management and Business Continuity Programs:

- Natural events, including drought, fire, avalanche, snow/ice/hail, tsunamis, windstorm/tropical storm, hurricane/typhoon/cyclone, biological, extreme heat/cold, flood/wind-driven water, earthquake/land shift, volcanic eruption, tornado, landslide/mudslide, dust/sand storm, and lightning storm.
- Technological events, including hazardous material release, explosion/fire, transportation accident, building/structural collapse, power/utility failure, extreme air pollution, radiological accident, dam/levee failure, fuel/resource shortage, strike, business interruption, financial collapse, and communication failure.
- Human events, including economic, general strike, terrorism (ecological, cyber, nuclear, biological, chemical), sabotage, hostage situation, civil unrest, enemy attack, arson, mass hysteria, and special events.

The security plan should include the development of detailed plans for the notification, response, and emergency operation of the data center following a natural, technological, or human disaster.

The data center operator, security architect, and designer should work with other departments and plans to identify, assess, and mitigate any foreseeable natural or other disasters. The security plan should whenever possible focus on prevention and mitigation to threats.

The security plan should consider and document the various data center or corporate assets and prioritize protection and recovery policies and procedures.

The security plan should put into place systems, processes and procedures prior to a disaster that will enable the data center to:

- Prepare for natural, technological or man-made events.
- Respond to disasters.
- Recover from disasters.
- Work with civilian or military authorities during a disaster.

The security plan should provide detailed measures to protect the following:

- Health and safety of data center or campus occupants at the time of the disaster
- Health and safety of emergency services and disaster aid personnel responding to the incident
- Ability for the data center to continue operations
- Security and recovery of corporate intellectual property assets
- Condition and usability of the site, campus, building(s), critical, and telecommunications infrastructure
- Utilities and telecommunications services
- The environment
- Economic and financial condition of the company
- Regulatory and contractual obligations
- Company's reputation

The security plan should identify the approved and contractual civilian and governmental resources for mutual aid in the event of a disaster.

The disaster recovery section of the security plan should be reviewed, updated, and documented at least once per year or following any of the following events:

- Identification of new hazards
- Regulatory changes
- Reorganizations, down-sizing, or significant growth
- Disasters
- Disaster preparedness drills
- Major changes on the site, campus, or building
- Changes in the venue of the data center (e.g., annexation into a city)

12.5.1.10 Personnel

The security plan should detail all hiring and termination procedures, which may affect the safety and security of the data center, its occupants, facilities, ITE, and other assets.

In cooperation with Human Resources policy and procedure, the security plan should detail mandatory information needed from each applicant, including:

- Name and variations (verified)
- Correct address
- Citizenship
- Military record
- References
- Any security clearances
- Previous education
- Employment history
- Background information regarding spouse and relatives
- Criminal convictions
- Organizational affiliations
- Previous residences
- Clearance for, and obtainment of, necessary biometric information and samples for use in security credentials and operations.

The security plan should detail policies and procedures, ensuring that essential information needed from an applicant and employee is obtained from a legally binding application, including the appropriate authorization for investigation and release of information forms.

The security plan should include details on applicant screening procedures, background investigation standards, employee conduct, and termination procedures.

The security plan should include recommendations for additional pre-employment screening for certain positions, which might include psychological, skills and aptitudes, or integrity tests.

The security plan should require that all data center employees have an exit interview. Exit interviews can enhance security by:

- Reducing the loss of confidential information and trade secrets through discussion of nondisclosure agreements and potential penalties.
- Discovering problems that existing employees cannot or will not reveal.
- Reducing loss of data center property through the use of checklists.
- Gives the employee a chance to express grievances, reducing the possibility of vandalism, sabotage, or violence.

12.6 Crime Prevention Through Environment Design

12.6.1 Recommendations

The crime reducing concepts and strategies of Crime Prevention through Environmental Design (CPTED) should be followed during the planning process of the design or retrofit of a data center. There are three underlying principles of CPTED. They are:

- Natural access control
- Natural surveillance
- Territorial enforcement

12.6.1.1 Natural Access Control

The data center security architect or designer should utilize natural access control (e.g., placement of doors, fences, lighting, landscaping, other natural or architectural features) to guide pedestrian traffic as it enters and leaves the site, campus, building, or a room or space inside the building.

Each data center room and area should be classified by the level of protection required based upon the sensitivity of the equipment or activity occurring therein. Each area of a data center, including all support areas, closets, critical facility areas, utility and service provider areas, loading docks, lobbies, equipment yards, and offices should be classified into one of five basic CPTED space types:

- Public, used to designate areas that are available for all pedestrian traffic. Public areas could include lobbies, dining areas of restaurants or cafeterias, parking garages, and hallways or sidewalks outside of the controlled access areas.
- Semipublic, which is a term describing areas that are usually accessed from public areas, but not available to everyone. These areas might include conference rooms, restrooms, or break areas which may be outside the controlled access area or may have limited control.
- Semiprivate, a term used to classify space where natural, physical, or electronic access control is used to control pedestrian traffic. Semiprivate areas would include general office space, walled offices not used for sensitive work, private floors in a multitenant building, and non-critical utility rooms.
- Private spaces, those that are restricted from most pedestrians, including unauthorized employees. Typical private areas might include the print rooms, call centers, private manager offices, a bank vault, a surgery suite, and the executive floor of an office tower.
- Critical areas, those that are restricted and controlled from all pedestrians but individuals specifically enumerated in the security plan, corporate policy, and procedure documents. Typical critical facility areas might include computer room of the data center, critical facilities areas, power and machine yards, telecommunications rooms (TRs) that contain corporate cabling or services, network operations centers (NOCs), tape rooms and ITE processing rooms.

The concept of natural access control can be found in the following practices, which should be considered during any data center design:

- Place lights and attractive landscaping along the main sidewalk leading to the front door of the business.
- Place vegetation so that there is a clear line of sight only to the desired entrance of a building.
- Use lakes, rocks, hills, and vegetation to reduce the number of potential entrances onto a data center site, campus, or building.
- Develop architectural features to obscure the distinctive features of a data center site and to reduce or eliminate vehicular access to the facility.

12.6.1.2 Natural Surveillance

The concept of natural surveillance relies on the use and placement of physical environmental features, walkways, open spaces, pedestrian traffic patterns, and work areas to maximize visibility of the activity within an area by those outside of it and outside the area by those inside it.

Data center security designers should design the rooms, areas, spaces, walkways, and site so that there are many ways for observers to see unauthorized traffic, activity, or criminal behavior. As much as possible, all areas of the data center buildings and site should make the occupants feel safe and comfortable.

Designers should seek to allow maximum use of technology in the future by not obscuring critical or risk-prone areas during the design of natural surveillance or natural access control. Redesign should allow for continued review of the adjacency of a lower CPTED classified space to a higher classified space and assure proper level of security features and methods between them.

12.6.1.3 Territorial Reinforcement

The concept of territorial reinforcement is to create a sense of community or belonging so that if an unauthorized person strays or intentionally enters an area normally restricted to them, they both feel out of place and at risk of being easily identified as such.

The data center security designer should ensure that the atmosphere contributes to a sense of territoriality. The secure space should produce the feeling or sense of proprietorship or territorial influence so that potential offenders perceive this and are discouraged from entering or offending. One way to accomplish territorial reinforcement is to create clear borders between controlled and public spaces so that potential offenders must cross into an unauthorized area in full view of authorized occupants.

12.7 Access Control

12.7.1 Requirements

All access control systems must allow emergency egress of the facility in compliance with applicable building codes. The facility designer shall review the applicable life safety code requirements with the AHJ and comply with all AHJ requirements, which can vary from one location to another. The designs, although compliant during the design/redesign period, should not inhibit future changes empowered by changes in AHJ, policy, or procedure requirements to provide the data center with higher levels of security.

12.7.2 Recommendations

12.7.2.1 General

Access to the data center should be restricted to authorized employees, contractors, or visitors using one or more of the following methods:

- Security guards, receptionist, or other personnel
- Card reader systems
- Biometric devices

Access control designs should support all of the following objectives:

- Permit or deny entry
- Document activity and could provide automatic notifications
- Alter the rate of movement within certain areas
- Protect occupants, materials, and information against accidental or malicious disclosure
- Prevent injury
- Prevent damage

All building access points, including maintenance entrances, equipment doors, and emergency exits, shall use some form of access control.

Access is controlled by authentication of the individual to the access point.

Methods of authentication should include one or more of the following:

- Type 1: What a person has (e.g., keys, cards)
- Type 2: What a person knows (e.g., passwords, codes work, order number)
- Type 3: What a person is (e.g., guard recognition, biometric data)

When possible, the computer room and other high-value, critical, or sensitive areas of the data center complex should require multifactor authentication. An example would be a two-factor authentication scheme for the computer room where both fingerprint scan and proximity card are required to enter. An example for a three-factor authentication scheme for any critical facility area would be proximity card, fingerprint scan, and entry of a valid work order ticket number for the specific area.

A list should be maintained of the employees and contractors that have been issued keys, magnetic cards, codes, tokens, and badges so that the devices can be confiscated upon termination, confiscated upon change of responsibilities, or to permit the access control codes to be changed.

The access control card system should be configured for multiple levels and multiple areas of access to include temporal changes in access to the more critical areas. Individuals authorized to critical areas, such as the data center floor or critical power and cooling equipment, should be strictly limited as to quantity of staff, need-for-access, and permanency of access.

It is important that HR or the department for which an employee or contractor worked immediately notify the “owner” of all access control systems (IT, facilities, or security) when an employee or contractor is terminated or no longer requires access to all areas for which they were/are authorized.

Access control should be coordinated with emergency services personnel with each local agency, including police, fire, and EMS. Access during emergencies should be immediately granted regardless of the day or time, utilizing any one of the following:

- Rapid entry key systems (such as knox–box)
- Preissued cards, badges, tokens, or codes
- FIPS 201 compliant cards
- Combination locks, vaults, cabinets
- Electronic key retention units
- Other locally approved methods and devices

When possible, alarms from access control events should transmit to a local or remote location where timely responses or other actions can be initiated. Typical locations include the following:

- Remote contract monitoring company
- Main guard station off-site
- Guard station in another building
- Guard station in the same building

The access control system should be interfaced to the VSS for automated presentation of data to the guard(s) and permanent records.

Where union labor is utilized in the building by the data center corporate enterprise or by another company located in the same building or campus, planning for a labor strike should be included in the security plan, disaster recovery plan, and access control systems.

In the event of a strike, the existing hardware or software authentication should be backed up, and the hardware or software authentication (e.g., locks, access control programming) for striking workers should be temporarily disabled or changed.

12.7.2.2 Locking Mechanisms

12.7.2.2.1 General

Locking mechanisms are grouped into two general categories with a variety of available types and security levels with each one:

Mechanical:

- Warded
- Lever
- Pin tumbler
- Wafer tumbler
- Dial type combination
- Electronic dial type combination
- Mechanical block out devices for equipment ports and cords

Hybrid—electrical and mechanical operation:

- Electric deadbolt
- Electric latch
- Electric strike
- Stair tower
- Electric lockset
- Exit device
- Electromagnetic lock
- Shear lock

The data center security design should include input from the risk, threat, and vulnerability assessment before selecting the appropriate locks for each area.

Planning and analysis should occur during the determination of the types of locking systems to be utilized in the data center. Planning criteria include:

- AHJ restrictions and allowances
- Total number of locks
- Classification of space
- Employee and contractor demographics and turnover
- Type of facility
- Local crime statistics
- Risk/benefit analysis
- Availability and use of other countermeasures

Both the level of skill needed to attack a locking mechanism as well as the psychological deterrence should be considered when selecting a locking mechanism. Among the vulnerabilities of mechanical locks that must be considered when selecting a locking device are:

- Force
- Separation of the door jamb from the door—door jamb and surround wall materials should be strong enough to meet the delay requirements needed
- Length of the bolt—a 25 mm (1 in) minimum should be used for all secure areas where risk of attack by force exists
- Inclusion of an astragal or metal plate covering the gap over the location where the latch enters the keeper
- Requiring a hardened plate to cover the exposed lock housing and cylinder
- High-quality pins in pin tumbler cylinders to prevent snapping of the pins and manual rotation of the plug
- Picking
- Taking impressions of keys
- Stealing or inheriting keys

12.7.2.2.2 Mechanical Locks

All lock tumblers should be periodically rotated to maintain security as employee and contractor terminations occur. This can be accomplished through rotation of just the tumbler or core or can involve the removal and rotation of the entire lockset.

Locks and keys should never be used as a primary method of access control for computer room doors or other high-value or sensitive areas.

Key control using a single great grand master process is not recommended. This is especially true with larger facilities.

All keys should be included in a comprehensive key control procedure.

All keys should have the following words molded or engraved into the key body: *DO NOT DUPLICATE*.

All keys should be coded.

When possible, keys should be made on special blanks that are not available to others.

All new installations of door locks should comply with regulatory requirements for disabled occupants. One example of this type of requirements is the ADA, which requires the use lever handles instead of doorknobs.

The security designer for the data center facility should consider the function of the lockset as part of the security, ingress, and egress traffic patterns. Functions of locksets are classified as follows:

- Office, where the handle on either side will operate the latch bolt; locking is accomplished using the thumb turn inside the room or a key on the outside of the room.
- Classroom, where the latch bolt is only operated by the handle inside, or a key outside.
- Institutional, where only a key will operate the latch bolt from either side.
- Corridor, where the same functionality exists as in the office scenario, but the key and thumb turn throw a deadbolt; for safe egress, the inside lever also opens both the deadbolt and the latch bolt.

12.7.2.2.3 Electrified Locksets

Electrified locksets should be a key central design element of any data center security plan. These locksets are locked and unlocked remotely and are commonly layered and integrated with other systems in the electronic access control system.

It is important for the data center security designer to consider the operation of the facility during normal and emergency conditions. The ability to utilize either a “fail safe” or “fail secure” condition for each door must take into consideration the location and emergency egress routes for all occupants as well as the location and risk to high-value equipment and other assets. Failure to design the appropriate lock can create a significant risk of injury or death to occupants because of entrapment or unauthorized entry because of inadvertent opening of doors to storage areas.

A fail-safe lock is one in which the locking mechanism unlocks under any failure condition.

A fail secure condition is where the locking mechanism remains locked under any failure condition.

It is important that fire codes be consulted for requirements for door locking mechanisms and functions. One example of this is the stair tower lock, which releases a dead-locking mechanism if power is removed, allowing the door handles to be used.

The electromagnetic lock is an important locking mechanism and secures the door by means of a power electromagnet, which is rated by the force required to open the door when it is energized—typically 2200 N (500 lbf) to 8900 N (2000 lbf).

Combinations of more than one lock type are an important design strategy and should be utilized when attempting to maintain security during normal operation, loss of power, and emergency conditions.

12.7.2.2.4 Cipher and Combination Locks

Cipher locks do not have the ability for multiple codes. The use of cipher locks for computer rooms doors and other high-value or sensitive areas is not recommended because of the high probability of compromise because of “shoulder surfing” and the lack of ability to track entry/exit data.

If cipher locks are used on any door, security, or other data center personnel should verify that the default setting has been changed.

Cipher lock combinations should be changed at least every 30 days; however, 90 days is the maximum time recommended without changing the combination.

12.7.2.3 Doors

NOTE: In general, the following provisions are applicable, except as modified by the AHJ.

All doors and other openings associated with the data center (e.g., data center floor, critical facilities rooms and areas, network facilities, etc.) should be provided with status devices (contacts, hinges, etc.) that annunciate and record all events to the access control and permanent documentation system(s).

All pedestrian doors located within the data center and computer room areas should comply with the required provisions for egress as follows:

- A sensor on the egress side must unlock the door upon detection of an occupant approaching the door
- The locking system is fail-safe
- All doors must utilize listed panic or fire exit hardware that, when operated, unlock the door
- A request-to-exit (REX) manual release device is provided adjacent to the door unlocks the door that meets the following requirements:
 - Has appropriate signage (“PUSH TO EXIT”)
 - Directly interrupts power to the door lock (e.g., is hardwired into the door lock control circuit)
 - When activated, unlocks the door for at least 30 seconds
- Initiation of an alarm condition in the facility fire alarm system or activation of the facility sprinkler system automatically unlocks the door, and the door remains unlocked until the fire alarm system is manually reset.

When enhanced security is required in the data center or computer room, exit doors should be equipped with delayed egress locking systems that do not allow egress for a typical period of 15 to 30 seconds after pressing of the exit device for no more than 3 seconds with the following provisions:

- Initiation of an alarm condition in the facility fire alarm system or activation of the facility sprinkler system automatically unlocks the door, and the door remains unlocked until the fire alarm system is manually reset.
- Initiation of the release process activates an audible alarm and visual signal in the vicinity of the door.
- After release, locking shall be by manual means only.
- Signage on egress side of door is provided (“PUSH UNTIL ALARM SOUNDS. DOOR CAN BE OPENED IN 15 SECONDS”).

Emergency exits should be monitored and alarmed if the door is opened for any reason without release from the access control system. The delay period should be determined by the amount of time needed for guard response, surveillance activation, or other method activated to monitor the location and reason for the emergency exit alarm.

An interface with the VSS should be provided to permanently archive the buffered video for the period before, during, and after a door alarm condition to allow security personnel to respond to the incident and investigate the incident.

12.7.2.4 Electronic Access Control (EAC)

12.7.2.4.1 General

All electronic access control (EAC) systems should be able to track the movement through access points independently. Each employee should have a unique pin or identification code, card, or other physical or electronic method of authentication.

Automated EAC systems should record all of the following:

- Entry and exit time
- Identification of the entrant
- Authorization mechanism

12.7.2.4.2 Touchpads

When keypads are used, they should utilize a high-security approach where each numeral is randomly scrambled to a new position each time the start button is pressed. This way, a bystander cannot see the code, learn the pattern, or identify telltale wear marks on certain keys to access where the ID code or PIN number cannot be accidentally shared with or stolen by onlookers.

When possible, the touchpad should be a hybrid device and contain a card reader or other electronic access control authentication method.

12.7.2.4.3 Card Systems

Card systems for access control provide a unique access/identification card for every individual with access authorization. Card readers are provided at all designated access entrances to the facility, which interface with the security system and door controls to unlock or open doors when a valid card is presented to the reader.

There are a variety of access card technologies and options available today, including:

- Barium ferrite
- Embossing readers
- Hollerith readers
- Magnetic stripe
- Optical character
- Proximity
- RFID
- Smart cards
- Watermark magnetic
- Wiegand wire

Card access technology should be integrated into the ID badge when possible.

12.7.2.4.4 Biometrics

Biometric authentication refers to technologies that measure and analyze human physical characteristics for authentication purposes. Biometrics is usually used in conjunction with identification card access to decrease database search times and improve reliability. Examples of physical characteristics used by biometric systems include:

- Fingerprints
- Eye retinas
- Eye irises
- Facial patterns
- Hand measurements

12.7.2.5 Special Access Control Applications

12.7.2.5.1 General Recommendations

All electronic card access systems for the data center should incorporate and have active the ability to detect more than one individual going through a controlled doorway with only one card or biometric authentication. Ultrasonic scanning of the mantrap compartment can verify that there is only one individual entering the facility and eliminates the ability of unauthorized individuals to piggyback behind an authorized employee, contractor, or visitor.

All electronic card access systems for the data center should incorporate and have active the anti-passback feature. This feature should only permit one entry without an accompanying exit. When activated, this feature should not interfere with normal and authorized movement within the data center or computer room but limit the ability of more than one employee, contractor, or visitor to use the card for the same ingress or egress.

In high-value or sensitive areas with restricted access, security designers should consider the use of the “two man rule.” This feature of electronic access control systems requires that at least two authorized persons be in any specified area at the same time. When a restricted room or area is empty, two authorized persons must use their access cards within a specific period, typically 45 seconds, or entry is denied and a log entry or some sort of notification is made.

12.7.2.5.2 Mantraps

Mantraps should be designed to provide secure access control, with or without the presence of security personnel, through the use of two interlocked doors on opposite sides of a controlled access compartment. Mantraps can utilize card readers, biometric scanners, and ultrasonic scanning of the mantrap compartment to limit the area to a designated number of authorized personnel able to pass into the secured area. Mantraps can be utilized to control both entry and exit.

In addition to the access control and intrusion sensors, each mantrap should also have the ability to sense chemical, biological, radiological, and nuclear threats within the controlled access compartment.

12.7.2.5.3 Sally Ports

Sally ports consist of a controlled pedestrian or vehicular interior or exterior space secured with two controlled and interlocked doors or gates. Sally ports operate by allowing personnel or vehicles entering the facility to enter the sally port space, and then close the first door before authentication occurs, with the second door being opened only after authentication is completed. Security options that should be considered when designing sally ports for the data center include:

- Designed to facilitate identity verification and authentication while the vehicle and pedestrian is still secured in the sally port space.
- When installed inside a building, sally ports should be able to withstand predetermined levels of explosions.
- Provide safe and isolated location for identification, authentication, and inspection.
- Should have fixed and mobile surveillance to facilitate inspection of vehicles.
- Should have normal and emergency communication equipment installed.
- Should have a secure room with access to the sally port for interviews without the need to leave the sally port area.
- Sally ports can be constructed of a variety of materials, ranging from barriers, such as a chain link fence for outdoor applications to explosion resistant glazed material for the in-building designs.

Sally ports should also be designed to restrict entry to one vehicle at a time to prevent unauthorized entry into the secured space via “piggybacking” or “tailgating”.

12.7.2.6 Turnstiles

If turnstiles are utilized to control pedestrian access to secure data centers, the turnstile should be full height and either integrated with the electronic access control system or monitored and controlled by guards. Half-height turnstiles are easily overcome and provide little security if not augmented by guards or other countermeasures.

12.7.2.7 Gatehouses

Considerations when designing and building gatehouses/guardhouses should include:

- Must provide unobstructed observation in all directions.
- Located in the center of the roadway, providing the ability to stop and inspect vehicles entering and exiting.
- Sufficient access for the volume of vehicles during shift changes and other busy times.
- Traffic arms, pop-up bollards, or other mechanisms to effectively control vehicular traffic.
- Access control for after-hours ingress and egress.
- A turnstile for pedestrian traffic if no inadequate pedestrian traffic control or sidewalks exist or cannot be sufficiently controlled by security staff.
- Buffer areas for those without prior authorization or for handling of employees, contractors, or others who have lost or have problematic identification badges.
- VSS surveillance using multiple cameras to monitor and record images of the driver/passengers, front and rear license plate locations, and a general view of the gatehouse and gate area.
- At least one concrete-filled bollard at each corner of the guardhouse at least 1 m (3.5 ft) high. Metal highway barriers are an acceptable alternate.
- Bullet resistance in high crime areas.

A remote gatehouse/checkpoint can reduce the number of guards or employees needed to secure a perimeter. If a remote gatehouse/checkpoint is used it should have the following features:

- VSS providing images of approaching vehicles, drivers, and optionally, the gate
- Lighting for after dark operation
- Intercom system
- A motor-operated gate
- One or more access control systems (e.g., cards, biometrics, keypads)
- Loop detectors

12.7.2.8 Badging and Identification

Identification badges should be issued by the employer and contain sufficient data to properly identify and authenticate the bearer. Information contained on the badge should include some or all of the following:

- Name of the bearer
- Department or division
- A photograph of the employee, contractor, or visitor
- A physical description of the employee, contractor, or visitor
- Special access privileges (e.g., computer room access)
- Date of issue or expiration
- Embedded/coded information required for high security such as biometric information for smart card badges

ID badges should be distinctive and difficult to forge or alter. In addition to the basic information, each ID badge should contain distinctive color symbols.

ID badges should be designed for the foreseeable circumstances of their use in the operation of the data center, including:

- Access control
- Meal purchase
- Inventory control
- Time and attendance
- Parking

All employees should be issued and required to display identification badges.

The data center should charge for replacements for lost badges where no acceptable explanation is provided or at some multiple of lost badges.

Lost badges that later are found to be used or attempted to be used by the employee, another employee, contractor, or visitor should trigger an immediate investigation.

Badges should be laminated in order to provide the highest level of tamper resistance.

Temporary identification badges should be issued for all visitors, contractors and delivery personnel.

All temporary identification badges should have some visible method by which employees, security, and law enforcement personnel can easily determine whether the badge has expired. Possible methods for ensuring that expired badges are not reused include:

- A rotating color scheme
- The expiration date printed on the badge
- The day of the week printed on the badge
- Use of self-adhesive tokens that gradually expire over a predetermined period, typically one day
- Use of badges that gradually expire over a given period, gradually displaying bars or some other visually distinctive method (see Figure 12-2)

Visitor, contractor, or delivery person badges should be visually distinctive from those worn by employees.

Identification badges should prominently display which visitors, contractors, and delivery personnel must be escorted.

Digital photos taken at the time of ID badge issuance should be stored securely for later comparison with individual ID badges.

12.8 Alarms

12.8.1 Introduction

Alarms utilize one or more sensor technologies to detect a variety of conditions relevant to the security of the data center. Sensor technology includes:

- Audio
- Capacitance
- Electro-mechanical
- Glass break sensors
- Passive infrared (PIR), which detects thermal or infrared images
- Light (e.g., photoelectric, laser)
- Ultrasonic and microwave
- Vibration

12.8.2 Recommendations

12.8.2.1 General

Audio sensors should be used in the data center perimeter to detect and record any sound in a protected area or filter sounds traveling along fencing or telecommunications conduit to eliminate sounds from traffic or weather and trigger an alarm if impact, cutting, or digging is detected.

Capacitance sensors should be used in the data center to detect changes in electronic fields and are primarily limited to monitoring the electronic field around protected objects.

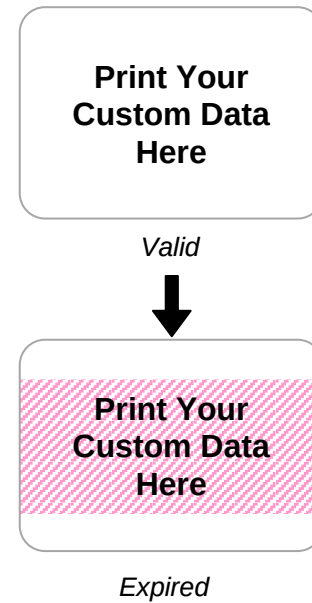


Figure 12-2
Example of a Visually Distinctive Expired Badge

Electro-mechanical sensors include things like foil, wire and screen detectors, pressure mats, and mechanical and magnetic contacts. When used as sensors in the data center, they should be installed so that the activity of the intruder causes some movement or pressure triggering an alarm and can be mounted on or in a wide variety of locations.

Glass break sensors can be installed on a wall or ceiling surface, but to directly receive the sound waves needed to trigger the sensor, they should be mounted directly across from the window being monitored. Some glass break sensors are subject to false alarms from RFI. Glass break sensors used in data center applications should contain technology immune from RFI induced false alarms.

Passive infrared (PIR) sensors in the data center should be installed so that an intruder must pass across its field of view. PIR devices can be used to protect perimeters, areas, or objects. This includes areas where barriers or mechanical detectors were historically the only countermeasure available, including skylights and maintenance holes.

Known conditions that create false alarms are:

- Rapid changes in temperature
- Bright windows or direct sunlight
- Insects
- Drafts
- RFI

Photoelectric sensors installed in the data center or campus should be used indoors or outdoors in any location where an invisible beam of light is monitored at the receiving end for interruption. False alarms can be triggered by some atmospheric conditions like snow and heavy rain or in an outdoor environment by animals.

Ultrasonic and microwave sensors operate much like PIR sensors, but they substitute sound waves for infrared detection as a trigger. These sensors should be used indoors where the types of movement are limited to protected area such as offices, storage areas, TRs, loading docks, and areas of the data center.

Vibration sensors should be placed in locations where there is a possibility of an attempt to penetrate a wall or floor of a safe, vault, storage area, or other secure area of the data center. Purpose-built data centers or highly secure sites should use sensors within or upon the exterior boundary fencing.

NOTE: Sensors should be hidden or not easily accessible, which may be accomplished through specific fencing materials, construction, or aesthetic elements.

Other sensors that should be considered for use in and around the secure areas of a data center include the following, which are commonly referred to as CBRNE sensors:

- Chemical
- Biological
- Radiological
- Nuclear
- Explosive

12.8.2.2 Intrusion

Intrusion alarms should be used to detect the presence and movement of unauthorized persons at a point of entry, room or general area, or in the proximity of an object.

Intrusion alarms should utilize one or more of the basic alarm triggers as follows:

- Break in an electrical circuit
- Interrupt a light beam
- Detect a sound
- Detect a vibration
- Detect a change in capacitance

12.8.2.3 Other Alarm Systems

Fire detection and prevention is covered in detail in Section 11.

Water detection is covered under leak detection in Section 10.

12.8.2.4 Integration

All alarm outputs should be terminated in one of three methods/locations:

- Local
- Central station
- Proprietary connection (security command center)

Direct connections of selected alarm outputs to EMS, fire, or law enforcement may be implemented if desired or implemented as required by the AHJ.

Local alarms should not be used as the only termination in a data center facility as there is no guarantee that the alarm will be detected and acted upon. Local alarms do have advantages when layered with other termination methods. Those advantages include:

- Psychological deterrent
- Low cost
- May interrupt criminal or unauthorized activity

If central station termination is utilized, the data center operator should periodically test and evaluate the training and response of the monitoring company. If the monitoring service also includes first responder alarm investigation, the background and training of the central station alarm investigators should be periodically evaluated.

Alarm and access control systems must be integrated to allow coordination of programming of desired security operational parameters and a coordinated response to alarm conditions. For example, in many facilities, initiation of a fire alarm signal will be programmed to automatically unlock emergency egress doors in the facility to allow quick evacuation of the facility by personnel. Initiation of a security alarm by motion detectors can be programmed to initiate automatic display of video of the location on the security system computers.

12.9 Surveillance

12.9.1 Introduction

Security employs two types of surveillance: physical and technical. Physical surveillance techniques are primarily done by humans and are outside the scope of this standard. Technical surveillance is accomplished by electronic equipment, typically cameras and other elements of a VSS.

The VSS serves several purposes in the security of the data center:

- Enable security and monitoring personnel to centrally view many locations simultaneously.
- Provide a visual record of monitored area during alarms and access control events.
- Record crimes, civil, and operational offenses for use as evidence in prosecution and human resources processes.
- Record monitored areas and employee activity for use as a defense in civil and criminal prosecution against the data center.
- Function as part of the video analytics system, which analyzes video content, apply system rules, and produce alarms when conditions are met (e.g., movement within an area that is scheduled to be unoccupied).

12.9.2 Recommendations

Placement of cameras, frames per second, resolution, lighting, and other criteria should all be determined as a result of a risk/threat and vulnerability assessment. A qualified security consultant should identify the vulnerable areas and evaluate the operational, technical, and environmental parameters before the VSS design is approved.

Camera placement should be coordinated with lighting designers to provide adequate image resolution to recognize faces, vehicles, types of activity, and other significant facts. This is especially important in outdoor situations where the type of image sensing technology, lens characteristics, and lighting can affect the usability of view or recorded video.

VSS equipment should provide views of both the front and rear of all in-scope systems, clearly identify individuals within the secured environments, and be time stamped.

Cameras should be protected against theft, vandalism or neutralization. Protection for cameras should include:

- Mounting the camera out of reach of pedestrian and vehicular traffic.
- Protecting the camera in a secure enclosure or dome.
- Environmental protection in extreme heat or cold conditions or when the camera's operation requires a controlled environment.
- Securely mounted and fastened to a stationary object.
- In high-risk situations, the camera may have an alarm sensor or switch attached.
- IP cameras can utilize simple network management protocol (SNMP) and trigger an alarm if the camera drops off the network.

When selecting a camera for any overt or covert monitoring scenario, the designer should consider the following performance criteria before selecting any elements of a VSS:

- Video analytics
- Backlight compensation
- Environmental operating limits
- Image sensing device
- Internet protocol (IP) capabilities
- Light compensation
- Method of synchronization
- Power over Ethernet capabilities
- Resolution
- Sensitivity
- Signal-to-noise ratio (SNR)
- Size—dimensions and weight
- Telemetry
- Video output level

Fixed cameras are designed to monitor a defined area and come with adjustable aiming provisions and lenses to allow field setting of the coverage zone and focal length. Once set in the field for the focal length and coverage area, they remain fixed.

Pan-tilt-zoom (PTZ) cameras have an integral motorized mechanism that allow remote control from a special joystick/keyboard controller to move the field of coverage and change image magnification within the limits of the camera. PTZ cameras can be programmed to automatically sweep designated areas within their field of view and can be manually controlled to cover areas or zoom in to an area where suspicious activity is detected.

Cameras mounted outdoors should be environmentally resistant and to have integral heaters and blowers to maintain the housing interior temperature within the camera's operating limits.

When low-light conditions are anticipated, the VSS should utilize cameras designed for this condition as follows:

- Day/night cameras are often used to provide color video during daytime conditions, which switch to monochrome video during nighttime conditions with lower lighting levels.
- Infrared (IR) illuminators generate infrared light that is nearly invisible to the human eye but will enable IR-sensitive cameras to produce high-quality images under nighttime conditions without requiring visible light illumination.
- Cameras should be installed to maximize the amount of lighting coming from behind the camera or directed in the same direction as the camera; avoid light sources that provide direct illumination on the camera lens. Current camera technology utilizes charge coupled device (CCD) chips, which are more sensitive to low light and the IR spectrum.
- Lighting sources for areas having video surveillance should have good color rendition such as fluorescent or HID metal halide. Avoid use of low-pressure sodium, high-pressure sodium, and mercury vapor lamp sources, which have poor color rendition and do not adequately support video surveillance equipment performance.

Some video surveillance systems have "video analytics" capability that allows distinguishing of movements detected by the cameras and triggering programmed response such as alarms, recording, or log entries. Cameras utilizing video analytics should be used to monitor high-value or sensitive equipment or areas of the data center where a specific asset is at risk or where it does not make sense to record the surveillance 24/7 such as very sporadic offenses.

Nonfunctioning, decoy or “dummy” cameras should not be used for any area of a data center. Decoys may be easily detectable and, if discovered, can lead to additional liability for the management of the data center facility.

IP cameras should be considered when selecting the VSS for the data center. They have the following performance advantages described below, but they require coordinating with network engineers to operate properly without degrading network performance:

- Cameras can use power over Ethernet (PoE), eliminating the need for separate power supplies, reducing labor and cable costs.
- Additionally, PoE can increase the resiliency of the cameras/security and reduce installation costs because PoE network devices are normally on redundant UPS and generators.
- Surveillance distribution is available to authorized users directly off the network.
- Existing structured cabling system (SCS) infrastructure is used in an open architecture.
- Camera system is scalable and easily expanded.
- Routine permanent archiving of video to capture authorized occupant entries and exits from the facility or controlled spaces may be done utilizing a network storage system rather than physical media.
- Archived video is often employed to maintain a record in case an incident occurs that requires an investigation.

If the VSS is monitored locally by guards or other personnel, the method(s) by which the cameras are monitored should be determined by the threat/risk and vulnerability of person(s) or assets in the area being monitored. The four methods of monitoring surveillance cameras include:

- Dedicated monitors
- Split screens
- Sequential switching
- Alarm switching

Integration of the VSS with alarms or access control applications should be part of the data center security plan. Examples of this would include automatic switching to a fixed camera when the two-man rule is violated for the computer room, or in the same scenario, having a PTZ camera automatically move to the data center access control point when the same alarm occurs.

The use of SNMP also should be used for events and alarms triggered by unauthorized access to or removal of physical layer infrastructure in the data center. An example of this would include the integration of fixed VSS cameras, intelligent patching and integrated alarms in a remote telecommunications room, where the attempted insertion into a data switch activates the surveillance system and notifies the network operations center of the possible unauthorized access.

12.10 Barriers

12.10.1 Definitions

Definitions used in this section are as follows:

barrier: a fabricated or natural obstacle used to control access to something or the movement of people, animals, vehicles, or any material in motion.

clear zone: an area separating an outdoor barrier from buildings or any form of natural or manufactured concealment.

compartmentalization: the isolation or segregation of assets from threats using architectural design or countermeasures, including physical barriers.

layering: the use of many layers of barriers, other countermeasures, or a mixture of both used to provide the maximum level of deterrence and delay (see Figure 12-3).

natural barrier: any object of nature that impedes or prevents access, including mountains, bodies of water, deserts, and swamps.

psychological barrier: a device, obstacle, or lack of obstacle that, by its presence alone, discourages unauthorized access or penetration.

structural barrier: something that physically deters or prevents unauthorized access, movement, destruction, or removal of data center assets.

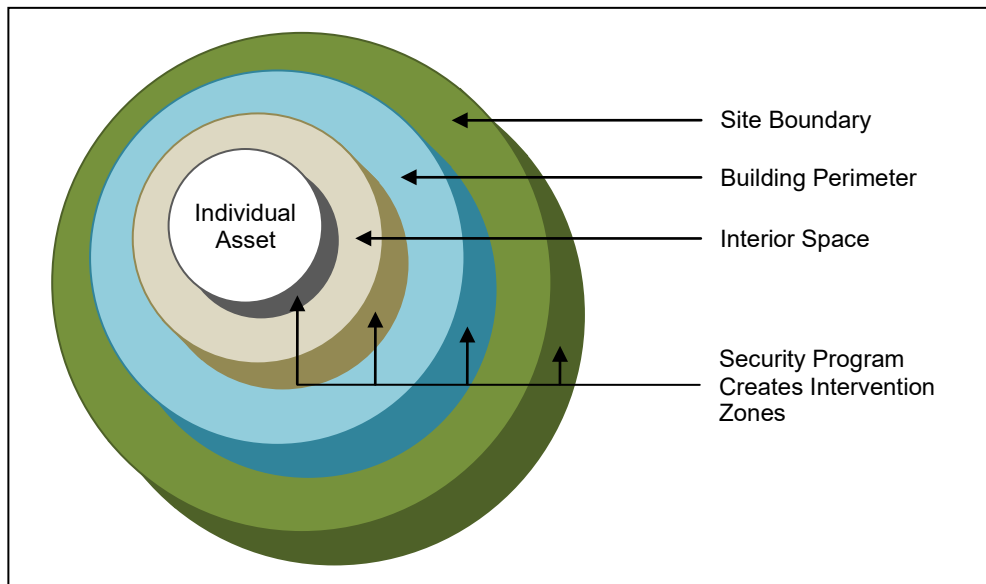


Figure 12-3
Security Layers

12.10.2 Introduction

Barriers can be classified into three major groups:

- Building exteriors
- Fences
- Masonry structures

Structural barriers are not impenetrable, but they are primarily used to delay entry so that another system(s) can detect and notify employees, guards, monitoring stations, or law enforcement. At a minimum, good use of barriers will force the intruder to leave evidence of penetration and simultaneously trigger an electronic or human countermeasure.

Structural barriers should be put in place to protect against accidental and intentional explosions. The architect and security designer for the data center should consider the relative resistance to explosion that the various barriers offer. The following list of barriers is organized from the most blast resistance to the least:

- Thick, reinforced concrete walls
- Thick brick or concrete walls without reinforcement
- Reinforced concrete walls
- Thick earthen barricades
- Building walls with steel frames
- Sturdy wooden frame walls
- Common brick walls
- Wire-reinforced glass
- Common glass

Table 12-1 demonstrates the thickness of a concrete wall needed to protect from the secondary damage caused by projectiles launched by an explosion at varying distances:

Barriers should be designed in layers so that the asset(s) that need to be protected lie behind or inside multiple levels with the objective of each barrier to create as much delay as possible.

Barriers should also be used to prevent or delay the unauthorized movement or removal of objects by employees, visitors, contractors, or other occupants.

Barriers should be used to delay or prevent access to or damage to the site, buildings, or areas of the data center.

Table 12-1 Thickness of Concrete Wall for Projectile Protection

<i>Distance from Explosion m (ft)</i>	<i>Projective Velocity m/s (ft/s)</i>	<i>Concrete Wall Thickness mm (in)</i>
30.5 m (100 ft)	610 m/s (2,000 f/s)	305 mm (12 in)
69 m (225 ft)	610 m/s (2,000 f/s)	254 mm (10 in)
152 m (500 ft)	457 m/s (1,500 f/s)	178 mm (7 in)
274 m (900 ft)	305 m/s (1,000 f/s)	127 mm (5 in)
716 m (2,350 ft)	152 m/s (500 f/s)	64 mm (2.5 in)

Source: *Protection of Assets Manual*, ASIS International

A barrier can also be utilized to prevent visual access to a building or asset. Preventing visual access will prevent the potential offender from knowing the location of the asset or that it even exists. An example of a visual barrier would be locating a data center inside an old warehouse or inside of a dense forest with no visual clues of its existence.

Barriers should be utilized to delay or prevent three types of penetration:

- By force
- By deception or stealth
- By accident

When barriers are used outdoors, a clear zone free of anything that could offer concealment, such as trees, weeds, rubbish, small buildings or vehicles, should be maintained.

Guidelines for clear zones around barriers used at data center site perimeters include:

- Clear zones should be maintained on both sides.
- The outside of the barrier should be at least 6 m (20 ft) away from all potential visual obstructions, including buildings, roads, parking lots, and natural objects like trees, rocks, and hills.
- The inside of barriers used for a perimeter should maintain a clear zone that is at least 15 m (50 ft) away from any building or other asset.

12.10.3 Vehicle Barriers

The data center architect and security designer should take into consideration the escalating use of vehicles to both inflict primary damage to buildings and persons (intentional and accidental), as well as a delivery mechanism for explosive devices.

Barriers that should be considered when designing protective barriers for the entrances and other vulnerable areas of the data center site and buildings include the following:

- Fences
- Metal highway guard rails
- Concrete vehicle bollards and barriers
- Concrete Jersey barriers
- Metal beams or posts
- Combinations of material such as tires, railroad ties, and earth

Table 12-2 illustrates the vulnerability of various barriers to penetration by vehicles.

Table 12-2 Vehicle Barrier Comparison

<i>Barrier Tested</i>	<i>Vehicle</i>	<i>Barrier Damage</i>	<i>Vehicle Damage</i>	<i>Occupant Injury</i>
Chain link fence	3/4 ton pickup truck	Full penetration	Paint scratched	No injury
Double swing gate	3/4 ton pickup truck	Full penetration	Slight dents	No injury
Chain link fence with 19 mm (0.75 in) cable	3/4 ton pickup truck	Full penetration, vehicle stopped, cable held	Extensive front end damage	Risk of injury
Concrete media barrier	3/4 ton pickup truck	No penetration	Major damage	Risk of injury
Tires	3/4 ton pickup truck	No penetration	Major damage	Risk of injury

Source: *Barrier Technology Handbook*, Sandia Laboratories

12.10.4 Building Exteriors

Building exteriors should be evaluated for their ability to delay potential attacks on the data center.

During data center planning, the ability of all building surfaces should be evaluated for their performance as security barriers. Existing structures being retrofitted as a data center should include both a physical survey of the structure and a review of available architectural drawings created during initial design and construction.

Evaluation of the architectural drawings and physical inspection of an existing building for the effectiveness of any wall, ceiling, or floor should consider the following metrics at a minimum:

- Amount of space existing between walls, ceiling, and floors
- Risk introduced by the existing or updated HVAC air handling spaces
- Modification of the original walls, ceiling, or floors
- Weaknesses revealed during the physical inspection
- Rooftop accessibility from adjacent structures
- Underfloor accessibility through tunneling
- Underfloor accessibility through drainage tunnels, subways, and other subterranean passageways

The six walls (floor, ceiling, and vertical walls) of any structure housing a data center should be composed of reinforced concrete or other masonry components because of the increase in penetration time over other commonly used materials.

12.10.5 Concrete Walls

Concrete walls make excellent barriers and offer excellent psychological deterrence and physical delay. Success in using concrete walls as barriers will depend on the thickness of the concrete and materials used for reinforcement. General guidelines for concrete walls can be found in the following sections.

Concrete or block walls that are used to support structural loads are not necessarily designed to provide enough delay to be an effective barrier. Unreinforced concrete walls offer little protection from penetration. For the security of a data center, all concrete walls should include steel reinforcing bars or rebar. Table 12-3 demonstrates the speed at which a 300 mm (12 in) thick reinforced concrete wall can be penetrated.

Concrete block walls that do not include a reinforcing material offer almost no resistance to penetration using small hand tools. When used for data center construction, concrete block walls should include some type of reinforcing methodology, typically filling the hollow core with concrete or mortar, installation of rebar, or both:

- 100 mm (4 in) thick reinforced concrete walls are typically used for curtain walls and provide little resistance to penetration with hand tools.
- 150 mm (6 in) thick reinforced concrete walls offer more delay, but they are still vulnerable to hand tools and small explosions.
- 200 mm (8 in) thick reinforced concrete walls are common as load-bearing structural support walls and can also be penetrated using hand tools.
- Concrete walls of greater than 200 mm (8 in) are usually found only in the construction of vaults or blast-resistant bunkers.

Table 12-3 Speed Of Concrete Wall Penetration*300 mm (12 in) thick concrete with #5 rebar on 150 mm (6 in) centers*

<i>People Needed</i>	<i>Equipment Needed</i>	<i>Equipment Weight kg (lb)</i>	<i>Minimum Time min</i>	<i>Maximum Time min</i>
2	Explosives, tamper plate, hand hydraulic	22 kg (48 lb)	2.8	8.4
2	Explosives, hand hydraulic bolt cutters	18 kg (39 lb)	2.8	8.4
1	Explosives, platter	102 kg (225 lb)	1.95	5.85
2	Roto hammer, sledge, punch, handheld power hydraulic bolt cutters, generator	73 kg (161 lb)	15.0	45.0
2	Explosives, tamper plate, handheld hydraulic bolt cutters	69 kg (153 lb)	1.4	4.2

Source: *Barrier Technology Handbook*, Sandia Laboratories

NOTE: Studies have shown that it can take under a minute to create a person-sized hole in a 200 mm (8 in), mortar-filled block wall with a common sledgehammer and only a few more seconds if 13 mm (0.50 in) steel rebar is added.

12.10.6 Building Openings

Building openings generally are utilized for one of the following purposes:

- Entrance (pedestrians and vehicles)
- Exit (pedestrians and vehicles)
- Natural illumination
- Ventilation
- Material movement (loading docks)
- Utility access
- Drainage

Any building opening less than 5.5 m (18 ft) above ground and larger than 62,000 mm² (96 in²) should be protected by a barrier, alarmed or monitored, for use as an unauthorized access point.

Building openings should be at least as difficult to penetrate as the walls, ceilings, or floor of a data center. Table 12-4 illustrates the amount of time needed to penetrate the standard industrial pedestrian door.

Doors are typically built from one or more of the following materials or a combination of them:

- Wood
- Glass
- Metal

The following should be considered when considering the design and construction of doors for the data center:

- If wooden doors are used, ensure that no gap exists between the doorstop and the doorjamb, which would allow shims or levers to be inserted.
- Hinge pins and mounting screws should always be mounted toward the protected side of the door.
- Hinge pins should always be welded or flanged to prevent unauthorized removal.
- When possible, hinges should be fastened through the doorframe, into the wall stud, or other structural member.
- Doorframes should be securely fastened to the wall studs or other structural member.

Windows mounted on the exterior of a data center building shell are designed for provide natural light, natural ventilation, and visual access, none of which are necessary or advisable for the computer room and many of the secured areas of the data center.

Table 12-4 Time to Penetrate Industrial Pedestrian Doors

<i>Penetration Method</i>	<i>Noise dB</i>	<i>Attack Area</i>	<i>Time Needed (minutes)</i>
Explosives	–	Door face	0.5–1.5
Thermal (Oxy-Lance)	70–76	Door face	1.5–2.5
Thermal (cutting torch)	60–64	Door face	2.0–6.0
Power drill	–	Panic bar	0.5
Axe through metal	72–110	Panic bar	1.5–5.0
Axe through glass	76–100	Panic bar	0.5
Lock pick	–	Lock	0.25–5.0
Wrench	–	Lock	0.5
Pry bar	74–76	Lock frame	0.5
Thermal (cutting torch)	60–73	Hinge pins	0.5–1.5
Hammer and punch	72–75	Hinge pins	1.0–3.0
Explosives	–	Hinge pins	1.0–2.5
Crowbar	60–100	Mesh/window	0.5–2.0

Source: *Barrier Technology Handbook*, Sandia Laboratories

The types of windows used in modern construction include:

- Awning
- Casement
- Horizontal sliding
- Jalousie
- Picture
- Projected

Only picture windows should be installed in any exterior walls of the data center shell.

Exterior windows should be included in the security risk assessment and the appropriate mesh or glazing material consistent with the desired delay or blast resistance desired.

If one or more of the walls of a computer room are exterior walls, there should be no windows of any type on the exterior computer room walls.

Exterior windows should never use putty or molding to secure the panes of glass or plastic in the frame. Only frame mounted (grooved) type of window mounting should be permitted for the data center shell.

Table 12-5 should be used as a guide when determining the amount of delay desired for a window.

12.10.7 Glazing

12.10.7.1 Overview

Glazing is the installation of glass, plastic, or glass/plastic laminates to increase building surface (especially windows and doors) resistance to explosion, impact, fire, or other threats.

When glass is utilized to fill building openings on the exterior of the data center building shell or interior wall openings, consideration should be given to the danger to occupants and equipment should an explosion occur. If interior or exterior glass is broken, the following undesirable events could occur:

- Unauthorized entry
- Physical injury because of sharp glass fragments, especially when they become airborne as the result of an explosion.
- Property damage to data center assets because of airborne sharp glass fragments following an explosion.
- Physical or property damage because of fragments of glass falling.

Table 12-5 Time to Penetrate Windows

<i>Type of Window</i>	<i>Tool</i>	<i>Penetration Time (minutes)</i>
<i>Glass</i>		
6 mm (1/4 in) tempered	Fire axe	0.05–0.15
6 mm (1/4 in) wire	Fire axe	0.15–0.45
6 mm (1/4 in) laminated	Fire axe	0.30–0.90
14 mm (9/16 in) security	Sledgehammer, Fire axe	0.75–2.25
<i>Plastic</i>		
6 mm (1/4 in) Lexan [®] , Lucite [™] , or Plexiglas [®]	Fire axe	0.05–0.15
	Demolition saw	0.15–0.45
13 mm (0.5 in) Lucite [™] or Plexiglas [®]	Fire axe	0.05–0.15
	Demolition saw	0.35–1.05
13 mm (0.5 in) Lexan [®]	Fire axe	2.0–6.0
	Sledgehammer	2.0–6.0
25 mm (1 in) Lucite [™] or Plexiglas [®]	Sledgehammer	0.05–0.15
	Fire axe	0.10–0.30
<i>Glass with enhancements</i>		
Glass with 2.9 mm (9–gauge) Mesh	Fire axe, Bolt cutters	0.25–1.35
Glass with 19 mm (3/4 in) Quarry screen	Demolition saw	0.75–2.25
	Cutting torch	1.35–4.05
Glass with 13 mm (0.5 in) Diagonal bars	Bolt cutters	0.5–1.5
	Hacksaw	1.3–3.9

Source: *Barrier Technology Handbook*, Sandia Laboratories

In conjunction and compliance with local codes and safety regulations, tempered glass should always be used in data center windows and doors. It is 3 to 5 times stronger than ordinary glass, and because of the effects of the tempering process, there is a decreased risk of injury and reduced fragment size of glass fragments following an explosion or penetration.

Plastic or polyester film should also be considered as a method to reduce the risk of injury, damage, and penetration from explosion or forced entry. Film reinforced windows reduce the fragment hazards by retaining glass fragments following an explosion or shattering incident.

Wired glass should also be considered for use in both interior and exterior installations. Many fire and safety codes require the use of glass with wire mesh embedded. It is important to note that while wired glass offers resistance to penetration from large objects, it offers little or no protection from shattered glass fragments or smaller projectiles.

Laminated glass, consisting of alternate layers of glass and plastic, should be considered for any window or door where impact resistance is essential. Tempered, wired and film reinforced glass all resist the initial impact, but they frequently fall away allowing unauthorized entry. Conversely, laminated glass remains in place and retains the ability to deter and further delay entry.

Some laminated glass has electrical properties that permit its use as an alarm. During the attempted penetration of the glass, an alarm is triggered allowing a) the sounding of audible burglar alarms or b) security or law enforcement personnel to gain valuable response time.

Because of their overall strength and resistance to breakage, designers should consider the use of acrylic and polycarbonate-based windows and door glass. These materials are approved for safety and have up to 17 times more resistance to breakage than glass of comparable thickness.

12.10.7.2 Bullet Resistant Glass or Glazing

If the threat of gunfire or other projectiles is present, the data center should consider the use of bullet-resisting glass. It is important to fully evaluate the nature and type of attacks being protected against since bullet-resisting glass is available in a variety of thicknesses (19 mm [3/4 in] to 119 mm [4.7 in]) and construction. Attacks can range from individuals with rocks or hammers to high-powered rifles, machine guns, or missiles. It is important to properly assess the risk and threat before selecting bullet-resisting glass.

Security designers should consider the eight levels of resistivity defined in UL 752, which quantifies resistivity based upon the ammunition used and shot pattern or placement:

- Level 1—4.8 mm (3/16 in) thick, solid, open-hearth steel with a tensile strength of 345000 kPa (50,000 psi) or 9 mm full copper jacket with lead core, 124 grain at 358 m/s (1,175 ft/s) – 3 shots
- Level 2—0.357 Magnum lead soft point, 158 grain at 381 m/s (1,250 ft/s) – 3 shots
- Level 3—0.44 Magnum lead, semiwadcuter gas checked, 240 grain at 411 m/s (1,350 ft/s) – 3 shots
- Level 4—0.30 caliber rifle lead core soft point, 180 grain at 774 m/s (2,540 ft/s) – 1 shot
- Level 5—7.62 mm rifle lead core full copper jacket, 150 grain, 838 m/s (2,750 ft/s) – 1 shot
- Level 6—9 mm full copper jacket lead core, 124 grain, 427 m/s (1,400 ft/s) – 5 shots
- Level 7—5.56 mm rifle lead core full copper jacket, 55 grain, 939 m/s (3,080 ft/s) – 5 shots
- Level 8—7.62 mm rifle lead core full copper jacket, 150 grain, 838 m/s (2,750 ft/s) – 5 shots

Supplemental—All tests have a supplemental shotgun test using a 12-gauge shotgun with 1 rifled lead slug, 437 grain, 483 m/s (1,585 ft/s) and the other 00 lead buckshot with 12 pellets, 650 grain, 366 m/s (1,200 ft/s).

12.10.7.3 Burglary-Resistant Glass or Glazing

The data center may be at a high risk for burglary because of quantity and value of the ITE located there. Any window or door containing glass should be evaluated for its resistance to burglary. Some of the criteria used to evaluate the resistance of glass to burglary include:

- Single blow impact testing (smash and grab)
- Multiple impact testing
- High-energy impact testing
- Performance

Data center security designers should also be aware of the five classes of protection defined by ASTM F1233, which evaluate and compare security-glazing methods against three metrics:

- Ballistic attack
- Forced entry
- A combination of both

Forced entry testing involves attacking security glazing using a predefined sequence of tools and weapons. The list below each class is in order of occurrence during classification:

- Class I—ball peen hammer
- Class II—ball peen hammer, 38 mm (1.5 in) pipe/sledge, fire extinguisher, sledge hammer, propane torch, ripping bar
- Class III—ram, 100 mm (4 in) pipe/sledge, sledge hammer, propane torch, ripping bar, chisel/hammer, gasoline, angle iron/sledge, sledge hammer
- Class IV—ram, 100 mm (4 in) pipe/sledge, sledge hammer, propane torch, fire axe, sledge hammer, wood splitting maul, chisel/hammer, sledge/hammer, methylene chloride, fire axe, sledge hammer, chisel/hammer, wood maul
- Class V—ram, 100 mm (4 in) pipe/sledge, sledge hammer, propane torch, fire axe, sledge hammer, wood splitting maul, chisel/hammer, sledge/hammer, methylene chloride, fire axe, sledge hammer, chisel/hammer, wood splitting maul

12.10.8 Fences and Metal Barriers

12.10.8.1 General

Fences should not be considered as a permanent barrier to forced entry. They introduce delay but not prevention and should be layered with other countermeasures like alarms, surveillance, and guards.

Security designers should consider that even 2.4 m (8 ft) tall fencing with three strands of barbed wire could be compromised in less than 10 seconds.

Fencing should be considered useful as a barrier for:

- Psychological deterrent
- Mark property boundaries
- Limited vehicle barrier
- Most small animals
- Casual intruders
- Opportunistic offenders

Fence design must take into consideration the type of risk and threat. Many fencing designed to prevent pedestrian entry have little or no delay factor for vehicles. Guard railing along a highway is one type of vehicular fence, which has almost no impact on the delay of pedestrians or animals.

12.10.8.2 Chain Link Fencing

The most widely used fencing for security purposes is the chain link fence.

The Chain Link Fence Manufacturers Institute (CLFMI) and the American Society for Testing and Materials (ASTM) maintain the specifications intended as the recognized standards for quality of manufacturing and installation.

Recommended design and installation guidelines for chain link fencing include:

- Line posts should not exceed 3 m (10 ft) spans on average.
- Post hole depths should be at a minimum of 600 mm (24 in) plus an additional 75 mm (3 in) for each 300 mm (12 in) increase in fence height over 1.2 m (4 ft).
- Terminal posts should be braced diagonally to the closest line post, if no top rail is present, and with no more than a 50° angle between the brace and the ground.
- If no top rail is used, then top tension wire must be installed.
NOTE: Top rails can be used as handholds for climbing the fence.
- The fencing fabric should be 2.9 mm (9 gauge) or greater, and the mesh openings should not be larger than 50 mm (2 in).
- Fencing fabric should reach within 50 mm (2 in) of firm ground, paving, or concrete.
- On soft ground, the fencing fabric should extend below ground and can be set into a concrete apron.
- Any bolts or nuts that are used to fasten any hardware to a fence should be spot welded.
- Any opening for drainage larger than 62,000 mm² (96 in²) should have additional grates, fencing, mesh, grills, or other barriers installed to discourage unauthorized access; drainage should not be impaired.
- For additional delay, a top guard, consisting of three strands of barbed wire, spaced 150 mm (6 in) apart and mounted on the top of the fence at a 45-degree angle outward, inward, or both directions should be considered; since the primary purpose of this fencing is to discourage or delay human entry, the fencing should be at least 2.1 m (7 ft) high, not including the top guard.
- In addition to barbed wire, other barrier protection obstacles can be added to the fencing such as spikes and barbed top guards.
- Gates should be the same height as adjacent fencing (including top guards).
- When privacy is required to conceal activity or remove visual identification of high-value or sensitive assets, strips of material can be woven into the chain link fence; plastic, wood, and fabric are all commonly used for privacy applications.
- Chain link fencing should also be considered for service provider areas, storage, and other areas for temporary security or when hard-walled construction is not an option.

A clear zone should be established for at least 6 m (20 ft) on both sides of the fence with anything that could be used as an aid to climb the fence removed. This includes the trimming of overhanging tree limbs. Other items that might be used to go over the fence include:

- Vehicles
- Boxes
- Ladders
- Construction material (e.g., wood, poles, concrete blocks)
- Skids
- Containers
- Equipment

12.10.9 Metal and Welded Wire Barriers

12.10.9.1 General

Expanded metal fabric consists of sheets of metal (carbon, galvanized, stainless steel, aluminum, and others) that have been cut or shaped and somewhat flattened or thinned for barrier material that:

- Is resistant to cutting
- Will not unravel or uncoil
- Is easy to fabricate and install
- Permits environmental conditioning, lighting, and inspection of secure spaces like storage areas, service provider cages, cabinets, and other data center areas
- Provides enhanced psychological deterrence

Expanded metal barrier material comes in four styles that should be designed for the anticipated risks and threats in the area installed. The four types of generally accepted expanded metal are:

- Standard
- Grate or diamond plate
- Flattened
- Architectural

Welded wire fabric is created by welding a series of wires at right angles forming a wire fabric where at each intersection the wires are welded together.

Welded wire fabric should be used when a less demanding barrier is needed than expanded wire. Other security applications where welded wire is used include:

- Tool rooms
- Utility areas
- Building automation control rooms
- Computer facilities and rooms
- Window guards
- Lockers
- Animal cages (laboratory environment)

Woven wire fabric is considered a barrier, but it is used for less demanding applications, and is not generally acceptable as a security countermeasure.

12.10.9.2 Barbed Wire

For the purposes of this section, barbed wire will also include barbed tape.

Although its original purpose was as an animal barrier, barbed wire is an important auxiliary security enhancement for many barriers, including fencing. Primary uses of barbed wire include:

- Fence fabric
- Top guard for chain link or other fencing
- Concertina coils
- Other barriers

The key benefit of barbed wire is that it is a psychological deterrent and should not be designed as a primary countermeasure to induce delay.

Recommended considerations when using barbed wire in a security design include:

- Number of barbs
- Design of barbs
- Location of barbs

To discourage potential intruders from gripping the barbed wire, designs for data center perimeters and other barbed wire installations should specify four-pointed barbs located on 75 mm (3 in) centers.

Barbed wire strands should be attached to posts that are less than 1.8 m (6 ft) apart with distance between the strands never exceeding 150 mm (6 in).

If soft soils, erosion, or small animals create vulnerabilities, then a single strand of barbed wire should be at ground level. This will also discourage tunneling.

For additional delay, barbed wire strands should be formed into concertina coils. Concertina coils are used in the following ways:

- Top guards on fences and other barriers
- Temporary barriers
- Tactical barriers

12.10.10 Gates

Data center perimeters should include no more gates than are necessary. Each gate provides more opportunity for operational failures (left unlocked or open) and vulnerability.

Gates can be manual or motor operated and are available in the following styles:

- Single-swing
- Double-swing
- Multifold
- Overhead single slide
- Overhead double slide
- Cantilever slide single
- Cantilever slide double
- Aircraft sliding gates

12.11 Lighting

12.11.1 Introduction

Effective lighting is a key component to an overall security program; it is a powerful psychological deterrent to criminal activities, and it enables security personnel to perform their work more efficiently. A good lighting design will include the following design parameters:

- Higher brightness levels improve the ability to detect objects and recognize people.
- Horizontal illumination levels assist in identifying objects that are horizontally oriented such as streets, sidewalks, steps, and horizontal obstacles; vertical illumination levels assist in identifying vertically oriented surfaces and assist in visual recognition of other personnel from a safe distance.
- Uniformity in the lighting system eliminates harsh shadows around buildings and surrounding areas; this makes the environment safer for pedestrians and drivers.
- Glare is excessive brightness coming from poorly designed or misapplied lighting fixtures or is reflected from glossy surfaces; glare should be minimized to maintain visibility of the area by personnel and video surveillance equipment.
- Horizontal and vertical lighting levels in parking lots and parking garages should be within limits recommended for visual identification. Lighting levels should be uniform with no dark areas around corners or vehicle parking slots where personnel may hide.
- Entrances to buildings should be illuminated at a higher level than the surrounding areas to increase safety and guide visitors into the facility.

12.12 Guards

12.12.1 Introduction

Security guards, also referred to as security officers, have the following basic functions when used for security of the data center:

- Patrol of perimeters, site, buildings, and areas
- Control vehicular and pedestrian traffic
- Escorts
- Inspection of shipments, packages, and visitors
- Other special duties

12.12.2 Recommendations

When present, security officers should monitor and control access through all perimeter openings.

Guards or security officers can be contract, employees, or a mixture of both.

All guards should be trained in the security plan and policy for the data center, building, or campus.

Guards should be utilized to identify, log, and monitor all nonemployees entering the facility, including vendors, contractors, and visitors.

Access to the facility, building, or data center should be granted only under conditions identified by the security plan or policy. Anyone not meeting those preset conditions should not be permitted into the facility until such time that those conditions are met.

12.13 Disaster Recovery Plan

12.13.1 Introduction

All data centers should have a detailed disaster recovery plan. The physical disaster recovery plan should be complimentary or integrated within the IT disaster recovery plan and the organization's business continuity plan (BCP).

12.13.2 Requirements

The data center disaster recovery plan shall deal with all phases of an emergency including:

- Planning
- Predisaster/incident activities
- The disaster/incident
- Response
- Recovery from the disaster/incident

The primary content, procedures, and all emergency lists shall be printed and posted as hard copies, with such postings being strictly maintained and current.

12.13.3 Recommendations

The data center should identify a disaster recovery manager (DRM) who is responsible for the coordination and implementation of the disaster recovery plan.

A detailed analysis of the impact of both long and short-term business interruptions should be conducted. The data center should evaluate the impact of total shutdown for up to 30 days.

Specific employees and contractors should participate in the creation and regular updating of the disaster recovery plan.

The planning for and classification of disasters should follow the guidelines outlined in NFPA 1600.

The disaster recovery plan should take into account the following types of major disasters:

- Aircraft crashes
- Chemical accidents
- Dust
- Earthquakes
- Epidemics
- Falling objects

<List continues on next page>

- Fire
- Electrical hazards
- Hurricanes
- Landslides
- Loss of utility services, including water, electric, and telecommunications
- Natural disasters
- Weather extremes

The disaster recovery plan should take into account the following types of criminal activity, which can have disastrous impact on the data center:

- Arson
- Blackmail
- Breaking and entering/burglary
- Bribery
- Collusion
- Conspiracy
- Disorderly conduct
- Embezzlement
- Extortion
- Fraud
- Kidnapping
- Looting
- Rape
- Riot
- Terrorism
- Theft
- Trespassing
- Vandalism
- White-collar crime

Data centers should regularly and routinely conduct disaster recovery tests.

The test should be evaluated and modifications made in the disaster recovery plan to address any issues.

Disaster recovery planning should include the creation of mutual aid agreements with other businesses or organizations.

Disaster recovery planning should include the identification of key employees or contractors necessary to restore operation to the data center during a disaster.

Backups should be identified in the event that the primary personnel identified are unable to respond.

Data center and security personnel should meet with appropriate federal, state, and local authorities that have control of surface roads and disaster zones and determine the forms of identification and authorization that will be required during a natural, technological, or human disaster.

Each employee or contractor designated as critical to restoring operation of the data center during a disaster should have some preapproved method of identification and authorization to enter disaster zones should the data center facility be classified as part of such.

Disaster plans should include the identification and listing of likely emergency routes.

Disaster plans should identify primary and secondary methods of communications between key personnel needed to restore operations to the data center.

Identified employees and contractors should have easy access to a contact list containing the names, addresses, telephone numbers, and other contact information for each primary and backup responder.

Because of the variable nature of the availability of communications during a disaster, multiple methods of communication should be available, including:

- Telephones
- Cellular phones
- Personal communication devices with electronic messaging capabilities (e.g., text, email)
- IP phones
- Pagers
- Land mobile radios
- Citizens band (CB) radios

Disaster recovery plans should include detailed plans for all aspects of emergency operation of the data center, including:

- Access/egress badges, keys, cards for all areas, including those normally off limits
- Access control plans for nonemergency personnel
- Operational checklists with detailed documentation and instructions on operation of equipment with which the emergency responder may not be familiar
- Facility shutdown procedures
- Emergency security procedures
- The location of all emergency equipment
- The use of fire and emergency equipment

12.14 Building Site Considerations

12.14.1 Introduction

The purpose of building site security is to prevent unauthorized entry or exit by employees and others to determine likely human, man-made, and natural threats and implement countermeasures. Site security also involves the control of pedestrian and vehicular traffic and should ensure that employees, visitors, contractors, and other pedestrians and vehicles can be monitored and inspected as needed.

12.14.2 General Recommendations

All exterior building openings larger than 62,000 mm² (96 in²) should be covered with a security grill using an approved wire fabric and tool resistant 13 mm (0.5 in) steel bars spaced no less than 200 mm (8 in) on center.

All security devices should be installed using security fasteners. Security fasteners eliminate the risk of easy removal and include:

- One-way screws
- Bolts
- Non-removable pins
- Setscrews
- Spot welds

Door hinges that mount to the exterior of the door should have non-removable pins, fixed pins, or center pivots.

Burglar-resistant window/door glazing shall meet the following minimum requirements:

- Total thickness of glass laminate shall be 6 mm (0.25 in) plus 60 mil vinyl film “sandwiched” between the glass.
- Glass shall be tempered, tested, and certified to ASTM Class III of F1233 or UL 972.
- If the window is insulated, the laminated assembly shall be on the exterior of the window.
- Bullet-resistant or blast-resistant glazing is recommended in high crime areas or for buildings near parking areas and roadways.

Bullet-resistant material should at a minimum meet UL super small arms (SSA) threat level using UL 972 test methods.

All exterior doors should have a lock with a deadbolt or equal locking capability.

Mortise locks used for security must adhere to BHMA A156.13 standards and must have a deadbolt throw of 25 mm (1 in) minimum.

12.14.3 Lighting

Lighting is one of the primary considerations for providing the security of occupants and assets in the data center. The following types of lighting should be considered for security use based upon their respective properties, life cycle, environmental conditions, and impact on other security systems (e.g., VSS):

- Incandescent
- Gaseous discharge (mercury/sodium vapor)
- Quartz
- Light emitting diode (LED)

Security or protective lighting should consider one of the four following types:

- Continuous
- Emergency
- Movable
- Standby

Basic security lighting should be provided to protect the safety of pedestrians, vehicles, and assets, as well as preventing concealment for unauthorized access to the data center site or buildings. Lighting should be provided at the following areas (at a minimum):

- Perimeter fencing
- Building perimeter
- All entrance gates—pedestrian and vehicular
- All building entrances and exits
- Vestibules and lobbies
- Gatehouses/guardhouses
- Windows and exterior openings when the risk of unauthorized access through them is determined
- All pedestrian walkways and public areas
- Stairwells.

Lighting should meet the minimum levels of intensity, measured in foot-candles, as listed in Table 12-6.

12.14.4 Perimeter Fencing and Barriers

Perimeter fencing, because of threats from local crime, breaking and entering, workplace violence, or other concerns, should include the following design guidelines:

- Fencing should be placed along property lines.
- When employee parking is separate from general parking, fencing or barriers should be used.
- Fencing should be placed along street frontage in high crime areas.
- Fencing should be placed along abutting buildings because of local crime concerns.

Perimeter fencing and gates for the data center should be constructed using the following minimum design requirements:

- Constructed of a 2.9 mm (9-gauge) steel wire with 50 mm (2 in) mesh chain link (minimum)
- For aesthetic purposes, vinyl cladding is acceptable
- 2.4 m (8 ft) high with no top guard
- 2.1 m (7 ft) high with top guard (fence height only)
- Installed in a straight line at ground level, no more than 50 mm (2 in) from the pavement, hard ground or concrete
- Ties fastening the fence fabric to the posts and rails should be 2.3 mm (11-gauge) steel or screw type fasteners

The top guard should face outward and upward and be constructed at a 45° angle. The top guard should only increase the height of the fence by 300 mm (12 in) but should have three strands of double-twisted, four-point barbed wire mounted 150 mm (6 in) equidistant apart.

Table 12-6 Minimum Lighting Levels

<i>Area</i>	<i>Minimum Lighting lx (fc)</i>
Outer perimeter	1.5 lx (0.15 fc)
Inner perimeter	4 lx (0.4 fc)
Base of perimeter fence	10 lx (1.0 fc)
Vehicular entrances	10 lx (1.0 fc)
Pedestrian entrances	20 lx (2.0 fc)
Restricted structures	20 lx (2.0 fc)
Clear zones	2 lx (0.2 fc)
Parking areas	10 lx (1.0 fc)

When fencing is adjacent to vehicular traffic lanes or parking areas, it should be protected by wheel stops, curbs, bollards, or guardrails as required.

When possible, clear zones should be established on either side of the fencing. The planting of even low shrubbery or plantings should be avoided if possible, but at a minimum should be placed no closer to the fence than 0.6 to 0.9 m (2 or 3 ft). Trees or other plantings should never provide points of concealment or assist in unauthorized access to the facility or site.

Signage should be placed on the fence warning of restricted or limited access. All security signage should be placed at 30 m (100 ft) intervals and 1.5 m (5 ft) above the ground.

The following special areas are known to cause breaches of the perimeter and will increase the risk of unauthorized entry:

- Sidewalk elevators
- Utility tunnels
- Storm sewers
- Piers, docks, and wharves

12.14.5 Automotive Threats and Concerns

Because of concerns over vehicle bombs, the following recommendations should be followed when designing parking areas and site traffic control:

- Maintain a minimum perimeter of 30 m (100 ft) from the building.
- Utilize concrete barriers at the curb.
- When possible, have all cars park at a distance from the building.
- Reduce or eliminate underground parking immediately under the data center building.

If possible, data centers should not be located in buildings adjacent to mid or high-rise parking garages.

If possible, elevators should never go directly from the parking garage to office space. Elevators should open and discharge into the lobby.

Parking garages should contain emergency phones or intercoms spaced no less than every 18 m (60 ft). Each telephone or intercom should be clearly marked as such and should be illuminated with blue or some other locally accepted color associated with police or security.

Any onsite parking facility should address the security of pedestrian and vehicular traffic. Surveillance is crucial for security in parking garages and is capable of providing adequate coverage. Key considerations in protecting property and safety include the placement of cameras in the following locations:

- Entrance and all exits
- Guard and cashier booths
- Elevator lobbies and elevators
- Ramps, driveways, and emergency call stations

The following is a list of potential threats that should be considered when assessing the risk of parking areas within or adjacent to data center buildings:

- Assault
- Carbon monoxide
- Chemical, biological, radiological, nuclear, or explosive incidents
- Explosion
- Fire
- Medical emergencies
- Robbery
- Terrorism
- Theft

12.14.6 Threat History

Historical information should be gathered during the planning for any security system design whether new or retrofitted into an existing data center. Typical information gathered during this investigation would include:

- Within the past 5 years, has anyone been successful at this location in damaging any part of the data center facility?
- What is the frequency of natural disasters for the data center site? What types of natural disasters have occurred and how often?
- Have any natural, technological, or human disasters rendered the data center or any business inoperable within the last 5 years? Ever?
- What is the frequency of the following within a 1.6 km (1 mi) radius of the data center facility
 - Assault?
 - Armed robbery?
 - Auto theft?
 - Burglary?
 - Drug trafficking?
 - Fires?
 - Floods?
 - Hurricane/tornado/cyclone?
 - Kidnapping?
 - Murder?
 - Terrorism?
 - Riot?
 - Vandalism?
 - Workplace violence?

The most common threats to all personnel should be identified, and training should be conducted to address these risks.

Employees should be trained to ensure that they act appropriately in high-risk situations such as workplace violence, sabotage, kidnapping, natural disasters, and robbery.

12.14.7 Natural Threats and Concerns

If possible, the data center should not be located within 80 km (50 mi) of an active volcano, earthquake fault line, or high erosion area.

The data center should not be located in any area where there is a substantial risk of flooding from dams, oceans, lakes, or other bodies of water.

The data center should not be located on a flood plain.

The data center should not be located below grade.

See Section 5 for other factors regarding the location and site selection of the data center.

12.14.8 Chemical, Biological, Radiological, Nuclear, and Explosives

Preparation for potential CBRNE threats should be conducted by security and operations personnel for each data center. Each data center should:

- Include CBRNE threat response in the security plan
- Classify threats and the appropriate response
- Include coordination with local EMS and law enforcement
- Include the CBRNE response in the disaster recovery/business continuity planning process

Nuclear power plants should be at least 80 km (50 mi) away.

The data center site should not be located within a 13 km (8 mi) radius of defense contractors or installations, government laboratories, or military facilities.

Explosions, whether accidental or because of sabotage, workplace violence, or terrorism should be considered as a threat to the data center building and computer room. The risks associated with explosions or bombs include:

- Injury or death of occupants
- Structural damage to the building
- Damage to the equipment and contents of the building
- Interruption of operations (downtime)

12.14.9 Medical Disasters and Epidemics

The data center should have personnel trained in first aid and cardiopulmonary resuscitation on duty anytime the data center site or buildings are occupied.

First aid supplies should be located in places and marked for easy identification and quick access in the event of an emergency.

First aid supplies should include automatic defibrillator(s) in a quantity recommended by the manufacturer to serve the number of occupants and buildings.

12.15 Building Shell

12.15.1 General Recommendations

The data center should have an evacuation plan, including procedures on notifying all building occupants and posted evacuation routes.

Public tours should not be conducted in areas where sensitive computer operations are active, personal or sensitive data is visible, or high-value items are stored. If public tours of the data center and computer room are conducted, cameras and camera phones should be prohibited.

All areas through which data passes (e.g., entrance rooms, TRs, media storage rooms, computer rooms) should have some level of access control installed.

High-value computer, satellite, network equipment, and other hardware/software should be stored in rooms with EAC to ensure that only authorized personnel enter and to provide a tracking log in the event of loss.

Media storage, waste disposal, and chemical storage should be separated from computer, network, and telecommunications equipment.

All service personnel, including janitorial, technical, and construction contractors, should be prescreened by security. Unscreened substitutes should be denied access to the site/building/data center.

12.15.2 Doorways And Windows

Skylights, light monitors, atriums, open courts, light courts, windows, or any other openings that penetrate the security of the roof should be approved by the security designer, including appropriate countermeasures to provide security appropriate with the area or room.

All heating, ventilation, and air conditioning openings larger than 5100 mm² (8 in²) should have some form of barrier installed to prevent unauthorized entry into the building. This recommendation also applies to any other utility openings that penetrate the roof or walls.

Doors located in lobby areas must have glazing that conforms to local building codes. View panes and glass doors must consist of burglar-resistant glass.

All exterior doors should be at least 1.3 mm (16 gauge) steel-reinforced solid core.

Roof hatches should be manufactured from a minimum of 1.3 mm (16 gauge) steel and should lock from the inside only.

When ladders for the rooftop are mounted on the building exterior, a security ladder cover should protect the first 3 m (10 ft) of the ladder.

All permanent roof access should be from the interior of the building.

Doors leading to the roof should meet the security requirements for exterior doors, including double-cylinder deadbolt locks.

Windows should not be placed in the computer room, storage areas, equipment rooms, restrooms, locker, or utility rooms. If windows are necessary or preexisting, the windowsill must be at least 2.4 m (8 ft) above finished floor or any other surface that might provide access.

Window frames should be constructed with rigid sash material that is anchored on the inside and is resistant to being pried open.

The doors to all utility rooms, entrance rooms, TRs, and computer rooms should be locked at all times when not in use. Doors to these rooms should be equipped with door position sensors that trigger an alert if the door is propped or held open for more than 30 seconds.

12.15.3 Signage and Displays

All closed, limited-access, restricted, and secured areas should be designated by the use of prominent signage.

Computer rooms, secure areas, and sensitive areas should not be located on all publicly accessible directories, signs, and maps.

12.15.4 Construction

When the data center is being planned for an existing structure, the security survey should include a structural analysis of the floors, ceilings, and walls to determine the estimated time needed to penetrate them.

Added intrusion alarm and surveillance systems should be designed when the resistance to penetration of any exterior or interior ceiling, wall, or floor is identified as a risk. This includes open plenum areas above dropped ceilings that extend over controlled areas or are separated only by drywall.

Exterior building doors should be constructed of solid metal, wood, mesh-reinforced glass, or covered with a rated metal screen.

When possible, there should be no external windows or doors leading into the computer room.

12.15.5 Elevators

Elevators opening to secure areas should have one or more electronic access control systems to ensure proper identification and authentication of passengers that visit the selected floor.

If possible, separate elevators should be designed to serve secured or sensitive areas.

12.15.6 Emergency Exits

Emergency exits should be configured so that they are only capable of being operated from the inside.

Planners should consider installing automatic door closers and removing door handles from the outside of the emergency exit doors, discouraging use of the door to reenter the facility.

12.15.7 Utilities

All utility feeds should be located underground. If utilities must enter the data center above ground, they must do so at the highest possible distance above ground and must be enclosed in a conduit until safely inside the building shell.

12.15.8 Hazardous Material Storage

Caustic or flammable clean fluids should always be stored in closets or rooms designated for that purpose. They should never be stored in entrance rooms, computer rooms, media storage rooms, TRs, or other locations where telecommunications, network, or computer equipment is installed or stored.

Cleaning fluids and all other caustic or flammable liquids should always be stored in approved containers and in as small of quantities as possible.

12.16 Data Center Security Design Recommendations

12.16.1 Site, Personnel, and Non-Critical Areas

12.16.1.1 Site

Prominently displayed signage, bearing language such as “Restricted Area” or “Controlled Area”, should be posted at every access point into the data center.

If the data center occupies an entire campus, the warning should be posted at every vehicle entry point and at regular intervals along the perimeter fencing or other barrier. However, the “tombstone” or other notifications shall not indicate the presence of a data center.

If security officers are assigned to monitor or patrol the data center areas, the frequency of patrol should be specified in the security plan or policy, and manual or electronic methods should be implemented that ensure the required frequency of patrols.

User access should be carefully monitored and controlled when any of the following circumstances apply:

- New hires
- Employees under any significant or extended disciplinary procedure or probation
- Employees who have been flagged because of unusual patterns of behavior or work hours

12.16.1.2 Office Area Security

Data center management should periodically conduct a live site survey with the goal of identifying vulnerabilities in employee behavior, office and cubicle design, and placement as well as insufficient locks, doors, access control, alarms, and other countermeasures. If the data center does not have a security officer or department, the site survey should be conducted by a qualified outside security consultant or agency.

Employees should lock offices, desks, and file cabinets at all times when not in use.

Sensitive, confidential, or operational information should not be left on desks or in the open when not in use.

Mail should not be left for longer than one business day in open trays or boxes.

All planning charts, white boards, and easels should be erased immediately after use.

Presentations, photographs, and other documents should be marked as such if they are sensitive or confidential.

Any proprietary or confidential information leaks should be investigated and the appropriate modifications made to the security plan, including policy, procedure, and training.

If a crime has been committed, the appropriate federal, state, or local law enforcement agency should be immediately notified.

The monitors and terminal displays for data center employees displaying sensitive or confidential information should be oriented in such a way as to not reveal the information to visitors or pedestrian traffic, commonly referred to as “shoulder surfing”.

12.16.1.3 Screening for Weapons and Contraband

When determined necessary by site conditions, threats, or other business indicators, screening for weapons, explosives, and other contraband should be conducted for all personnel entering the data center.

Screening procedures should be included in the security plan.

Screening procedures may include the use of metal detectors, x-ray machines, explosive detectors, vapor detectors, particle detectors, and canines.

12.16.1.4 Disposal Of Media and Printed Material

All confidential and proprietary information should be disposed of as dictated by data center policy and procedure.

Media and printed material should be stored in secure containers prior to its destruction.

The pickup of confidential material for destruction should be supervised and logged. If the material is destroyed onsite, the process should be constantly supervised.

The disposal of confidential materials should be coordinated with the disaster recovery plan so that confidential material is protected even during a disaster.

12.16.1.5 Human Factor

All employees should sign a confidentiality agreement when first hired.

Any abnormal or suspicious behavior on the part of employees or contractors should be reported to facility security or data center management. Reportable activity would include:

- Illegal use of or attempts to access restricted files
- Misuse of computer-related resources, including software and hardware
- Unauthorized destruction of any property
- Unauthorized loading of software or other information
- Examining waste receptacles for sensitive information
- Presence in an unauthorized area or room

There should be a periodic review of all keys, codes, magnetic cards, badges, and the personnel who have them to ensure that current employees and contractors possessing keys, cards, codes, badges, and tokens still have a confirmed need to enter the computer room.

Human resources termination procedures should include a termination checklist that must be completed and require that all items returned before the employee receives their final paycheck and departing benefits. The checklist should include:

- The return of:
 - Parking passes, badges, and cards (including those mounted on vehicles)
 - Company identification badges
 - All access cards, magnetic cards, proximity cards
 - All keys
 - All company/organization-owned equipment, including computers, phones, radios, test equipment, and tools
- Cipher locks and combination locks codes immediately changed or if permanently coded, new locks installed
- Voicemail passwords changed or deleted
- PBX, computer, network, VPN, and any other passwords changed or the user account deleted
- Computer, network, and telephone equipment returned
- Sensitive or proprietary information returned
- Data center-owned software returned
- Data center-owned property returned, including hardware, vehicles, uniforms, or any other real property
- Business memberships, calling cards, and credit cards should be surrendered and cancelled
- Business bills, such as expense reports, should be reconciled

12.16.1.6 Theft

The data center should have a detailed asset log or database in which all computer, network, and telecommunications equipment is tracked, including removable media.

The use of an electronic asset program (EAP) is encouraged.

EAP tags should be affixed to all computers, network equipment, telecommunications equipment, and removable media such as magnetic and other media.

Sensors should be located at the entry/exit points for all locations where high-value or sensitive items are stored.

The EAP system should be integrated with the facility VSS, access control, and alarm systems so that entry/exit events can be recorded and suspicious events acted upon and a time-stamped video of an event can be saved for investigative purposes.

Unique identification numbers should be permanently affixed, etched, or stamped on all computer, network, and telecommunications equipment.

In high-risk areas or situations, personal computers, laptops and other computer and network equipment should be permanently fastened to some part of the building or piece of furniture.

12.16.2 Computer Room and Critical Facility Areas Special Considerations

12.16.2.1 General

The security plan should contain special considerations for computer rooms and critical facility areas.

All computer rooms and other areas deemed mission critical, inside and outside the building itself, to the operation of the data center should be considered restricted areas.

All security personnel should be made aware of the location of these areas.

All sides of a computer room, including ceiling and underfloor when those areas represent possible points of entry, should be protected by intrusion alarms and surveillance.

Electronic access control (EAC) shall be installed to track and control all ingress and egress to computer rooms and all critical areas.

The use of access control, surveillance, and alarms should be deployed as detailed in the policies and procedures outlined of the security plan to protect all computer rooms and critical facilities. Typical countermeasures deployed to protect these areas include:

- Access control devices, including locks and barriers
- CBRNE detection and protection
- Guard patrols
- Intrusion alarms
- Man traps
- Sensor driven alarms, including fire, smoke, water, and temperature
- Signage
- Surveillance

In a “lights out” data center or when employees and security personnel are not on site 24/7, the intrusion alarms should be monitored by at least one central station such as the corporate NOC or security centers.

Access to the computer room shall be controlled at all times.

All data center and computer room main and backup power supplies, entrance rooms, TRs, and other mission-critical utilities should be located in secure areas with periodic inspections for sabotage.

Badging policy should be strictly enforced in the computer room. If an employee loses or forgets a badge, he or shee should be required to wear a visitor badge, complying with any visitor escort policy(s) until such time that the badge is replaced or found.

The ability to authorize access in to the computer room should be limited to as few personnel as possible.

Computer room doors should remain closed and locked at all times. When possible, the door(s) should be alarmed to prevent propping open the computer room door.

All visitors and contractors should be required to sign an entry/exit log prior to entering the computer room, even when they are escorted.

Employees should be trained and encouraged to challenge unknown individuals found in the computer room.

Data centers should consider implementing the two-man rule for the computer room and other areas containing high value or sensitive contents.

All after-hour entry/exit into the computer room should be tracked and reviewed by data center security or management personnel.

All removable recording media should be secured when not in use to reduce the likelihood of theft or damage.

Critical information storage areas, such as tape vaults, should be prohibited for use as a work area.

It is a good practice to inspect all containers (including lunch boxes and briefcases) that leave the computer room, high-value, and sensitive areas. This helps prevent the unauthorized removal of proprietary information and storage media.

Authorized data center personnel should be required to remain with all hardware, software, and integration vendors while installation, maintenance, or upgrades are being performed.

Unless job functions requires it, programming or coding personnel should not automatically be granted access to the computer room.

12.16.2.2 Construction

If possible, the computer room and data center support areas should be located on floors above grade and in a multistory structure above the level known to be at risk for flood.

When possible, computer rooms should be physically separated from less secure areas. These areas should be marked as “restricted” or “controlled areas” consistent with signage policy.

Data centers located within multi-storied buildings that have multiple tenants should have structural and security studies performed with the resulting recommendations implemented to reduce the risk of damage to data center equipment from portable explosives detonated above or below the data center ITE or critical facilities systems.

Computer rooms should always contain a drainage system with a capacity large enough to handle potential leakage from sprinklers, chilled water pipes, and any potable water pipes that pass through or adjacent to the computer room.

Computer room floor drains should always be fitted with back-flow valves.

The computer area roof should be constructed to drain or guide water away from the computer room.

The data center should have a supply of waterproof sheets or covers available to adequately cover all hardware, equipment, and supplies.

An industrial wet/dry vacuum cleaner should be kept close to the computer room in the event of a water leak. Vacuum cleaners used in the computer room should be micro filtered with a minimum 99.8% HEPA filter to prevent particles from being released back into the data center. Allowed particulate size may be predetermined thus the vacuum cleaner used should correspond to this determination.

12.16.2.3 Eavesdropping

Computer rooms handling highly sensitive or valuable data should consider the installation of electronic field emanation reduction features (Tempest) to prevent electronic eavesdropping of data processing activities.

When highly sensitive or valuable data is present, the computer room and any data center area processing this data should be periodically checked for electronic eavesdropping devices.

12.16.2.4 Media

The computer room should contain a certified fireproof magnetic media cabinet/safe for the storage of critical documents and removable media.

The marking, handling, storing, destroying, or using of storage media should be limited to specific authorized employees or contractors.

12.16.2.5 Fire Prevention

Computer rooms should not have any trash receptacles. All unpacking should occur outside the computer room, and any trash in the computer room should be promptly removed.

Caustic or flammable cleaning fluids shall not be stored in the computer room.

12.16.2.6 Dust

Paper shredding, paper bursting, and report separation equipment should always be located outside of the computer room.

Paper products and supplies should always be stored outside of the computer room.

If paper products are required to be stored in the computer room, then the supply should be limited to no more than one day's worth.

This page intentionally left blank

13 Data Center Management and Building Systems

13.1 Data Center Infrastructure Management

13.1.1 Introduction

Data center infrastructure management (DCIM) is a software application or a suite of software applications that are configured to gather, monitor, and aggregate data from multiple sub systems within a facility. In its true sense, DCIM is not a management tool because it does not directly control data center devices and components. It is used as a data collection and reporting tool. The result of the aggregated data is utilized for automated or manual adjustments to physical infrastructure in order to increase efficiency, provide fault tolerance, provide workflow management, and implement changes resulting from expansion or consolidation of the facility. DCIM can source data from directly connected components such as electrical components (e.g., UPS, PDUs, RPPs) or environmental (e.g., CRACs, CRAHs, temperature probes, humidity probes, wireless environmental reporting devices). Automated adjustments are performed by subsystems, such as a building automation system (BAS) or building management system (BMS), and are initiated by those systems.

DCIM can also source and share data with other facility systems such as BAS, BMS, and EPMS. Each of the human machine interfaces (HMIs) within the other facility systems can also utilize the aggregated data collected by DCIM in order to determine facility based adjustments to be made by the BAS and BMS.

The DCIM suite of applications can be both localized and cloud based, depending upon the specific application service. This allows great flexibility as well as functionality by users from varying business groups within an organization. For instance, a data center manager would typically use a localized application in order to assess effects of changes within the environment when considering the purchase of new IT hardware. A facility manager might want to establish an energy cost reduction policy. Through the monitoring and assessment combined of power and cooling attributes within the data center via the DCIM, adjustments can be made via the BMS to control these items more effectively and efficiently. An energy procurement manager would use a cloud-based application in order to assess energy cost projections across their organization's fleet of data centers. These projections might be based upon stored utilization data that can establish trend metrics in order to forecast future usage.

13.1.2 Components

13.1.2.1 Appliances

The DCIM may include:

- A centralized server or virtual appliance
- Client console or web client
- HTTP or HTTPS connection to access the end-user interface
- Standard TCP protocol connections for end-user notifications

Figure 13-1 shows an example of DCIM architecture. The DCIM architecture should permit managing devices on either the company/organization network or a separate dedicated network. The DCIM should also allow management devices that can reside on both the public LAN and the private LAN. Management and monitoring functions may be implemented as either firmware or software configuration within the appliances. Other more complex functions such as workflow management, change management, and analytics, may be performed either by servers within the data center or in the cloud on a server in a service provider's data center. The application requirements should include end user scalability, allowing for future expansion and enhancements.

13.1.2.2 Subsystems

DCIM can provide reporting and establish metrics for decision making through information acquired from components that are directly connected to the network, or from facility subsystems that have a primary purpose to control building functions. When referring to direct connected components, it is assumed that these components reside on the same network as the DCIM tool without any need for media or protocol conversion. These components might consist of SNMP-enabled power and cooling devices that are located within a data center. However, to obtain the required information to make good decisions, operational data may need to be gathered from devices that are not connected to the LAN or are outside of the building. These devices might consist of power substations and electrical switchgear that are monitored by an EPMS with a protocol such as Modbus. They may also include chillers, cooling towers, and pumps that are managed by a BAS/BMS with a protocol such as BACnet. They may also consist of equipment with no LAN connections that are monitored using a proprietary protocol.

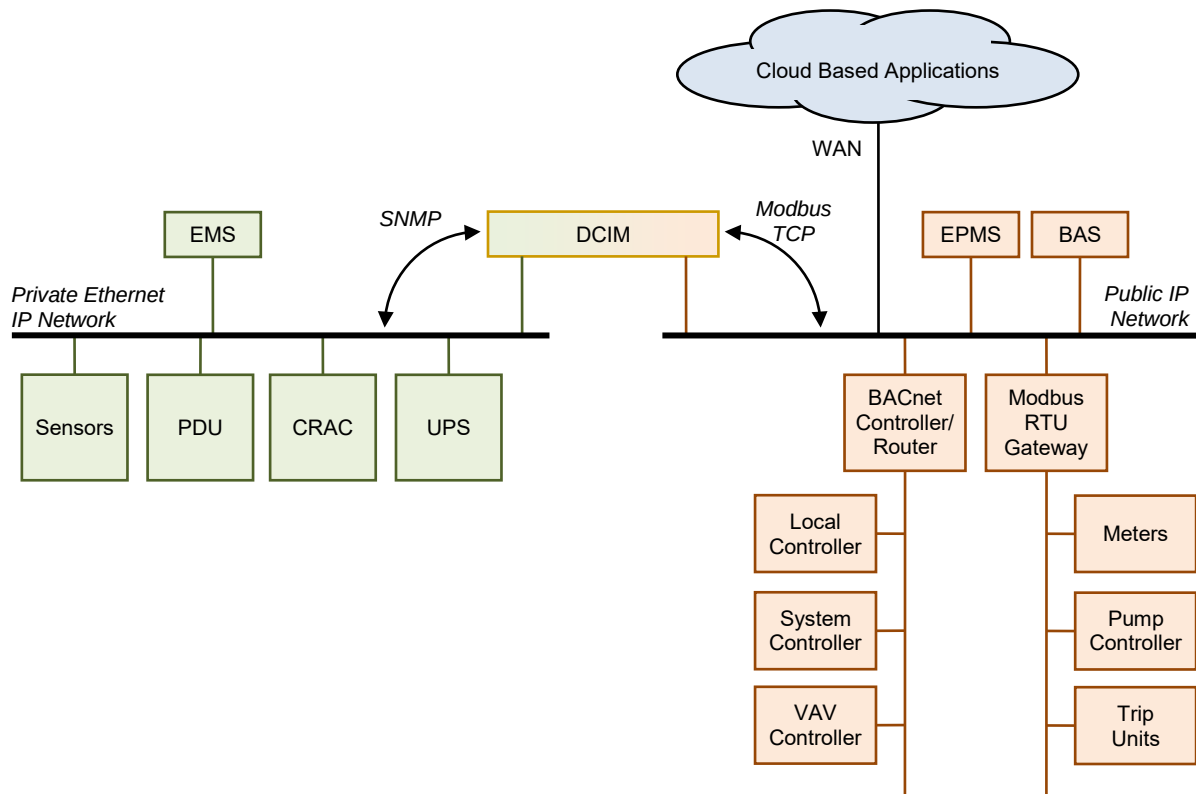


Figure 13-1
Example DCIM Architecture

13.1.2.3 Modules

In base form, DCIM may consist of a base application for providing a unified view of critical components and their operation. It can also be configured for specific environments through the use of add-on software modules. Specific purpose modules may be geared to healthcare, colocation, financial, educational, industrial, and other vertical markets. In addition to the specific purpose modules, add-ons for workflow management, capacity management, planning, and asset tracking can be incorporated into the DCIM suite.

13.1.2.4 Building Automation Subsystem

A BAS is a control system comprised of hardware (e.g., controllers, cabling, input/output devices) and a software application or suite of software applications that automate the electrical and mechanical subsystems. A BAS may integrate with another BAS of a different system to coordinate their operation in a productive and efficient manner or may be managed by a BMS. A BAS may communicate with BMS subsets, allowing for automated operational changes in order to achieve the goal of an established parameter or set of parameters.

13.1.2.5 Building Management Subsystem

A BMS is a management system that monitors, with the integration of one or more BAS, facility functions such as airflow, temperature, and water flow. A BMS may also provide the control functionality of the individual BAS systems. Although these functions are automated through their specific BAS, the BMS can be used to make adjustments. Adjustments through a BMS are typically performed manually through a HMI.

13.1.2.6 Energy Management Subsystem

An energy management system (EMS) is basically a BAS; however, it has evolved with a focus not only on the coordination and intercommunication of various subsystems for the purpose of system control, but it also has a main focus on how to obtain the maximum efficiency at all times based upon real time data. An EMS will control systems, but it typically does not make changes or adjustments for increased efficiency based upon the data that is being shared.

13.1.2.7 Electrical Power Management Subsystem

An electrical power management system (EPMS) is designed to monitor and report power quality, power utilization, peak demand, and peak forecasting. The EPMS incorporates a power monitoring strategy to capture specific, pre-established parameters at the time of an electrical disturbance, including a waveform at a specific point in time. The disturbance is time stamped and stored locally on a metering device, but it is periodically or continuously uploaded to a software package that is specific to the EPMS subset. This software package will share data with the DCIM in order to help make evaluations or corrections to the electrical system based upon risk, mission criticality, and cost.

13.1.2.8 Enterprise Management Subsystem

DCIM can incorporate plug-ins that support network, operational, and enterprise systems. These systems can provide measurements, such as processor load versus electrical load, that can be beneficial in determining optimal operations such as if server hardware is providing optimal value for its energy consumption. Alarm thresholds can be set not only for events such as utilization or security violations, but also for thermal events, redundancy breaches, power availability, and other physical conditions. Alarms and notification are typically communicated to the DCIM via a summary alarm; alarms (e.g., power or cooling failure) may also be independently communicated as specified by owner or operational requirements.

13.1.3 Communication Protocols, Media and Hardware

Protocols are not limited for DCIM, but most systems use TCP/IP. Subsystems may also incorporate standardized automation control protocols, (e.g., ISO 16484-5 [BACnet], ISO/IEC 14908-1 [LONTalk]), open use protocols (e.g., Modbus), or proprietary protocols specific to the system or manufacturer. LAN hardware and associated media is needed to provide an Ethernet gateway for communication between the DCIM and the subsystems as well as providing the communication link between the DCIM and the remote client accessing it. The components needed may include switches, routers, hubs, telecommunications standards-compliant balanced twisted pair cable, optical fiber media, IP addresses, firewalls, and client workstations/servers although other components may be required for a particular solution.

DCIM servers access managed devices and are managed by client workstations using LAN connections. The virtual DCIM appliance is delivered as an open virtualization archive (OVA) and is supported on VMware. The virtual appliance is expected to function properly on any virtualization platform that supports the OVA format or has an appropriate converter utility. The virtual appliance shall be fault tolerant utilizing a 1 CPU configuration only, which eliminates dependencies upon multiple physical machines.

13.1.4 Reporting

Reporting metrics, such as PUE and DCIE, are totally dependent upon the collection, aggregation, and processing of lower level sub systems, devices, and sensors. If the DCIM is unable to obtain information from all sub-systems, devices, and sensors, the PUE and DCIE measurement can never be correct. Although real time reporting is most accurate at a given point in time, the need for continuous monitoring can be reduced if the DCIM can effectively calculate, model, and simulate effects of changes in the environment. Therefore, the communication polling frequency can be reduced, thus taxing the network to a lesser degree and the amount of metering devices can be reduced. In this respect, a more capable DCIM can provide an advantage to a retrofit facility with limited network and metering capabilities. DCIM plug-ins and add on modules can communicate with Enterprise Management Systems to collect operational data from active hardware such as servers, switches, and storage devices. This data can be used along with data from facility subsystems to calculate IT dependencies on power, cooling, and space allocation at the rack and device level. Manual entries are also accommodated in order to create simulations or “what if” scenarios for planning IT upgrades, moves, adds, and changes.

13.1.5 Recommendations and Conclusion

DCIM should consist of an open communication architecture. This architecture exhibits the distinct ability to interface with any third party software or device over standard IP and industrial communication protocols. Alerts are required for critical threshold breaches as well as trending in order to forecast potential risk. Finally, DCIM should be scalable, enabling the user to monitor conditions on directly connected devices within a small data center or indirectly connected devices through subsystems within an enterprise environment. DCIM should have the ability to perform calculations based upon aggregated data from a proportionate number of devices and meters, but exhibiting the ability to make assumptions based upon whether the number of devices and meters are lesser or greater.

13.2 Building Automation Systems

13.2.1 Introduction

A building automation system (BAS) can be defined as an assemblage of products designed for the control, monitoring, and optimization of various functions and services provided for the operation of a building. Building systems typically include lighting, heating/ventilation/air conditioning (HVAC) systems, power, security, telecommunications services, and life safety systems. Building automation's basic control technologies have been in existence for some time. The term *intelligent building* is used as a synonym for facilities using advanced BAS technology. BAS hardware is typically represented by one or more control and processing units and by a number of peripheral devices that control the operation of building systems. The control unit, based on the information supplied by the peripheral devices as well as preset instructions, runs the system. The control unit can be as simple as a relay or timer to control a water heater on/off switch or as sophisticated as a microprocessor operating on fuzzy logic. The cabling linking the control unit to the peripheral units can be telecommunication standards-compliant balanced twisted pair, optical fiber, coaxial, low-voltage, or even power cables.

A BMS enables an operator or building engineer to monitor some or all of the systems and equipment that manage the building environment. BMSs typically do not include the control and optimization functions of a BAS.

For the purposes of this standard, automated controls will be defined as a system that provides monitoring and control of a mechanical, electrical, or electronic system designed for a specific process or operation such as automatic door openers, conveyor systems, or manufacturing machinery. Automated controls are not included in this standard.

Structured cabling provides several benefits to BAS, including systems that use IP protocols and those that do not. A standards-compliant structured cabling system provides a generic cabling system that can transport a wide range of protocols used for BAS, including Ethernet, ARCnet, and TIA/EIA-485-A, allowing the BAS to evolve without changing cabling. A generic, standards-compliant, structured cabling system is also designed to support a wide variety of other applications, such as voice, LANs, and video, allowing the installed cabling to be efficiently utilized and allowing new services to be deployed without running new cable. A structured cabling system is also easier to administer and troubleshoot than an unstructured cabling system. The disadvantage of structured cabling is that some proprietary or legacy BAS equipment may not function properly on standard-compliant structured cabling, thus requiring the installation of two parallel networks, which should be segregated to minimize maintenance errors.

NOTE: For additional details on applicable to a BAS, refer to BICSI 005 and TIA-862-A. For data center communications cabling refer to Section 14, ISO/IEC 24764, CENELEC EN 50173-5, and TIA-942-A.

13.2.2 Components

13.2.2.1 Cabling

13.2.2.1.1 Recommendations

Use standard structured cabling to support BAS as it provides the greatest flexibility in choice of a BAS system protocol.

13.2.2.1.2 Additional Information

Typically, BAS and BMS systems will require dedicated interconnect wiring between the mechanical systems of a building, such as boilers, chillers, chiller control systems, plumbing systems, water treatment, expansion tanks, and unit heaters and the peripheral devices that provide the most immediate level of system monitoring and control. In most modern systems, this level of cabling is the most likely to require proprietary or nonstandard communications cabling. Because of the inherent limitations this type of cabling may have, these peripheral devices should be located within close physical proximity to the mechanical systems to which they are connected.

Most BAS and BMS systems can then utilize structured cabling infrastructure, including cabling pathways and telecommunications spaces, which can provide network connectivity between the peripheral devices and a central control unit. The cabling infrastructure can also be used for connection to the operator interface (workstation).

13.2.2.2 Hardware

13.2.2.2.1 Introduction

A BAS system includes the following components:

- Input/output devices—these provide control for a single function such as a pressure meter, damper, or valve actuator
- Unitary controllers—these provide limited control functions for a single mechanical system such as an AHU, boiler, or water pump
- Distributed processors—these provide control functions for one or more unitary controllers or complex mechanical systems such as chilled water systems
- Head end—this controls one or more distributed processors, and can include a connection for a laptop computer, one or more installed workstations, and servers that provide database functions; the head end can be used to provide real-time control, programming, and historical data that can be used to display trends under multiple environmental conditions. These trends can be used to provide ways to run a facility more efficiently.

13.2.2.2.2 Requirements

All hardware shall be fault tolerant, that is failing to a condition that maintains the systems in a stable operating condition. This may be in the open, closed, on, or off position depending on the specific system configuration. The amount of hardware redundancy of equipment shall be determined by the Class of the system that the BAS is supporting.

13.2.2.3 Communications

13.2.2.3.1 Requirements

BMS/BAS systems shall conform to an open architecture specification for interfaces to the equipment and systems to be monitored and support SNMP to report status to other management systems.

Monitoring of BMS/BAS alarms shall be available in the data center's operations center or a similar location wherever the network is being monitored.

13.2.2.3.2 Recommendations

Many mechanical and electrical systems manufacturers are using open protocols for BAS connections such as BACnet, LONTalk, SNMP, and HTTP. Each protocol has advantages and disadvantages, and each data center owner/operator will use different criteria to choose which system to use. Typically, however, control and head end systems can be designed to communicate with mechanical systems using any of these open protocols.

The building automation should interface with the data center central power and environmental monitoring and control system (PEMCS). The PEMCS should include a remote engineering console and manual overrides for all automatic controls and set points.

13.2.2.3.3 Additional Information

Proprietary communications are becoming less common, but they may still be an issue in an existing facility with an older BAS system. Where newer BAS systems may be added in such a facility, gateways can possibly be used to translate a proprietary protocol to a modern open protocol.

BASs that perform systems integration can communicate with mechanical systems and associated controllers supplied by different manufacturers, even if the BAS, mechanical systems, and controllers are installed at different times. The use of open protocols is essential to the success of systems integration.

13.2.3 Cabling Design Considerations

13.2.3.1 General Cabling Standards

13.2.3.1.1 Introduction

BAS cabling is intended to:

- Integrate common services
- Accommodate diverse BAS applications
- Facilitate on-going maintenance and provide the capability of rapid deployment of BAS services
- Provide redundancy for safety and security requirements
- Satisfy requirements for systems and service such as:
 - Building control and monitoring device services
 - Building automation data telecommunications
 - Audio
 - Telecommunications
 - CCTV
 - Other low-voltage systems provided for building infrastructure

13.2.3.1.2 Requirements

Networks supporting a mission-critical data center's BAS must be highly reliable and available. To ensure security systems availability, the design and construction shall take into account the potential for network survivability. Specifically:

- Dual (or multiple) network cabling may be considered to interconnect vital equipment and platforms; the dual network cables should be laid along different paths to minimize the chances of being damaged at the same time.
- Separate TRs may be allocated to host the redundant equipment and be placed with sufficient physical separation to reduce the chances of all the equipment being damaged at once because of fire or some other localized catastrophic event.

Active components and equipment shall only be installed at the ends of the link and never within.

PoE midspan devices shall be installed in the TR, HDA, MDA, or where the link end resides.

13.2.3.1.3 Recommendations

In the presence of equipment and cable faults, such as power outage, fires, and broken cables, the BAS should be designed to provide extended operations without interruption as long as possible within safety guidelines.

A horizontal connection point (HCP) is similar in function and design as a consolidation point (CP). The number of links served by an HCP should be limited to 12. A HCP and a CP can be housed within the same zone box utilizing the same patch panel. If done this way, voice/data circuits should be assigned from the first port as the BAS service should be assigned starting at the last port.

13.2.3.2 Topology

13.2.3.2.1 Requirements

Unless strictly specified otherwise by the BAS equipment manufacturer, the cabling shall use a hierarchical star topology and follow the specifications of TIA-862-A for the portion of the BAS cabling that uses structured cabling. Some equipment, such as sensors, may require a topology other than a hierarchical star topology for the portion of the system that does not use structured cabling. In that case, follow manufacturer's instructions and local codes.

A centralized BAS must be deployed according to the manufacturer's instructions.

13.2.3.2.2 Recommendations

A centralized BAS can use the star topology even though this approach may have distance limitations.

A zone-based topology is recommended for large data centers.

Each cabinet and rack line-up (or pod) may have its own zone management enclosure or patch panel. However, they shall allow for uninterrupted links for alarms and control systems monitoring from a central location.

13.2.3.3 Media

13.2.3.3.1 Introduction

Media are the different cabling materials used to transport information and commands throughout the links.

13.2.3.3.2 Recommendations

BAS devices are interconnected with the same physical layer cabling that supports many other applications in the data center environment. As such, preferred BAS media are the same as other applications media. For additional information about the categories/classes of cabling, refer to Sections 14.8 and 14.9.

13.2.3.3.3 Additional information

Media conversion is employed whenever two different media must interface to create a communications link. For example, a balanced twisted-pair to fiber media conversion unit may be used at the ends of an optical fiber link to allow for equipment with balanced twisted-pair ports to communicate with each other through longer distances or an environment with a higher EMI potential, depending on its pathway environment.

Some devices may require cable types not typically used in structured cabling. However, this may prevent future upgrades or vendor replacement.

13.2.3.4 Pathways and Spaces

13.2.3.4.1 Introduction

Pathways are the systems of cable trays, raceways, ducts, and non-continuous supports used to route and protect the cables.

13.2.3.4.2 Requirements

The BAS cabling and communications systems cabling shall use separate pathways whenever there is likely to be electromagnetic interference between them. Pathways and spaces used exclusively for BAS cabling shall be clearly marked as such.

13.2.3.4.3 Recommendations

Consider dedicated pathways for mission-critical BAS systems.

13.2.3.5 Cabling Management and Termination

13.2.3.5.1 Introduction

Cabling management is the system and standards by which cabling and cabling infrastructure systems are installed, maintained, and labeled both initially and throughout the data center's lifespan.

13.2.3.5.2 Recommendations

Data center BAS cabling should terminate in separate dedicated IDC blocks and patch panels and not share IDC blocks and patch panels terminating communications links.

Data center BAS IDC blocks and patch panels should be clearly marked as such.

13.2.3.6 Enclosures

13.2.3.6.1 Requirements

Enclosures for BAS are classified as either wall mountable or cabinet or rack mountable. Cabinet or rack mountable enclosures shall meet applicable ISO/IEC or ANSI requirements and allow for mounting within 19 in or 23 in racks.

External enclosures shall:

- Provide enough securing points for a safe attachment to a wall
- Provide protection from outdoor's harsh environment at least to the level required by the equipment installed inside
- Be lockable

Internal enclosures shall:

- Have dimensions allowing for fitting in wall spaces and provide enough space to terminate and properly protect incoming and outgoing wiring
- Be lockable, if required
- Meet local fire codes to ensure equipment survivability and reliability during a fire

13.2.3.6.2 Recommendations

Enclosures dedicated to security systems should allow for installation of extra locks to prevent unauthorized access.

13.3 Electronic Safety and Security Systems

13.3.1 Introduction

To support the safety and security plans of a data center, traditional safety and security systems are increasingly using network concepts and infrastructure to support and provide their intended functionality. Termed “convergence,” network capability and communication is now seen in all manner of systems, including safety (e.g., fire detection and notification, access control, video surveillance and intrusion detection systems). Additionally, these systems are also being integrated with other building systems such as lighting and temperature control.

13.3.2 Cabling Infrastructure

13.3.2.1 Requirements

All systems shall meet applicable codes and AHJ requirements. Additionally, cabling infrastructure for ESS systems shall meet BICSI 005.

13.3.2.2 Recommendations

The cabling infrastructure for life safety and critical security systems, should meet, at a minimum, the requirements of Class C2 (see Section 14.2).

Pathways used to support ESS systems should remain separate from communication and other system pathways.

14 Telecommunications Cabling, Infrastructure, Pathways and Spaces

14.1 Introduction

This section is intended to provide design standards for the telecommunications cabling requirements relating to:

- New data centers
- Additions to existing data centers
- Modifications and renovations to existing data centers

NOTE: See TIA-942-A, CENELEC EN 50173-5, ISO/IEC 24764, or other applicable data center telecommunications cabling standards regarding data center telecommunications cabling topologies and distributors.

Telecommunications distribution consists of two basic elements—the distribution pathways and related spaces and the distribution cabling system.

Telecommunications cabling is, therefore, one subset of telecommunications distribution and may be described as a specific system of balanced twisted-pair, unbalanced cabling (e.g., coaxial) and optical fiber cabling, equipment/patch cords, connecting hardware, and other components supplied as a single entity.

The following partial listing of common services and systems should be considered when the cabling is designed:

- Voice, modem, and facsimile telecommunications service
- Switching and server equipment
- Computer and telecommunications management connections
- Keyboard/video/mouse (KVM) connections
- Intelligent infrastructure management (IIM)
- Wide area networks (WAN)
- Local area networks (LAN)
- Storage area networks (SAN)
- Wireless systems utilized in the data center including wireless LANs
- Other building signaling systems (building automation systems such as fire, security, power, HVAC, and EMS)

In addition to satisfying today's telecommunications requirements, the cabling should be planned to reduce ongoing maintenance and relocation. It should also accommodate future equipment and service changes. Consideration should be given to accommodating a diversity of user applications in order to reduce or eliminate the probability of requiring changes to the cabling as equipment needs evolve. The cabling can be accessed for reconfiguration under the access floor or overhead on cable raceway systems. However, in a properly planned facility, disturbance of the cabling should only occur during the addition of new cabling.

14.2 Telecommunications Cabling Infrastructure Classes

14.2.1 Introduction

A properly designed, installed, and implemented telecommunications cabling infrastructure will support the network architecture. When implemented correctly, redundancy, scalability, and flexibility will not only meet the initial network architecture needs, but also enable adaptation to future network architecture requirements where possible.

To some, it may seem unusual to extract the telecommunications cabling infrastructure, a sub-set of the entire network architecture and infrastructure, as a separate data center services layer. The telecommunications cabling infrastructure has been extracted as a separate data center services layer because:

- There is a clear delineation between the standards bodies that oversee the physical characteristics of the telecommunications cabling infrastructure components (e.g., ISO/IEC, TIA) and the higher layers of the network protocols (e.g., IEEE). It is important to maintain that separation within the BICSI data center services end-to-end reliability classification so that appropriate implementation and best practices guidance can be provided to align with the standards independently developed by these standard bodies.

<List continues on next page>

- Although the design of a data center needs to start with a thorough understanding of each service layer starting from the top down, the physical build-out of data centers begins from the bottom-up. The physical network cabling infrastructure must be designed and built often before the complete details of the network architecture are clearly defined. However, if the targeted reliability Class has been identified, the appropriate physical network cabling infrastructure can be designed and implemented.

The telecommunications cabling infrastructure service layer consists of:

- Entrance Pathways: The entrance pathways supporting the service provider's, leased, or customer-owned outside plant cabling from the property line to the data center building.
- Entrance Rooms (ER): The room or area that supports the network service provider's edge equipment, terminating outside plant cable and provisions for their optical switches.
- Main Distribution Area (MDA): The room or area that supports customer-owned core equipment, including routers, core switches, firewall, load balancers, DNS, and possibly core SAN fabric switches.
- Horizontal Distribution Area (HDA): The area that supports intermediate switching and the horizontal cross-connect field between the EDA and MDA.
- Equipment Distribution Area (EDA): The equipment racks and cabinets that house processing or storage systems hardware. Equipment areas that support large frame processing or storage systems are also considered an EDA.

For the telecommunications cabling infrastructure reliability classes, the corresponding class designation is prefaced with a "C" to identify it represents the "cabling infrastructure" reliability criteria.

14.2.2 Class C0 and C1 Telecommunications Infrastructure

A Class C0 or C1 telecommunications cabling infrastructure is a single path cabling infrastructure. The cross-connect fields throughout the data center support a single path, non-redundant network architecture.

Table 14-1 Class C0 and C1 Overview

Entrance Pathways:	Single path, multiple conduits (as specified in Section 14.5.1) from property line to ER
Entrance Room:	One ER accommodates service provider
Main Distribution Area:	One MDA supports all core equipment
Intermediate Distribution Area	Each HDA supported by a single MDA or IDA
Horizontal Distribution Area:	Non-redundant HDA to support any intermediary switching equipment and horizontal cross-connect fields, multiple HDAs may be required to support port counts and distance limitations within large computer rooms.

14.2.3 Class C2 Telecommunications Infrastructure

A Class C2 telecommunications cabling infrastructure is a single path cabling infrastructure. The cross-connect fields throughout the data center support a single path, non-redundant network architecture. It contains redundant entrance pathways to support, at a minimum, a single link from two providers or ringed topology from one provider.

Table 14-2 Class C2 Overview

Entrance Pathways:	Redundant and diverse multi-path, each path with multiple conduits (as specified in Section 14.5.1) from property line to ER
Entrance Room:	One ER accommodates service provider(s)
Main Distribution Area:	One MDA supports all core equipment
Intermediate Distribution Area	Each HDA supported by a single MDA or IDA
Horizontal Distribution Area:	Non-redundant HDA to support any intermediary switching equipment and horizontal cross-connect fields, multiple HDAs may be required to support port counts and distance limitations within large computer rooms.

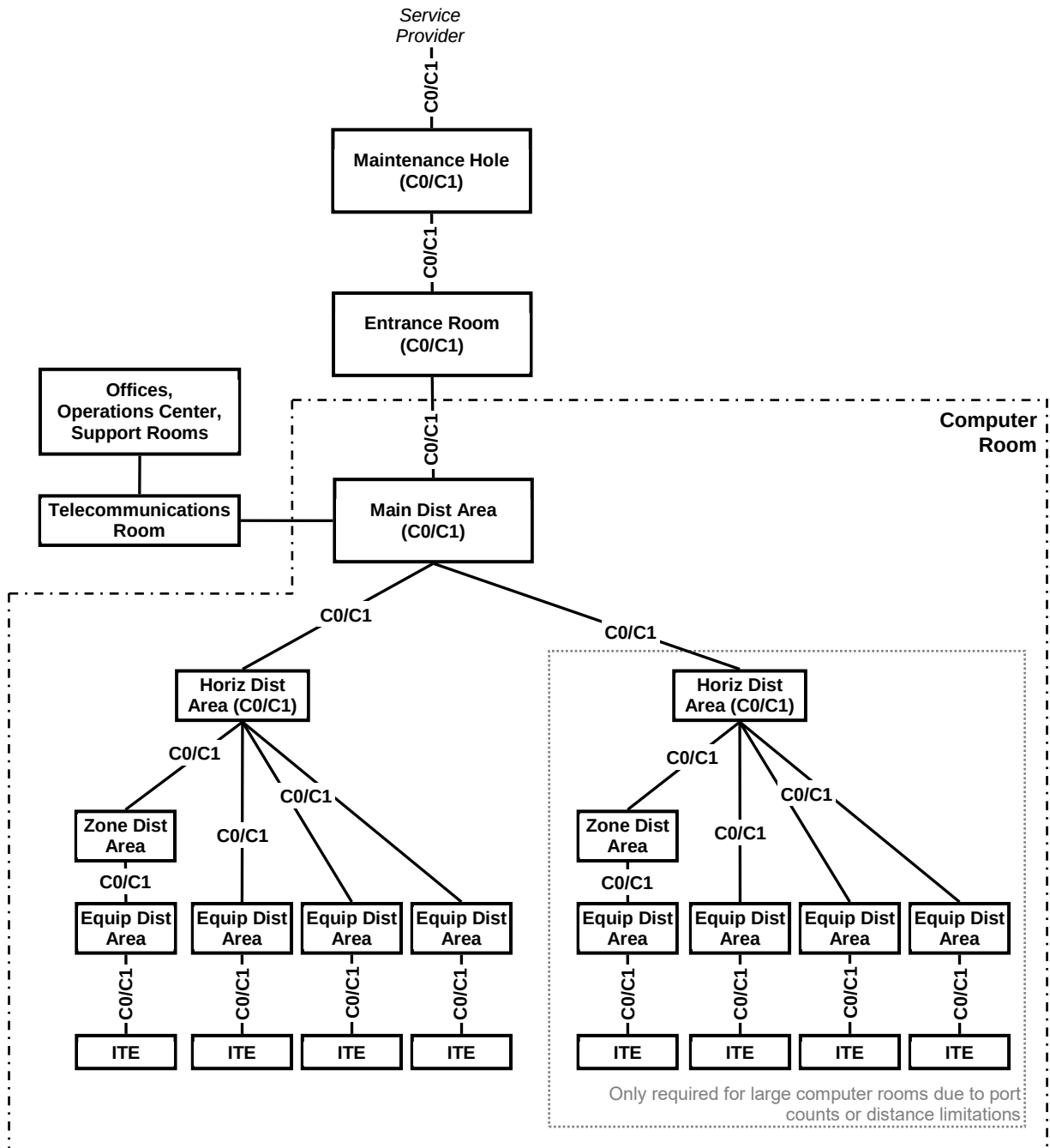


Figure 14-1
Class C0 and C1 Concept Diagram

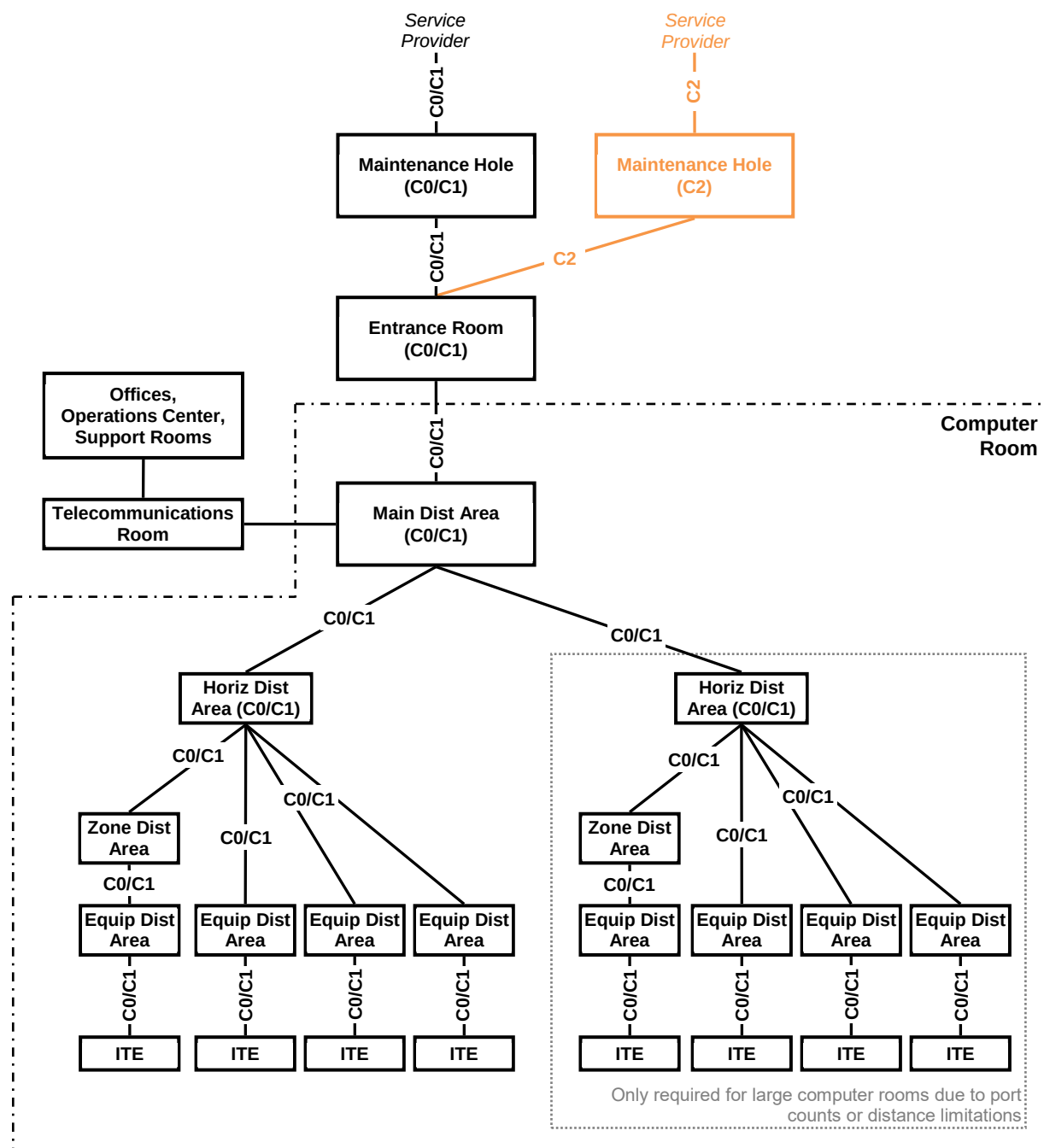


Figure 14-2
Class C2 Concept Diagram

14.2.4 Class C3 Telecommunications Infrastructure

A Class C3 telecommunications cabling infrastructure is a redundant path cabling infrastructure that has redundant cross-connect fields for all backbone network cabling. The redundant backbone cabling is intended to support a redundant network topology (e.g., redundant switches, routers. See class N3 network topology in Section 15.6.

Physically separated redundant horizontal cross-connects and redundant horizontal cabling to equipment cabinets (EDAs) is also recommended. Physical separation between redundant MDAs, IDAs, or HDAs may minimize common modes of failure that may be present within the supporting critical infrastructure (e.g., failure of sprinkler system, raised floor system, cabling pathway system, grounding system). Physical separation may also minimize failure because of any event caused by human error or component failure, which is not contained within a MDA or HDA cabinet, thereby exposing adjacent cabinets to risk of failure. Having redundant distributors and cabling may increase operational complexity.

Table 14-3 Class C3 Overview

Entrance Pathways:	Redundant and diverse multi-path, each path with multiple conduits (as specified in Section 14.5.1) from property line to each ER
Entrance Room:	Two ERs to support multiple service providers, providing physical separation between redundant providers edge equipment
Main Distribution Area:	MDAs support the main cross-connect (MC) and backbone network equipment. Redundant MDAs should be physically separated.
Intermediate Distribution Area	IDAs support the intermediate cross-connect (IC) and possibly backbone network equipment. Redundant IDAs should be physically separated.
Horizontal Distribution Area:	HDAs support horizontal cross-connects and may support access layer switches. Equipment cabinets (EDAs) should (but are not required to) have horizontal cabling to two different, physically separated HDAs.

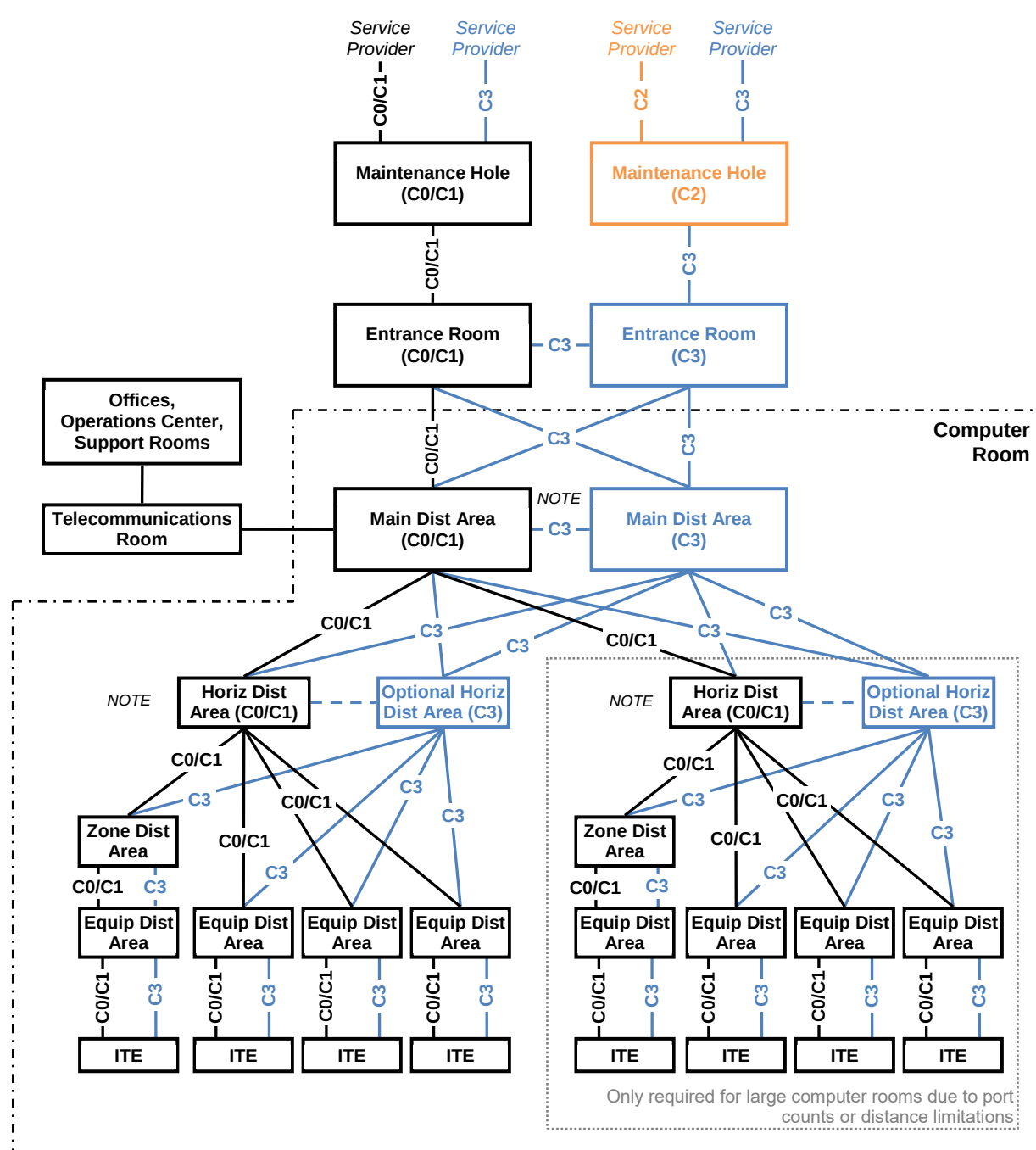
14.2.5 Class C4 Telecommunications Infrastructure

A Class C4 telecommunications infrastructure is a redundant path cabling infrastructure that has redundant cross-connect fields throughout data center network to support redundant network architecture. It contains redundant entrance facilities to support multiple network service provider topologies.

Physical separation between redundant MDAs or HDAs is required to minimize common modes of failure that may be present within the supporting critical infrastructure (e.g., failure of; sprinkler system, raised floor system, cabling infrastructure pathway system, grounding system, electrical distribution system) or any event caused by human error or component failure, which is not contained within one MDA or HDA cabinet, thereby exposing adjacent cabinets to risk of failure as well.

Table 14-4 Class C4 Overview

Entrance Pathways:	Redundant and diverse multi-path, each path with multiple conduits (as specified in Section 14.5.1) from property line to each ER
Entrance Room:	Two ERs to support multiple service providers, providing physical separation between redundant providers edge equipment
Main Distribution Area:	Two MDAs to support redundant core equipment. Physical separation between redundant MDAs is required to minimize common modes of failure that may be present within the supporting critical infrastructure.
Intermediate Distribution Area	Redundant physically separated IDAs. If an HDA has backbone cabling to IDAs, it must be supported by diversely routed backbone cabling to two physically separated IDAs.
Horizontal Distribution Area:	Redundant HDAs to support any intermediary redundant switching equipment and horizontal cross-connect fields, additional HDAs may be required on both the "A" and "B" network fabric to support increased port counts and distance limitations within large computer rooms. Physical separation between redundant HDAs is required to minimize common modes of failure that may be present within the supporting critical infrastructure.



NOTE: Physical separation between redundant MDA and HDA is required to minimize common modes of failure.

Figure 14-3
Class C3 Concept Diagram

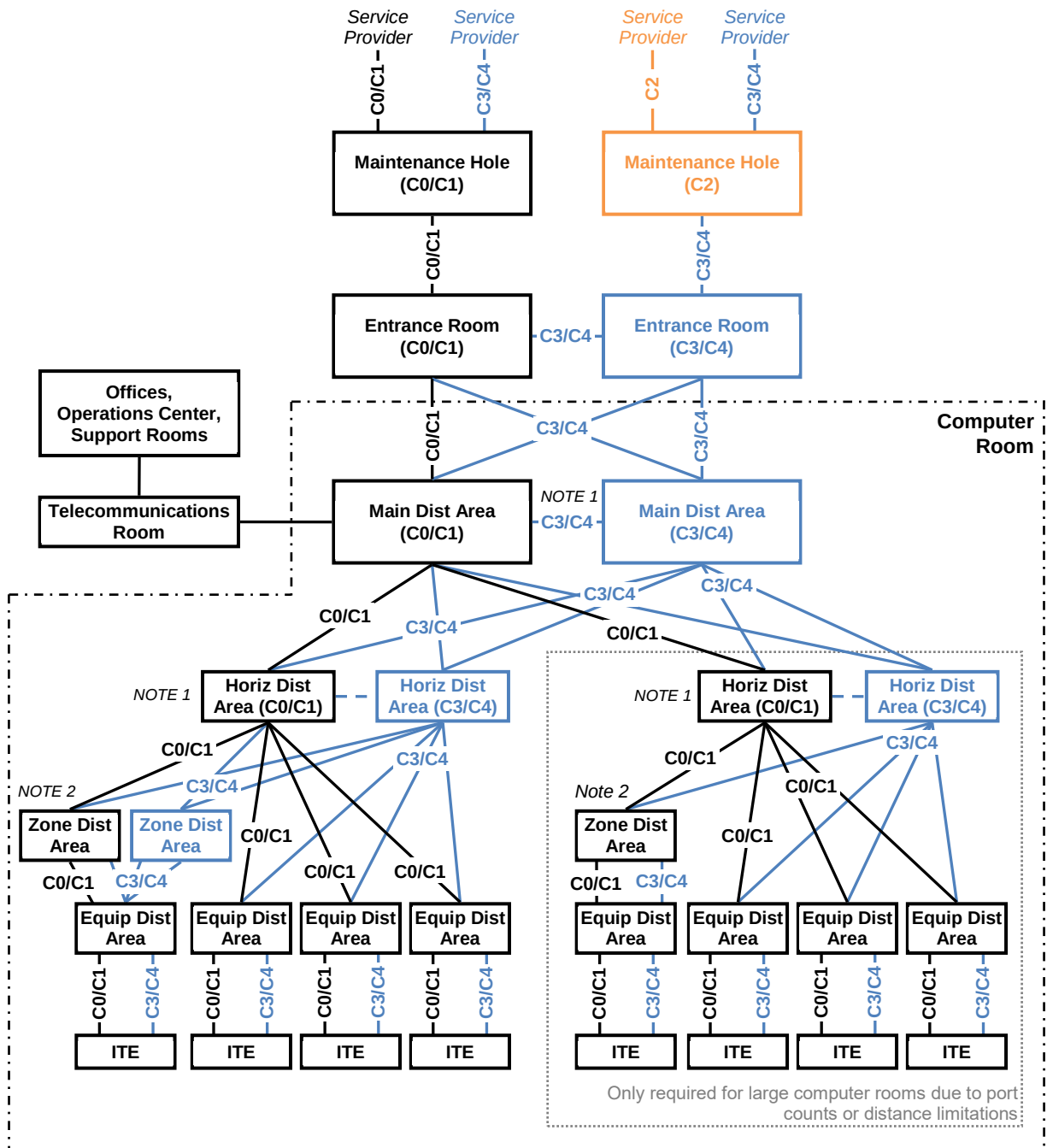


Figure 14-4
Class C4 Concept Diagram

14.3 Cabling Topology

14.3.1 Introduction

The basic cabling elements of the data center star topology include:

- Horizontal cabling
- Backbone cabling
- Equipment cabling
- TIA main cross-connect (MC) or ISO/CENELEC main distributor (MD) in the main distribution area (MDA)
- TIA intermediate cross-connect (IC) or ISO/CENELEC intermediate distributor (ID) in the intermediate distribution area (IDA)
- TIA horizontal cross-connect (HC) or ISO/CENELEC zone distributor (ZD) in the horizontal distribution area (HDA), intermediate distribution area (IDA), or main distribution area (MDA)
- TIA zone outlet, TIA consolidation point (CP) or ISO/CENELEC local distribution point (LDP) in the zone distribution area
- Equipment outlets (EO) in the equipment distribution area (EDA)

14.3.2 Horizontal Cabling Topology

14.3.2.1 Requirements

The horizontal cabling shall be installed in a star topology. Each EDA shall be connected to a TIA HC or an ISO/CENELEC ZD in a HDA, IDA, or MDA via horizontal cabling.

14.3.3 Backbone Cabling Topology

14.3.3.1 Requirements

The backbone cabling shall use the hierarchical star topology, as illustrated by Figure 14-5, wherein each HC in the HDA is cabled directly to an MC in the MDA or an IC in an IDA. There shall be no more than two hierarchical levels of cross-connects in the backbone cabling.

Direct backbone cabling to the HC shall be allowed when distance limitations are encountered.

14.3.3.2 Recommendations

The presence of an HDA or IDA is not mandatory. Cabling extending from the TIA HC or ISO/CENELEC ZD in the HDA, IDA, or MDA to the mechanical termination in the EDA is considered horizontal cabling. Sufficient horizontal cable slack should be considered to allow migration to a cross-connect in the HDA, IDA, or MDA.

Backbone cabling cross-connects may be located in TRs, computer rooms, MDAs, IDAs, HDAs, or at entrance rooms.

14.3.4 Accommodation of Non-Star Configurations

14.3.4.1 Introduction

The topology, as shown in Figure 14-5, with the appropriate interconnections, electronics, or adapters in data center distribution areas, accommodates systems that are designed for non-star configurations such as ring, bus, or tree.

14.3.4.2 Recommendations

Cabling is permitted between entrance rooms, MDAs, IDAs, and HDAs to provide redundancy and to avoid exceeding application cabling distance restrictions for connections that route through two HDAs.

14.3.5 Redundant Cabling Topologies

14.3.5.1 Introduction

Redundant topologies can include a parallel hierarchy with redundant distribution areas. These topologies are in addition to the star topology specified in this standard.

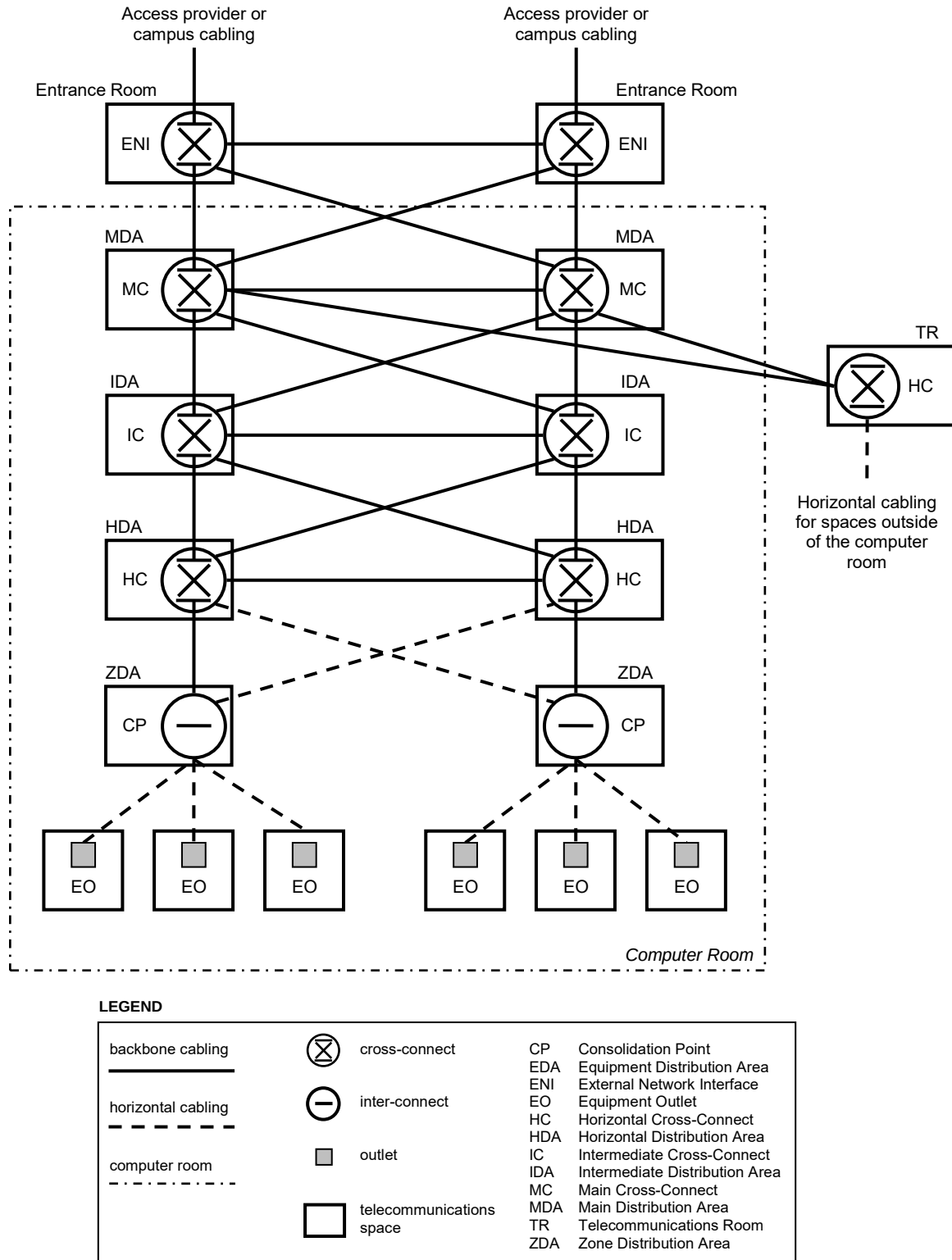


Figure 14-5
Data Center Cabling Topology Example

14.4 Data Center Spaces for Telecommunications

14.4.1 Introduction

Data center spaces dedicated to supporting the telecommunications cabling system and related equipment are listed below. These spaces include:

- Entrance room
- Main distribution area (MDA)
- Intermediate distribution area (IDA)
- Horizontal distribution area (HDA)
- Zone distribution area (ZDA)
- Equipment distribution area (EDA)

These spaces may be physically separated or may exist within different areas of the same room through the use of partitions or location.

14.4.2 Design and Structural Requirements

Data center telecommunications spaces such as the MDA and entrance room(s), shall be sized for full data center occupancy, including all anticipated expansions and planned applications.

All data center spaces for telecommunications shall have the same mechanical and electrical redundancy as the computer room(s).

The computer room shall provide an operational environment in line with the limits and requirements set out in the applicable telecommunications cabling and data center standards for an M₁I₁C₁E₁ environment (see ISO/IEC TR 29106 or TIA TSB-185).

See Section 7 regarding architectural requirements and recommendations for telecommunications spaces, including door sizes and ceiling heights.

14.4.3 Entrance Rooms

14.4.3.1 Introduction

The entrance room may include both access provider and customer-owned cabling. This space may include the access provider demarcation hardware and access provider equipment and the location where conversion takes place between cabling that is suitable for outside plant applications and cabling that is suitable for premises (i.e., inside plant) applications.

The entrance room interfaces with the data center through the MDA. However, direct connections from intermediate distribution areas (IDAs) or horizontal distribution areas (HDAs) to the entrance rooms are permitted to avoid exceeding circuit distance limitations. The entrance room may be adjacent to or combined with the MDA.

14.4.3.2 Requirements

Access providers that serve the building shall be contacted to ascertain the point(s) of entry to the property and the requirements for their telecommunications cabling, terminations, and equipment.

Class C2 and higher data centers shall have diverse entrance facilities, preferably with route diversity from the data center to different access providers. For example, a Class C2 data center may be served from multiple central offices and multiple service provider point-of-presences that enter the property at different locations.

The location of each building entrance facility shall be coordinated with routing of access provider pathways as well as internal pathways and shall not conflict with the location of other building facilities such as power, gas, and water.

14.4.3.3 Recommendations

Each building point-of-entry supporting an access provider's outside plant facilities should be located on different (or even opposite) sides of the building. Conduit duct banks and their associated maintenance holes and other pathways from the access provider central offices and service provider point-of-presences to the building's entrance facilities should be separated by at least 20 m (66 ft) along their entire routes.

A conduit duct bank with appropriately placed maintenance holes that surrounds a data center and incorporates multiple building entrance facilities should be considered for the data center. At least one conduit for replacement cables should be set aside for each internal and entrance pathway to facilitate rapid replacement of cables. The use of innerduct, either conventional or fabric, is recommended to aid in cable management and increased utilization of available conduit space.

When using multiple entrance rooms, entrance rooms should be at least 20 m (66 ft) apart and be in separate fire protection zones. The two entrance rooms should not share power distribution units or air conditioning equipment. Telecommunications entrance cabling for data centers should not be routed through a common equipment room unless cabling is segregated from common access via conduit or other means.

Entrance rooms should be outside the computer room proper to improve security. However, they may be placed in the computer room or consolidated with the main distribution area if cabling distances for circuits is an issue, security is not an issue, or other security measures are used to ensure security (such as escorting and monitoring the activities of all technicians in the computer room).

14.4.3.4 Additional Information

Where used for the purpose of demarcation, the entrance room typically has separate areas for access provider demarcation:

- Demarcation for low-speed balanced twisted-pair circuits (e.g., DS-0, ISDN BRI, telephone lines)
- Demarcation for high-speed balanced twisted-pair circuits (e.g., DS-1 [T-1 or fractional T-1], ISDN Primary Rate, E-1 [CEPT-1])
- Demarcation for high speed coaxial cabling circuits, (e.g., DS-3 [T-3] and E-3 [CEPT-3])
- Demarcation for high speed optical fiber circuits (e.g., SONET/SDH, Fast Ethernet, 1/10/40/100 Gigabit Ethernet)

Each of these functions may be provided on customer-provided meet-me racks, cabinets, or frames where all service providers hand-off their circuits (see Section 14.6.3).

If an access provider demarks its services into cabinets or racks, the customer typically installs cabling from that access provider's demarcation point to the desired patching location or user equipment.

14.4.4 Main Distribution Area (MDA)

14.4.4.1 Introduction

The MDA includes the main cross-connect (MC), which is the central point of distribution for the data center structured cabling system. The main cross-connect is called the main distributor (MD) in CENELEC EN 50173-5 and in ISO/IEC 24764.

Equipment typically located in the MDA includes:

- Core routers
- Core, spine, or interconnection layer LAN and SAN switches
- High-performance computing switches
- PBX or voice gateways
- T-3 (M13) multiplexers

The MDA may serve one or more IDAs, HDAs, and EDAs within the data center and one or more telecommunications rooms (TRs) located outside the computer room space to support office spaces, operations center, and other external support rooms.

The MDA may include a horizontal cross-connect (TIA) or zone distributor (ISO/CENELEC) when equipment areas are served directly from the MDA. This space is inside the computer room; it may be located in a dedicated room for improved security.

14.4.4.2 Requirements

Every data center shall have at least one MDA. A second MDA shall be provided to meet the availability requirements of the telecommunications infrastructure (e.g., Class C4). If two MDAs are present, both shall meet all requirements of the MDA as specified in the applicable data center standard.

Access provider provisioning equipment (e.g., M13 multiplexers) may be located in the MDA rather than in the entrance room to avoid the need for a second entrance room because of circuit distance restrictions.

14.4.4.3 Recommendations

A second MDA is recommended in Class C3 data centers. Each MDA should have fully diverse cable routes to access multiple entry points so that no single point of failure exists within the site.

When utilizing two MDAs, the MDAs should:

- Have core routers and switches distributed between the MDAs
- Distribute circuits between the two spaces
- Be located in different fire protection zones
- Be served by different power distribution units and air conditioning equipment

14.4.5 Intermediate Distribution Area (IDA)**14.4.5.1 Introduction**

The intermediate distribution area (IDA) is the space that supports the intermediate cross-connect. The intermediate cross-connect is called the intermediate distributor (ID) in CENELEC EN 50173-5 and in ISO/IEC 24764.

It may be used to provide a second level cabling subsystem in data centers too large to be accommodated with only MDAs and HDAs. The IDA is optional and may include active equipment such as LAN and SAN switches.

The IDA may include the horizontal cross-connect (TIA) or zone distributor (ISO/CENELEC) for equipment areas served directly from the IDA.

14.4.5.2 Recommendations

The IDA may be inside the computer room but can be located in a dedicated room or a secure cage within the computer room for additional security.

14.4.6 Horizontal Distribution Area (HDA)**14.4.6.1 Introduction**

The HDA is used to serve equipment not supported by a horizontal cross-connect (HC) or zone distributor (ZD) in an IDA or MDA. The HDA is the distribution point for cabling to the EDAs.

Equipment typically located in the HDA includes:

- LAN switches
- SAN switches
- Keyboard/video/mouse (KVM) switches

This equipment is used to provide network connectivity to the end equipment located in the EDAs. A small data center may not require any HDAs as the entire data center may be able to be supported from the MDA. A typical data center will have several HDAs.

14.4.6.2 Recommendations

The HDA is typically inside the computer room, but it can be located in a dedicated room or a secure cage within the computer room for additional security.

14.4.7 Zone Distribution Area (ZDA)**14.4.7.1 Introduction**

The ZDA is an optional interconnection point within the horizontal cabling located between the HDA and the EDA to allow frequent reconfiguration and added flexibility.

The consolidation point in the ZDA is called the local distribution point or LDP in CENELEC EN 50173-5 and in ISO/IEC 24764.

14.4.7.2 Requirements

Horizontal cabling shall contain no more than one ZDA between the HC in the HDA and the mechanical termination in the EDA.

14.4.7.3 Recommendations

The zone distribution area may also serve as a zone outlet for nearby equipment in the computer room.

14.4.8 Equipment Distribution Area (EDA)

14.4.8.1 Introduction

The EDA is the space allocated for end equipment, including all forms of telecommunications equipment (e.g., computer equipment, telephony equipment).

The telecommunications outlet (TO) in the EDA is called the equipment outlet (EO) in ISO/IEC 24764, CENELEC EN 50173-5, and TIA-942-A.

14.4.8.2 Requirements

EDA areas shall not serve the purposes of an entrance room, MDA, IDA, or HDA.

14.5 Outside Plant Cabling Infrastructure

14.5.1 Underground Service Pathways

14.5.1.1 Requirements

The upper surface of underground cable pathways shall be no less than 600 mm (24 in) below the surface.

Non-metallic conduits shall be encased in concrete with a minimum 17000 kPa (2500 lb/sq in) compressible strength where there is vehicular traffic above or a bend in the conduits.

Telecommunications entrance pathways shall terminate in a secure area within the data center.

The telecommunications entrance pathways shall be coordinated with other electrical underground pathways (e.g., conduits) and mechanical underground piping systems (e.g., water, waste) while maintaining appropriate pathway separation from physical and operational perspectives.

14.5.1.2 Recommendations

The data center site should include multiple duct banks with customer owned maintenance holes from the property line to the data center.

Duct banks should consist of a minimum of four 100 mm (trade size 4) or equivalent conduits or raceways. If initial plans include more than three access providers providing service to the facility, one additional 100 mm (trade size 4) or equivalent conduit or raceway should be provided for every additional access provider. Each carrier's cabling should be in separate, dedicated conduits or raceways. Carriers should not share pathways.

Where not defined by the AHJ, duct banks and conduits should be located at a sufficient depth, typically 600 mm (24 in) to 750 mm (30 in) below surface grade, so both live or dynamic and dead (static) or earth loads can be sustained by the conduit structure. Conduits should be a depth greater than the depth of anticipated future digging.

In regions susceptible to frost, the top of the conduit(s) should be below the frost line. Where this is not practical, adequate protection should be provided to ensure that conduits do not become damaged as a result of ground shifting, particularly at the point of entry into the building.

Maintenance holes and hand holes on the data center property should have locks or other means of deterring access such as nonstandard bolts. The maintenance holes and hand holes should have intrusion detection devices connected to the building security system and monitoring of the maintenance holes and hand holes by CCTV or other means.

Redundant duct banks should have a 20 m (66 ft) separation minimum along the entire route from the property line to the facility. Where possible, redundant maintenance holes should be connected with at least one 100 mm (trade size 4) or equivalent conduit or raceway.

Conduits for cable replacement should be designated and marked separately from those for additional cables.

When multiple access providers are providing service to the facility, coordination of security requirements of each individual access provider should be within the secure space.

The secure area that houses the telecommunications entrance facility (pathway termination) should preferably be in a telecommunications entrance room that is separate from the computer room.

Any pull boxes or splice boxes for data center cabling (entrance cabling or cabling between portions of the data center) that are located in public spaces or shared tenant spaces should be lockable. They should also be monitored by the data center security system using either a camera or remote alarm.

Entrance to utility tunnels used for telecommunications entrance rooms and other data center cabling should be lockable. If the tunnels are used by multiple tenants or cannot be locked, they should be monitored by the data center security system using either a camera or remote alarm.

14.5.2 Aerial Service Pathways

14.5.2.1 Requirements

Routes for aerial access pathways shall follow same provisioning guidelines from an availability and security perspective as underground data pathways. All aerial pathways shall be properly bonded and grounded as per AHJ requirements.

14.5.2.2 Recommendations

The use of aerial cabling pathways should generally be avoided because of vulnerability to outages. Aerial cabling route selection should take into consideration a number of factors, including, but not limited to, terrain, soil conditions, aesthetics, proximity to direct-buried and underground utilities, access, and weather conditions.

Customer-owned satellite dish farms or aerial towers should be located within the secure perimeter of the facility.

14.6 Access Providers

14.6.1 Access Provider Coordination

14.6.1.1 Requirements

Data center designers shall coordinate with all access providers to determine the access providers' requirements and to ensure that the data center's circuit, demarcation, and entrance facility requirements are provided to satisfy the access providers' specifications.

14.6.1.2 Additional Information

Access providers typically require the following information when planning entrance facilities:

- Address of the building
- General information concerning other uses of the building, including other tenants
- Plans with detailed drawings of telecommunications entrance conduits from the property line to the entrance rooms, including location of maintenance holes, hand holes, and pull boxes
- Assignment of conduits and innerducts to the access provider
- Floor plans for the entrance rooms
- Assigned location of the access providers' protectors, racks, and cabinets
- Routing of cabling within entrance room (e.g., under access floor, over cabinets and racks, other)
- Expected quantity and type of circuits to be provisioned by the access provider, including any planned or foreseen additions or upgrades
- Media types and approximate distances of circuits to be provisioned by the carrier
- Service-level agreements
- Detailed schedules for the project, including date that the access provider will be able to install entrance cabling and equipment in the entrance room and required service activation date
- Requested location and interface for demarcation of each type of circuit to be provided by the access provider
- Carrier office diversity desired, preferably at least two separate access provider offices and service provider point-of-presences
- Carrier route diversity desired, preferably a minimum distance between any two routes of at least 20 m (66 ft) along their entire routes
- Specification of pathways to be used for access provider cabling (e.g., aerial cabling allowed or all underground)
- Type and rating of firestopping measures used at the site
- Requested service date
- Name, telephone number, and e-mail address of primary customer contact and local site contact
- Security requirements for lockable containment and cabinets
- Colocation providers may be required to provide customer name and contact details, if requesting on behalf of their customers

The access providers typically provide the following information:

- Space and mounting requirements for protectors and terminations of balanced twisted-pair cabling
- Quantity and dimensions of access provider's cabinets and racks or space requirements if they are to be provisioned in client cabinets and racks
- Power requirements for equipment, including receptacle types
- Access provider equipment service clearances
- Location of serving access provider central offices
- Route of access provider cabling and minimum separation between routes
- Specification on pathways used (e.g., all underground or portions of routes that are served by aerial cabling)
- Installation and service schedule

14.6.2 Redundancy

14.6.2.1 Introduction

Having multiple access providers protects against total loss of service in the event of a service outage affecting one of the access providers but not the others. However, it is necessary to ensure that the access providers are not sharing facilities that would result in one or more single points of failure that would cause a total service outage despite having multiple access providers.

14.6.2.2 Recommendations

Continuity of telecommunications access provider services to the data center can be improved by using multiple access providers, multiple access provider central offices, and multiple diverse pathways from the access provider central offices to the data center.

The customer should ensure that its services are provisioned from different access provider offices, and the pathways to these access provider cabling centers and central offices are diversely routed. These diversely routed pathways should be physically separated by at least 20 m (66 ft) at all points along their routes.

Access providers should install circuit-provisioning equipment in both entrance rooms so that circuits of all required types can be provisioned from either room. The access provider provisioning equipment in one entrance room should not be subsidiary to the equipment in the other entrance room. The access provider equipment in each entrance room should be able to operate in the event of a failure in another entrance room.

14.6.3 Access Provider Demarcation

14.6.3.1 Introduction

The centralized location for demarcation to all access providers may be referred to as “meet-me” areas or “meet-me” racks.

14.6.3.2 General Requirements

In buildings where base isolation is used, access providers shall provide sufficient cable slack to accommodate displacement of the base isolation units.

14.6.3.3 General Recommendations

Access providers should provide demarcation for their circuits in a common owner specified cabinet or rack rather than in their own cabinets or racks as this simplifies cross-connects and management of circuits. Separate demarcation cabinets or racks for each type of circuit may be desirable (e.g., low speed, E-1/T-1, E-3/T-3, optical fiber for STM-x/OC-x services and Ethernet delivery). Cabling from the computer room to the entrance room should terminate in the demarcation areas.

14.6.3.4 Demarcation of Low-speed Circuits

14.6.3.4.1 Recommendations

Access providers should be asked to provide demarcation of low-speed circuits on insulation displacement connection (IDC) connecting hardware. While service providers may prefer a specific type of IDC connecting hardware (e.g., 66-block), they may be willing to hand off circuits on another type of IDC connecting hardware upon request. Access provider should coordinate the type of connectors used with those used by the data center. Cabling from the low-speed circuit demarcation area to the main distribution area should be terminated on IDC connecting hardware near the access provider IDC connecting hardware.

Circuits from access providers are terminated using one or two pairs on the access provider IDC connecting hardware. Different circuits have different termination sequences as illustrated in Figure 14-6 and Figure 14-7.

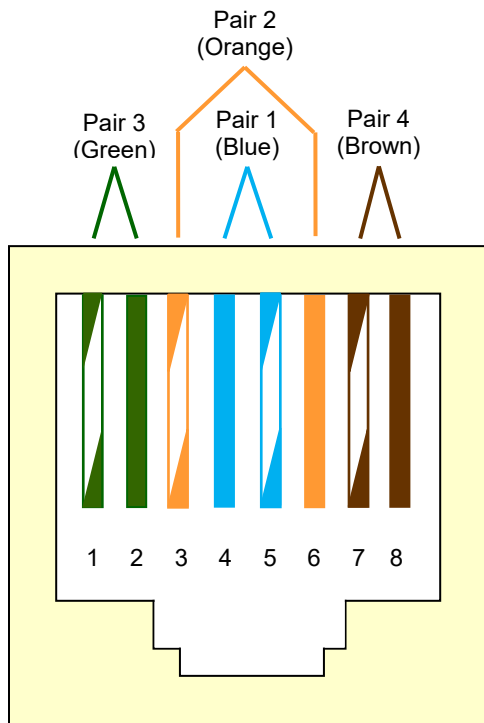


Figure 14-6
Cross-Connection Circuits to IDC Connecting
Hardware Cabled to Modular Jacks in the T568A
8-Pin Sequence

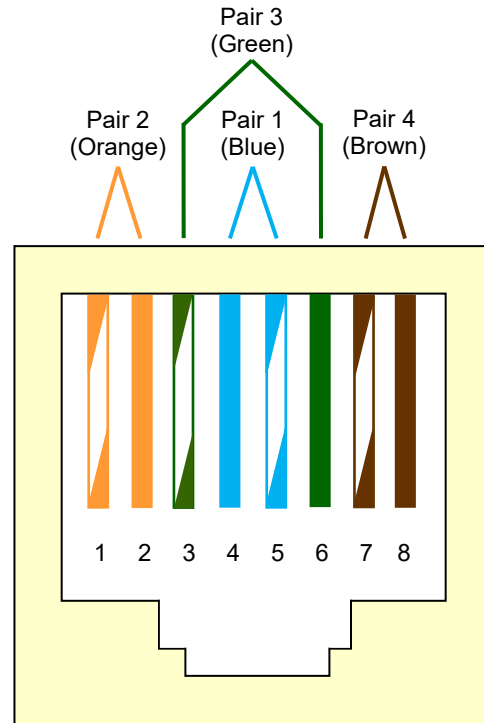


Figure 14-7
Cross-Connection Circuits to IDC Connecting
Hardware Cabled to Modular Jacks in the T568B
8-Pin Sequence

Each 4-pair cable from the entrance room to the other spaces in the data center should be terminated in an IDC connector or an eight-position modular jack of compatible performance where the cable terminates outside the entrance room. The IDC connector or eight-position modular jack telecommunications outlet/connector should meet the modular interface requirements specified in standards such as the IEC 60603-7 series of standards.

Pin/pair assignments should be as shown in the T568A sequence or, optionally, per the T568B sequence if necessary to accommodate certain 8-pin cabling systems. The colors shown are associated with the horizontal distribution cable. Figure 14-6 and Figure 14-7 depict the front view of a female telecommunications outlet/connector and provide the list of the pair positions for various circuit types.

14.6.3.4.2 Additional Information

The conversion from access provider 1-pair and 2-pair cabling to 4-pair cabling used by the data center structured cabling system can occur either in the low-speed circuit demarcation area or in the main distribution area (MDA).

The access provider and customer IDC connecting hardware can be mounted on a plywood backboard, frame, rack, or cabinet. Dual-sided frames should be used for mounting large numbers of IDC connecting hardware (3000+ pairs).

14.6.3.5 Demarcation of E-1 and T-1 Circuits

14.6.3.5.1 Introduction

Coordinate with the local access providers that will install DS-1/E-1 DSX panels in the DS-1/E-1 demarcation area. Their equipment will preferably fit in 482.6 mm (19-inch) racks/cabinets. However, 584.2 mm (23-inch) racks/cabinets may be required by some local access providers, particularly in North America.

14.6.3.5.2 Recommendations

The DSX-1 patch panels may require power for indicator lights. Thus, cabinets or racks supporting access provider DSX-1 patch panels should have at least one electrical circuit or power strip to power DSX-1 panels. As most DSX-1 facilities use -48 V_{DC} or $+24\text{ V}_{\text{DC}}$ to power their indicators, provisions for DC power sources and fuse panels should be included in any DSX facility.

Cabinet or rack space should be allocated for access provider and customer patch panels, including growth. Access providers may require cabinet or rack space for rectifiers to power DSX-1 patch panels.

A single 4-pair cable can accommodate one T-1 transmit and receive pair. When multiple T-1 circuits are carried on a multipair cable arrangement, multiple cables should be provided; transmit signals should be carried on one multipair cable and the receive signals driven through a separate multipair cable.

If support staff has the test equipment and knowledge to troubleshoot T-1 circuits, the DS-1 demarcation area can use DSX-1 panels to terminate T-1 cabling to the main distribution area. These DSX-1 panels should have either modular jacks or IDC terminations at the rear although wirewrap terminations are acceptable and may still be used.

DSX-1 panels for the main distribution area can be located on the same racks, frames, or cabinets as the ones used for distribution cabling. If DSX panels are separate, they should be located in a space adjacent to the cabinets or racks used for distribution cabling.

The owner or the owner's agent may decide to provide multiplexers (e.g., M13 or similar multiplexer) to demultiplex access provider E-3/T-3 circuits to individual E-1/T-1 circuits. Multiplexers may be placed in the computer room, extending the distance from the entrance rooms that E-1/T-1 circuits can be provisioned. E-1/T-1 circuits from a customer-provided multiplexer should not be terminated in the entrance room E-1/T-1 demarcation area.

The coaxial or optical fiber connecting hardware can be located on the same or separate racks, frames, or cabinets as the ones used for other access provider patch panels. If they are separate, they should be adjacent to the racks/cabinets assigned to the access provider's equipment.

As with other services, the access provider should be consulted to determine and agree to the format of the services from an E-1/T-1 carrier. The normal practice is to have these services provided via telecommunications outlet/connectors.

Access providers should be asked to hand-off E-1/T-1 circuits on RJ48X jacks (individual 8-position modular jacks with loop back), preferably on a DSX-1 patch panel mounted on a customer-owned rack installed in the DS-1 demarcation area. Patch panels from multiple access providers and the customer may occupy the same cabinet or rack.

14.6.3.5.3 Additional Information

Access providers can alternatively hand off DS-1 circuits on IDC connecting hardware. These IDC connecting hardware can be placed on the same frame, backboard, rack, or cabinet as the IDC connecting hardware for low-speed circuits.

The customer may request that the demarcation for E-1 or T-1 circuits be provisioned in the MDA rather than in the entrance room to ensure that circuit distance restrictions are not exceeded. See TIA-942-A for distances for T-1 and E-1 circuits in data centers. As described in TIA-942-A, note that customer side-DSX panels provide test access for circuits, but they reduce maximum circuit distances.

14.6.3.6 Demarcation of T-3 and E-3 Coaxial Cabling Circuits

14.6.3.6.1 Recommendations

Access providers should be asked to hand-off E-3 or T-3 coaxial circuits on pairs of female BNC connectors, preferably on a DSX-3 patch panel on a customer-owned cabinet or rack installed in the E-3/T-3 demarcation area. Patch panels from multiple access providers and the customer may occupy the same cabinet or rack.

Coordination with the local access providers should involve the installation of DS-3 DSX panels in the DS-3 demarcation area. This equipment should be mounted in 482.6 mm (19-inch) cabinets or racks in order to maintain consistency with other racks/cabinets. However, 584.2 mm (23-inch) cabinets or racks may be required by some local access providers, particularly in North America.

If support staff has the test equipment and knowledge to troubleshoot E-3 or T-3 circuits, the E-3/T-3 demarcation area can use DSX-3 panels to terminate 734-type coaxial cabling to the main distribution area. These DSX-3 panels should have BNC connectors at the rear.

The DSX-3 patch panels may require power for indicator lights. Thus, racks/cabinets supporting access provider DSX-3 patch panels should have at least one electrical circuit and a power strip. As most DSX-3 facilities use -48 V_{DC} or $+24\text{ V}_{\text{DC}}$ to power their indicators, provisions for DC power sources and fuse panels should be included in any DSX facility.

Allocate cabinet and rackspace for access provider and customer patch panels, including growth. Access providers may require cabinet and rack space for rectifiers to power DSX-3 patch panels.

Cabling from the E-3/T-3 demarcation area to the main distribution area should be 734-type coaxial cable. Cables in the E-3/T-3 demarcation area can be terminated on a customer patch panel with 75-ohm BNC connectors or directly on an access provider DSX-3 patch panel. Access provider DSX-3 patch panels typically have the BNC connectors on the rear of the panels. Thus, BNC patch panels for cabling to the main distribution area should be oriented with the front of the patch panels on the same side of the cabinet or rack as the rear of the access provider DSX-3 panels.

All connectors and patch panels for E-3 and T-3 cabling should use 75-ohm BNC connectors.

14.6.3.6.2 Additional Information

The customer may request that the demarcation for E-3 or T-3 circuits be provisioned in the MDA rather than in the entrance room to ensure that circuit distance restrictions are not exceeded. See the applicable cabling standard (e.g., TIA-942-A) for maximum distances of T-3 and E-3 circuits over coaxial cabling in data centers. As described in TIA-942-A, note that customer side-DSX panels provide test access for circuits, but they reduce maximum circuit distances.

14.6.3.7 Demarcation of Optical Fiber Circuits

14.6.3.7.1 Recommendations

Access providers should terminate optical fiber circuits on optical fiber patch panels installed on cabinets or racks in the fiber demarcation area. Optical fiber patch panels from multiple access providers and the customer may occupy the same cabinet or rack. The optical fiber interface should comply with requirements defined in the cabling standards being followed (e.g., IEC 61754-20 [duplex LC-APC]). If requested, access providers may be able to provide a different format connector that is compatible with existing connector formats being used to simplify equipment cord and patch cord requirements.

Coordination with the local access providers should involve the installation of optical fiber patch panels in the optical fiber demarcation area. This equipment should be mounted in 482.6 mm (19-inch) cabinets or racks in order to maintain consistency with other racks/cabinets. However, 584.2 mm (23-inch) cabinets or racks may be required by some local access providers, particularly in North America.

Cabling from the optical fiber demarcation area to the main cross-connect in the main distribution area should be coordinated to ensure that the correct quantity, circuit type, media type and interface type are provided.

14.6.3.7.2 Additional Information

The customer may request that the demarcation of optical fiber circuits be provisioned in the MDA rather than in the entrance room to ensure that service provision performance requirements and onward circuit distance restrictions are not exceeded.

In a high-density fiber environment, access providers should consider installing free-standing frames such as two-post frames.

14.7 Telecommunications Cabling Pathways

14.7.1 General

14.7.1.1 Requirements

Except where otherwise specified, data center cabling pathways shall adhere to the specifications of relevant cabling and containment specifications such as TIA-569-C, CENELEC EN 50174-2, or ISO/IEC 14763-2.

Pathways shall be sized for full data center occupancy, including all anticipated expansions and planned applications.

The maximum depth of telecommunications cabling within a solid bottomed cabling pathway (e.g., cable tray, duct) shall not exceed 150 mm (6 in), regardless of the depth of the cable pathway.

For cabling pathway systems that do not contain a solid bottom, the maximum depth of installed cabling is determined by the spot loading and pressure it exerts on the support points of the pathway system. The height of the cable can be determined by using Equation 14-1 or 14-2, where L is the largest distance between support points in the specific cable pathway system and H is the resultant calculated allowed height of the cables.

For values of L as measure in millimeters (mm):

$$H (mm) = \frac{150}{1 + (L \times 0.0007)} \quad (14-1)$$

For values of L as measured in inches (in):

$$H (in) = \frac{152.4}{25.4 + (L \times 0.4516)} \quad (14-2)$$

Cable heights in these pathways shall not exceed this calculated value. For convenience, Table 14-5 summarizes the calculated results for common interval distances between supports.

Table 14-5 Maximum Cable Stacking Height in Cabling Pathways

<i>L</i> Distance between points of support (mm)	<i>H</i> Maximum stacking height in cable pathways (mm)	<i>L</i> Distance between points of support (in)	<i>H</i> Maximum stacking height in cable pathways (in)
0 mm	150.0 mm	0 in	6.00 in
100 mm	140.2 mm	4 in	5.60 in
150 mm	135.7 mm	6 in	5.42 in
250 mm	127.7 mm	12 in	4.94 in
500 mm	111.1 mm	24 in	4.21 in
750 mm	98.4 mm	36 in	3.66 in
1000 mm	88.2 mm	48 in	3.24 in
1500 mm	73.2 mm	60 in	2.90 in

Pathway systems shall be secured in accordance with AHJ, seismic requirements for the location, and the planned long-term loading. When access floor systems are used, any one of the following methods shall be permitted:

- Attachment to metal struts that are captured below the floor by two or more access floor stringers
- Attachment to metal struts below the access floor that are suitably attached to the permanent floor
- Attachment via threaded rod directly to the permanent floor
- Attachment to channel bases bolted to floor slab

Structured cabling shall not share space within a dedicated optical fiber raceway with optical fiber equipment cords and patch cords.

14.7.1.2 Recommendations

Where it is not possible to adequately size pathways for full data center occupancy, including future expansions and applications, consider other media (such as optical fiber) or different network architectures (such as distributed LAN and SAN switching) to reduce cabling requirements.

In locations where seismic activity could create a potential risk, telecommunications pathways should be braced per AHJ and applicable standards (see Section 8).

There should be separate raceways or a divider in the raceway to separate balanced twisted-pair and optical fiber cabling.

Optical fiber equipment cords and patch cords should be installed in a dedicated optical fiber pathway that ensures that proper bend radius control is maintained throughout the installation.

Where it is not practical to separate optical fiber and balanced twisted-pair cabling, optical fiber cabling should be on top of, rather than underneath, balanced twisted-pair cabling.

Optical fiber cabling should not touch the slab or lay on top of the access floor when it exits a cable tray.

Cabling and cabling pathways should be installed overhead if ceiling heights permit.

All telecommunications cabling under the access floor should be installed in a cabling pathway that is listed or classified by a nationally recognized testing laboratory (NRTL). In the equipment cabinet aisles, allocate separate aisles for power and telecommunications cabling. Telecommunications cabling should be in the hot aisles (the aisles at the rear of the cabinets) and the power cabling should be in the cold aisles (the aisles at the front of the cabinets). Placing the telecommunications cabling in the cold aisles is not recommended as the telecommunications raceways may block airflow to perforated tiles, which should be located in the cold aisles.

14.7.2 Security

14.7.2.1 Requirements

Telecommunications cabling for data centers shall not be routed through spaces accessible by the public or by other tenants of the building unless the cables are in enclosed conduit or other secure pathways.

14.7.2.2 Recommendations

Physical access to cabling infrastructure should be limited strictly to data center cabling engineers and access provider personnel (under data center supervision) on a strictly need-to-access basis.

Any maintenance holes or hand holes on the data center property should have a lock or other means to prevent unauthorized access.

14.7.3 Separation of Power and Telecommunications Cabling

14.7.3.1 Requirements

To minimize coupling between power cabling and balanced twisted-pair cabling, the separation and segregation between power cabling and balanced twisted-pair cabling shall follow the requirements specified by the AHJ and defined in the cabling and pathways standards being followed.

AHJ may require a barrier or greater separation than specified in the cabling and pathways standards.

Where they are used, metallic cabling pathways shall be properly bonded and grounded as per AHJ requirements and applicable standards (e.g., NECA/BICSI-607, TIA-607-B).

14.7.3.2 Recommendations

For computer rooms that use the space under access floor systems for the routing of power and balanced twisted-pair cabling, allocate separate aisles for power and telecommunications cabling whenever possible. Where it is not possible to allocate separate aisles for power cabling and telecommunications cabling in the main aisles, then provide both horizontal and vertical separation of power cabling and telecommunications cabling in the same aisles. Provide horizontal separation by allocating different rows of tiles in the main aisles for power cabling and telecommunications cabling with the power cabling and telecommunications cabling as far apart from each other as possible. Additionally, vertical separation should be provided by placing the telecommunications cabling in cable trays (e.g., wire basket tray) as far above the power cables as possible with the top of the cable tray no less than 50 mm (2 in) below the bottom of the access floor tile.

14.7.3.3 Additional Information

There are no requirements for separation of power and telecommunications cabling crossing at right angles, except the separation requirements mandated by applicable electrical codes.

Refer to applicable cabling standards (e.g., ISO/IEC 14763-2, CENELEC 50174-2, TIA-942-A) regarding requirements for separation of power and telecommunications cabling.

The performance of a cabling pathway system is dependent on its proper installation, including supports and cabling. Neglecting installation and maintenance guidelines could lead to personal injury as well as damage to property.

14.7.4 Cable Tray Support Systems

14.7.4.1 General Requirements

When routing telecommunications cabling from a cabling pathway to entry into cabinets or frames or when changing between levels of cabling pathways, the cabling shall be managed to maintain their minimum bend radius requirements and be protected from damage or compression when crossing any edge of the cabling pathway system.

Cable ladders and cable tray shall be installed per manufacturers' recommendations.

Supports for the cable ladders and cable tray shall be independent from non-telecommunications utilities (e.g., ducts, conduits, plumbing, luminaries).

WARNING: Cable tray shall not be used as a walkway, ladder, or support for people unless the tray is specifically designed for such use.

14.7.4.2 Overhead Cable Trays

14.7.4.2.1 Requirements

In data centers that use overhead pathways, 150 mm (6 in) minimum access headroom shall be provided from the top of the pathway to the obstruction located above such as another pathway or the ceiling. This clearance requirement does not apply where cable trays cross each other or cross beams, pipes or other building structures.

Typical cable tray types for overhead cable installation include wire basket cable tray, ladder type, or center spine cable tray. Adjacent sections of metallic cable tray shall be bonded together and grounded per manufacturers' guidelines, /NECA/BICSI 607, other applicable standards (e.g., TIA-607-B), and AHJ (e.g., NFPA 70) and shall be listed or classified by a NRTL for this purpose. The metallic cable tray system shall be bonded to the data center common bonding network.

When they are supported from above, overhead cable ladders or trays (if used) shall be suspended from the structure above utilizing M12 (0.5 in) or greater threaded rods as required for structural support. Alternatively, the cable trays or ladders may be supported by an overhead support structure using support pillars or a suspended frame designed to support the load of the cable tray and cables.

If used for seismic bracing, ladder racks and cable tray shall be continuous wall to wall to form a brace for the equipment.

Cable tray shall not be routed directly below fire suppression or sprinkler systems.

14.7.4.2.2 Recommendations

In data centers that use overhead pathways, 300 mm (12 in) minimum access headroom should be provided from the top of the pathway to the obstruction located above such as another pathway or the ceiling.

Overhead cabling improves cooling efficiency and is a best practice where ceiling heights permit because it can substantially reduce losses because of supply airflow obstruction and turbulence caused by underfloor cabling and cabling pathways. Other potential advantages of overhead cable tray systems include elimination of access floor, separation of telecommunications cabling from power cabling and plumbing, flood survival, and improved access to cabling. Methods can include ladder racks or cable trays. Care must be taken in the placement of overhead cabling to ensure that return air flow is not obstructed. (See also Section 10.6).

Overhead cable trays may be installed in several layers to provide additional capacity. An installation may include two or three layers of cable trays, one for power cabling and one or two for telecommunications cabling. These overhead cable trays may be supplemented by a duct or tray system for optical fiber equipment cords or patch cords and if there is no access floor system, by brackets for the computer room bonding network.

In aisles and other common spaces in colocation facilities and other shared tenant data centers, overhead cable trays should be protected by one of the following means:

- Solid bottoms and covers
- Height at least 2.7 m (9 ft) above the finished floor to limit accessibility
- Protected through alternate means from accidental and intentional damage

When choosing between supporting cable trays from overhead or from below, overhead suspension is preferred as suspended cable trays provide more flexibility when adding or removing cabinets and racks of varying heights. However, suspended cable trays may require a dedicated support infrastructure and additional planning to preserve the structural integrity of the ceiling. Mechanically fastening cable trays directly to cabinets or racks offers a more compact design that does not affect the structural integrity of the ceiling. However, this method is only suitable if cabinets and racks to which these cable trays are attached will remain throughout the life of the computer room and it is certain that no equipment, cabinets, or racks taller than those to which the cable trays are attached will be needed.

14.7.4.3 Underfloor Cable Trays

14.7.4.3.1 Requirements

When telecommunications cabling is installed under the access floor, it shall be installed in cabling pathways that have no sharp edges that can potentially damage cables.

If the underfloor cable tray attaches to the access floor pedestals or stringers, the loading and attachment method shall comply with the floor manufacturer's specifications.

Clearance from the bottom of the access floor tile to the top of the cable tray or other raceway shall be at least 50 mm (2 in) to permit cable bundles and innerduct to exit out the top of the tray without incurring damage.

Metallic cable trays utilized in underfloor applications shall be listed or classified by an applicable NRTL. Adjacent sections of metallic cable tray shall be mechanically bonded together and provide electrical continuity and conductivity. Metallic cable trays shall be bonded to the data center's common bonding network.

The maximum depth of telecommunications cabling in the cable tray shall not exceed 150 mm (6 in) regardless of the depth of the cable tray.

14.7.4.3.2 Recommendations

The underfloor cable trays may be installed in multiple layers to provide additional capacity. Typical installations include two or three layers of cable trays, one for power cabling, and one or two for telecommunications cabling. These underfloor cable trays may be supplemented by a duct or tray system to manage optical fiber jumpers, patch cords, and equipment cords. There should be 300 mm (12 in) and no less than 150 mm (6 in) clearance between layers of underfloor cable trays run in parallel and stacked directly above each other.

14.7.4.4 Coordination of Cable Tray Routes

14.7.4.4.1 Recommendations

Planning of overhead cable trays for telecommunications cabling should be coordinated with architects, mechanical engineers, electrical engineers, and plumbing and structural engineers that are designing luminaires, plumbing, HVAC, power, and fire protection systems. Coordination should consider routing, clearances, and accessibility; consider use of three-dimensional drawings to simplify coordination.

Lighting fixtures (luminaires) and sprinkler heads should be placed between cable trays, not directly above cable trays.

Underfloor cable tray routing should be coordinated with other underfloor systems during the planning stages of the building.

14.7.4.5 Underfloor Foam Mats

14.7.4.5.1 Requirements

Where foam matting is used as an underfloor pathway or containment, the foam matting shall be secured to prevent lifting where low or no cables are present and to prevent disturbance of the underfloor airflow.

Foam matting shall also comply with the fire performance requirements for the space it occupies.

14.7.4.5.2 Recommendations

Where foam matting is used as an underfloor pathway or containment, it should be a minimum of 13 mm (0.5 in) thick and fill the aisle between the floor pedestals.

14.8 Backbone Cabling

14.8.1 Introduction

The function of the backbone cabling is to provide connections between the MDA, IDA, HDA, and entrance rooms in the data center cabling system.

Backbone cabling consists of the backbone cables, MC/MD, IC/ID, mechanical terminations, equipment cords, and patch cords or jumpers used for backbone-to-backbone cross-connection.

The backbone cabling is expected to serve the needs of the data center occupants for one or several planning phases, each phase spanning a time scale that may span days, months, or years. During each planning period, the backbone cabling design should accommodate growth and changes in service requirements without the installation of additional cabling. The length of the planning period is ultimately dependent on the design logistics, including material procurement, transportation, and installation and specification control.

14.8.2 General Requirements

The backbone cabling shall allow network reconfiguration and future growth without disturbance of the backbone cabling.

14.8.3 General Recommendations

The backbone cabling should support different connectivity requirements, including both the network and physical console connectivity such as local area networks, wide area networks, storage area networks, computer channels, and equipment console connections.

14.8.4 Cabling Types

14.8.4.1 Introduction

Cabling specified by this standard is applicable to different application requirements within the data center environment. Depending upon the characteristics of the individual application, choices with respect to transmission media should be made. In making this choice, factors to be considered include:

- Flexibility with respect to supported services
- Required useful life of cabling
- Computer room size
- Type and quantity of systems supported
- Channel capacity (transmission performance characteristics) within the cabling system
- Equipment vendor recommendations or specifications

14.8.4.2 Requirements

Each recognized cable has individual characteristics that make it suitable for a range of applications defined against each category or cabling type in the applicable cabling standards. A single cable may not satisfy all end user requirements. It may be necessary to use more than one medium in the backbone cabling. In those instances, the different media shall use the same facility architecture with the same location for cross-connects, mechanical terminations, and interbuilding entrance facilities.

As a result of the wide range of services and site sizes where backbone cabling will be used, more than one transmission medium is recognized. This standard specifies the transmission media that shall be used individually or in combination in the backbone cabling.

Recognized cables, associated connecting hardware, jumpers, patch cords, equipment cords, and zone area cords shall meet all applicable requirements specified in applicable standards and related addenda (e.g., ISO/IEC 11801, TIA-568-series).

Backbone cabling shall consist of one or more of the following media types:

- 100-ohm balanced twisted-pair Category 3/Class C minimum, (Category 6/Class E or higher recommended)
- OM3 multimode optical fiber cable minimum, (OM4 multimode optical fiber cable recommended)
- OS1 or OS2, single-mode optical fiber cable
- 75-ohm coaxial cabling (Telcordia GR-139-CORE 734-type and 735-type)

NOTE:

1. 734-type and 735-type 75-ohm coaxial cables as specified in Telcordia GR-139-CORE are permitted for E-1, E-3, and T-3 circuits.
2. If specific applications require other types of cabling (e.g., Infiniband cabling, TIA-232, V.35, SCSI), the other types may be installed in addition to the cabling listed above. Transmission performance compliance with applicable standards shall apply to local requirements.
3. To determine the suitability of the cabling types listed above for specific applications, systems suppliers, equipment manufacturers, and systems integrators should be consulted.

14.8.5 Redundant Backbone Cabling

14.8.5.1 Introduction

Redundant backbone cabling protects against an outage caused by damage to the primary backbone cabling. Redundant backbone cabling may be provided in several ways, depending on the degree of protection desired.

14.8.5.2 Recommendations

Backbone cabling between two spaces (e.g., a horizontal distribution area and a main distribution area) can be provided by running two cabling channels between these spaces, preferably along different routes. If the computer room has two main distribution areas, redundant backbone cabling to the horizontal distribution area may not be necessary although the routing of cabling to the two main distribution areas should follow different routes.

Some degree of redundancy can also be provided by installing backbone cabling between horizontal distribution areas. If the backbone cabling from the main distribution area to the horizontal distribution area is damaged, connections can be patched through another horizontal distribution area.

14.8.6 Backbone Cabling Length Limitations

14.8.6.1 Introduction

The supportable backbone cabling topologies for the media types recognized in this standard are application and media dependent. Refer to applicable standards for additional information regarding optical fiber and balanced twisted-pair cabling design considerations, including recommended distances and allowable maximum channel insertion loss based on the application's requirements.

Applications with data rates equal to or greater than 1 Gb/s should be reviewed in detail to assess support over existing cabling as well as the design for new cabling. For optical fiber, when designing individual optical fiber links or assessing existing cabling, the maximum allowable channel insertion loss for each application must be considered. For balanced twisted-pair cabling, application distances can be constrained by the cabling category.

The compilation of application information detailed in applicable standards (e.g., TIA-568-C.0, EN 50173-5, ISO/IEC 11801) provide the basic information to make informed decisions about optical fiber and balanced twisted-pair cabling usage and system design.

Interconnections between the individual areas, which are outside the scope of this standard, may be accomplished by employing equipment and technologies normally used for wide area applications.

14.8.6.2 Requirements

In data centers that use longer balanced twisted-pair equipment cords and patch cords, the backbone cabling distances shall be designed to accommodate the maximum cordage length so that when configuring channels for use with applications the combination of equipment cord, permanent link and patch cords never exceeds the channel loss limits.

14.8.6.3 Recommendations

Users of this standard are advised to consult the specific standards associated with the planned service or equipment manufacturers and systems integrators to determine the suitability of the cabling described herein for specific applications.

For balanced twisted-pair cabling, to reduce the effect of multiple connections in close proximity on NEXT loss and return loss, cabling system manufacturers' guidance should be sought on their recommendations for the minimum distance between connection points in a channel. Without that guidance, the backbone cabling lengths should be at least 15 m (50 ft).

14.8.7 Centralized Optical Fiber Cabling

14.8.7.1 Introduction

Many users of data networks implement their network architecture with centralized electronics versus distributed electronics in the computer room.

Centralized cabling provides connections from EDAs to centralized cross-connects by allowing the use of pull-through cabling, interconnection, or splices in the HDA and IDA.

Centralized optical fiber topologies permit the intermediate distribution areas and horizontal distribution areas to have no switches.

An example of centralized optical fiber cabling is shown in Figure 14-8.

14.8.7.2 General Requirements

The administration of moves, adds, and changes for centralized optical fiber cabling shall be performed at the centralized cross-connect. Centralized cabling design shall allow for migration (in part or in total) of the pull-through, interconnect, or splice implementation to a cross-connection implementation.

Centralized cabling design shall allow for the addition and removal of horizontal and backbone optical fiber cabling. Sufficient space shall be left in the HDA and IDA to allow for the addition of patch panels needed for the migration of the pull-through, interconnect, or splice to a cross-connection.

Sufficient cable slack shall exist in the HDA and IDA to allow movement of the cables when migrating to a cross-connection. Cable slack storage shall provide cable bend radius control so that optical fiber cable bend radius limitations are not violated. Optical fiber cable slack shall be stored in protective enclosures.

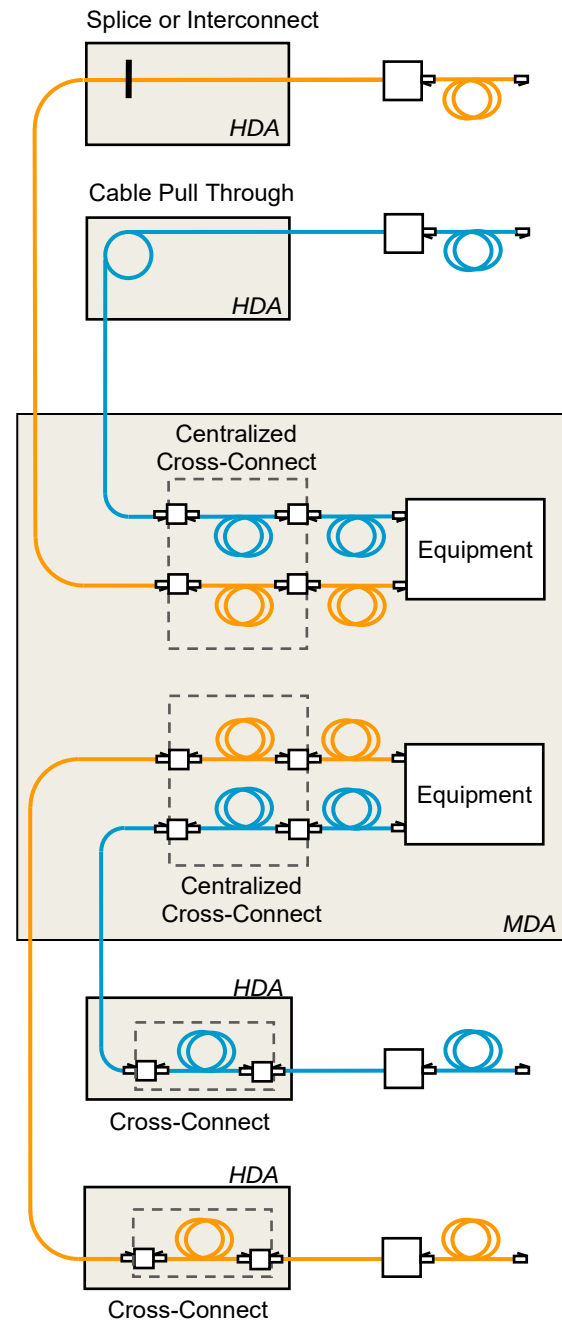


Figure 14-8
Centralized Optical Fiber Cabling Example

14.8.7.3 General Recommendations

Cable slack may be stored as jacketed cable or unjacketed optical fiber (buffered or coated). The layout of the termination hardware should accommodate modular growth in an orderly manner.

14.8.7.4 Centralized Optical Fiber Length Limitations

Centralized cabling implementations shall consider the length limitations of current and expected future protocols, particularly for multimode optical fiber.

NOTE: Future applications may increase demands on the bandwidth performance from the optical fiber and reduce the operational channel distance.

14.8.7.5 Centralized Cabling Implementation

14.8.7.5.1 Requirements

Centralized cabling design shall allow for migration (in part or in total) of the pull-through (continuous sheath cables), interconnect, or splice implementation to a cross-connection implementation or configuration utilizing equipment (e.g., switches) in the distributors. Centralized cabling shall support the administration and labeling requirements of the cabling standards being followed. Administration of moves and changes shall be performed at the centralized cross-connect. In addition, computer room splice and interconnect hardware shall be labeled with unique identifiers on each termination position. Polarity shall adhere to the requirements of the cabling standards being followed. Service loop storage shall provide bend radius control so that optical fiber bend radius limitations are not violated.

14.8.7.5.2 Recommendations

The computer room backbone subsystem should be designed with sufficient spare circuit capacity to service network equipment needs from the centralized cross-connect without the need to pull additional computer room backbone cables. The computer room backbone optical fiber strand count should be sized to deliver present and future loading to the maximum expected equipment density within the area served by the computer room. Generally, a minimum of two optical fiber strands are required for each network connection device served by the optical fiber cabling system. Service loops for migration to cross-connect or distributed equipment configurations may be stored as jacketed cable or unjacketed fiber (buffered or coated).

14.9 Horizontal Cabling

14.9.1 Introduction

The horizontal cabling is the portion of the telecommunications cabling system that extends from the equipment outlet (EO) in the EDA to the TIA HC or ISO/CENELEC ZD in an HDA, IDA, or MDA.

The horizontal cabling includes:

- Horizontal cables
- Mechanical terminations
- Equipment cords, patch cords, or jumpers;
- TIA zone outlet, TIA consolidation point (CP), or ISO/CENELEC local distribution point (LDP) in the optional ZDA

14.9.2 Cabling Types

14.9.2.1 Requirements

Because of the wide range of services and site sizes where horizontal cabling will be used, more than one transmission medium is recognized. This standard specifies transmission media, which shall be used individually or in combination in the horizontal cabling.

Recognized cabling, associated connecting hardware, jumpers, patch cords, and equipment cords shall meet all applicable requirements specified in applicable standards and related addenda (e.g., ISO/IEC 11801, TIA-568-series).

Horizontal cabling shall consist of one or more of the following media types:

- 4-pair 100-ohm balanced twisted-pair Category 6/Class E minimum (Category 6A/Class E_A or higher recommended)
- OM3 multimode optical fiber cable minimum (OM4 multimode optical fiber cable recommended where horizontal fiber cabling lengths exceed 70 m [230 ft])
- OS1 or OS2, single-mode optical fiber cable

NOTE:

1. Category 5e/Class D cabling may be used in an existing data center that already utilizes Category 5e/Class D cabling.
2. 734-type and 735-type 75-ohm coaxial cables as specified in Telcordia GR-139-CORE are permitted for E-1, E-3, and T-3 circuits.
3. If specific applications require other types of cabling (e.g., Infiniband cabling, TIA-232, V.35, SCSI), the other types may be installed in addition to the cabling listed above. Transmission performance compliance with applicable standards shall apply to local requirements.
4. To determine the suitability of the cabling types listed above for specific applications, systems suppliers, equipment manufacturers, and systems integrators should be consulted.

14.9.3 Redundant Horizontal Cabling

14.9.3.1 Recommendations

Horizontal cabling to critical systems should be diversely routed to improve resilience. Care should be taken not to exceed maximum horizontal cabling lengths when selecting cabling pathways. Critical systems can be supported by two different horizontal distribution areas as long as maximum cabling length limitations are not exceeded. This degree of redundancy may not provide much more resilience than diversely routing the horizontal cabling if the two horizontal distribution areas are in the same fire protection zone.

14.9.4 Balanced Twisted-Pair Cabling

14.9.4.1 Introduction

Balanced twisted-pair cabling performance is described using a scale based on classes or categories, as defined by ISO/IEC and TIA, respectively. While Category 3/Class C is the minimum acceptable performance for backbone cabling, Category 6/Class E is the minimum requirement in TIA-942-A and CENELEC EN 50173-5 for horizontal cabling, and Category 6A/Class E_A is the minimum requirement as listed in ISO/IEC 24764.

Table 14-6 is based on the minimum cabling channel performance requirements of specific balanced twisted-pair cabling.

14.9.4.2 Recommendations

Category 6A/Class E_A is the minimum performance level recommended for balanced twisted-pair cabling in a data center with the exception of network access cabling to the external network interface (ENI) located in telecommunications entrance rooms.

14.9.4.3 Balanced Twisted-Pair Cabling Supportable Distances

Maximum supportable distances for applications using balanced twisted-pair cabling can be found in the cabling standards being followed (e.g., ISO/IEC 11801, CENELEC EN 50173-5, TIA-568-C.0).

14.9.5 Optical Fiber Cabling

14.9.5.1 Introduction

There are four classes of multimode optical fiber cabling (OM1, OM2, OM3, and OM4) and two classes of single-mode optical fiber cabling (OS1 and OS2). Table 14-7 shows the minimum bandwidth or optical performance for each optical fiber cable by type.

14.9.5.2 Requirements

OS1 single-mode and OM3 multimode cable are the minimum performance optical fiber types specified in this standard.

14.9.5.3 Recommendations

OM4 multimode optical fiber is recommended to support 100 Gbps Ethernet, particularly the 4-lane implementation. Multimode optical fiber should be terminated with MPO connectors where 40G and 100G Ethernet is expected to be supported initially or in the future (e.g., backbone cabling between distributors, top of rack switches, and high performance servers).

Table 14-6 Balanced Twisted-Pair Cabling Channel Performance

<i>CENELEC and ISO classes/categories¹</i>	<i>TIA categories</i>	<i>Frequency characterization</i>
Class D/Category 5	Category 5e	100 MHz
Class E/Category 6	Category 6	250 MHz
Class E _A /Category 6A	Augmented Category 6	500 MHz
Class F/Category 7	n/a ²	600 MHz
Class F _A /Category 7 _A	n/a ²	1000 MHz
Class I/Category 8.1 ³	Category 8 ³	2000 MHz
Class II/Category 8.2 ³	Category 8 ³	2000 MHz

NOTE 1: Component performance is indicated by the term “Category”, with system performance indicated by the term “Class”.

NOTE 2: TIA does not define an equivalent.

NOTE 3: Category 8 cabling is not ratified at time of publication of this document, but it is designed primarily for data center use; therefore, it may not allow the same configurations and distances as previous categories.

Table 14-7 Optical Fiber Cable Performance By Type

<i>Classification</i>	<i>Optical Fiber Type</i>	<i>Performance</i>
OM1 ¹	62.5/125 µm multimode	Minimum overfilled launch bandwidth of 200 and 500 MHz•km at 850 and 1300 nm, respectively
OM2 ¹	50/125 µm multimode 62.5/125 µm multimode	Minimum overfilled launch bandwidth of 500 and 500 MHz•km at 850 and 1300 nm, respectively
OM3	50/125 µm 850 nm laser-optimized	Minimum overfilled launch bandwidth of 1500 and 500 MHz•km at 850 and 1300 nm, respectively and an effective modal bandwidth of 2000 MHz•km at 850 nm using a restricted mode launch (e.g., vertical cavity surface emitting laser [VCSEL])
OM4	50/125 µm 850 nm laser-optimized	Minimum overfilled launch bandwidth of 3500 and 500 MHz•km at 850 and 1300 nm, respectively and an effective modal bandwidth of 4700 MHz•km at 850 nm using a restricted mode launch (e.g., VCSEL)
OS1	Single-mode	Minimum bandwidth of single-mode optical fiber cable is not characterized in the same manner as multimode. Loss characterization is 1.0 dB per km at 1310 nm and 1550 nm for indoor and 0.5 dB per km at 1310 nm and 1550 nm for outdoor.
OS2	Single-mode	Minimum bandwidth of single-mode optical fiber cable is not characterized in the same manner as multimode. Loss characterization is 0.4 dB per km at 1310 nm, 1383 nm, and 1550 nm for both indoor and outdoor. OS2 fiber is optimized for performance at the 1383 nm window (and is defined in ITU-G652.D).

NOTE: OM1 and OM 2 are not recognized for use in data centers and are included here only for completeness.

14.9.5.4 Component Channel Method Versus Application Based Method

There are two methods used for the design and implementation of optical fiber cabling solutions: component channel method and application-based method.

14.9.5.4.1 Component Channel Method

Traditionally, the component method has been used to design and assemble optical fiber cabling solutions without detailed consideration for the applications that eventually will run over the optical fiber cabling channel. This lack of coordination can result in many discussions and disagreements between designers, installers, and operations staff over who is responsible for what when the network equipment is discovered to be inoperable.

Knowledge of the applications to be supported is critical to the effective delivery and future proofing of the optical fiber cabling infrastructure. The designer should first determine what applications are required, the type of connectors, the bandwidth performance, and optical fiber cabling type. The designer should then relate this to the optical performance charts and tables in the cabling standards being followed. The designer can then obtain the maximum permitted loss per optical fiber type and maximum distance over which the application can be supported. Selection and assembly of components is concluded on an accumulated loss basis; the resulting performance is measured against the whole channel and does not identify or acknowledge a worst individual event or component loss figure.

This approach can be used to the designer's and operator's advantage when considering the use of more than two connectors or connectors that experience greater signal losses over a shorter channel distance. It effectively converts bandwidth gains into connector loss. Most manufacturers will not recommend or support more than six connectors (three mated pairs of connectors, not including the connectors at the equipment and not including splices) in a multimode or single-mode optical fiber cabling channel because of the resulting cumulative system attenuation.

The demands from the latest and next generation high-speed applications have considerable distance limiting aspects. The applications can only be expected to operate effectively when the balance of media choice, distance, bandwidth, and component loss are all within the prescribed parameters for each application to be supported.

14.9.5.4.2 Application-Based Method

If the applications to be deployed are known, the data center cabling designer can get detailed information about channel losses and maximum channel distance supported for each optical fiber media type from the cabling standards being followed. Dedicated home run optical fiber cabling solutions can be configured from approved component sets.

14.9.5.5 Optical Fiber Cabling Supportable Distances

Maximum supportable distances and maximum channel attenuation for applications using optical fiber cabling can be found in applicable standards (e.g., TIA-568-C.0, ISO/IEC 11801, CENELEC EN 50173-1). Application tables in these standards are based on the minimum performance requirements for OM1–OM4 classifications of multimode fiber and OS1–OS2 single-mode fiber.

14.9.5.6 Single-Mode and Multimode Connector Color Recommendations

The single-mode connector or a visible portion of it should be blue in color, referring to a flat-polished optical fiber endface; the color green should signify a connector featuring an angle polished optical fiber endface. Where a mixture of OS1 and OS2 exist in a single data center space or room, additional identification should be applied to clearly identify the fiber type used.

The multimode connector or a visible portion of it should be:

- Beige for an OM1, 62.5 μm connector (not recognized in standard)
- Black for an OM2, 50 μm connector (not recognized in standard)
- Aqua for an OM3 or OM4, 50 μm laser-optimized connector

Where a mixture of OM3 and OM4 exist in a single data center space or room, additional identification should be applied to clearly identify the fiber type used.

Adapter housing color should represent the cabling performance of the installed permanent fiber using the connector color scheme above.

14.9.6 Shared Sheath Guidelines

14.9.6.1 Introduction

Shared sheath guidelines described in this section are not intended to cover all system designs and installations. It is recommended that the user consult with equipment manufacturers, applications standards, and system providers for additional information.

In general, applications using no common frequencies tend not to interfere with each another. A good example of this is mixing analog voice and digital data signals within the same cable sheath. In a single balanced twisted-pair cable, multiple applications of the same type may operate on different twisted pairs simultaneously without any problems.

14.9.6.2 Recommendations

The designer and installer should follow the recommendations for shared sheath implementation described in the cabling standards being followed.

14.9.6.3 Hybrid and Bundled Cable Assembly Applications

14.9.6.3.1 Introduction

Hybrid and bundled cable assemblies are used to group multiple individual cables together to form a single cable unit routed along a common path. These individual cables may be of the same or different types (e.g., optical fiber cabling and balanced twisted-pair cabling) or of the same or different categories (e.g., Category 6A/Class E_A cabling with Category 6/Class E cabling).

Hybrid cable assemblies are manufactured in a factory whereas bundled cable assemblies may be assembled either in a factory, at a third-party facility, or on site by the installer.

NOTE: Bundled cables are sometimes referred to as loomed, speed-wrap, or whip cable assemblies.

14.9.6.3.2 Requirements

When bundled and hybrid cables are used for horizontal cabling, each cable type shall be recognized and meet the transmission (e.g., recognized categories/classes) and color-code specifications (e.g., 4-pair color-code groupings) for that cable type. Additionally, hybrid or bundled cable assemblies shall meet the hybrid or bundled cable assembly requirements of applicable standards (e.g., ISO/IEC 11801, TIA-568-series, CENELEC EN 50173-1). These requirements apply to hybrid cables and bundled cables assembled prior to installation.

Hybrid and bundled cable assemblies may be installed either as cable or as preconnectorized assemblies. These assemblies, known as trunk cable assemblies, may be pre-connectorized on one or both ends. When used, these hybrid and bundled trunk assemblies are required to meet the hybrid and bundled transmission performance requirements of applicable standards (e.g., ISO/IEC 11801, TIA-568-series, CENELEC EN 50173-1).

14.9.6.3.3 Recommendations

There are a number of other types of horizontal cabling that have not been defined in this standard, yet they may be effective for specific applications. Although these other types of horizontal cabling are not part of the requirements of this standard, they may be used in addition to the best practices offered by this standard.

14.9.6.4 Trunk Cabling Assemblies

14.9.6.4.1 Introduction

Trunk cabling assemblies consist of two or more preconnectorized cabling links of the same or different types or categories that may either be covered by one overall sheath or a collection of individual cable units, which are bound together to form a single trunk unit. Trunk cabling assemblies are capable of supporting multiple devices. A trunk cabling assembly may be terminated at one end or both ends with connectors. Trunk cabling assemblies may be a convenient and economical alternative to installing a number of individual cables and then applying field termination techniques to connectorize the cables.

Balanced twisted-pair and optical fiber trunk cabling assemblies offer the following features, benefits, and disadvantages as shown in Table 14-8.

Table 14-8 Advantages and Disadvantages of Trunk Cabling Assemblies

<i>Feature/Benefit</i>	<i>Advantages</i>	<i>Disadvantages</i>
Quality controlled factory terminations	Yes	
Potentially reduced installation labor time	Yes	
Fewer cables improves cable management	Yes	
Less dependence on installer/technician skills and experience	Yes	
Requires a high degree of accuracy when ordering lengths to avoid mistakes		Yes
If a trunk cabling assembly is damaged, multiple cable units within the trunk cabling assembly may be adversely affected		Yes
Factory terminated optical fiber trunk cabling assemblies may yield better permanent link optical mated pair loss vs. field terminated connectors	Yes	
Trunk cabling assemblies may require larger bend radii than the equivalent individual cables		Yes

14.9.7 Horizontal Cabling Length Limitations

14.9.7.1 Introduction

The horizontal cabling length limitations are the cable lengths from the mechanical termination of the cabling at the TIA HC or ISO/IEC ZD in the HDA, IDA, or the MDA to the mechanical termination of the cabling on the EO in the EDA.

14.9.7.2 Requirements

For maximum and minimum cabling lengths, refer to the applicable cabling standards.

14.9.7.3 Recommendations

Horizontal cabling distances in a computer room may need to be reduced to compensate for longer equipment cords in the data center distribution areas. Therefore, careful considerations to the horizontal cabling distance should be made to ensure that cabling distances and transmission requirements are not exceeded when the equipment cords are attached.

NOTE: For balanced twisted-pair cabling, to reduce the effect of multiple connections in close proximity on NEXT loss and return loss and without further guidance from manufacturers, the zone distribution area termination should be located at least 15 m (50 ft) from the horizontal distribution area termination. Consult with the cabling system manufacturer about the minimum distances supported by the chosen product set. Their recommendations may reduce space needed to collect excess cable.

14.9.7.4 Balanced Twisted-Pair Cord Length Limitations

14.9.7.4.1 Introduction

Balanced twisted-pair equipment cords and patch cord assemblies may be constructed with either solid or stranded conductors. The insertion loss (attenuation) performance of stranded cables used in the assembly of these cords is greater than the attenuation of solid conductor cables. While a generic cabling system has a physical channel distance limitation of 100 m (328 ft), there is an assumption made that the combined length of equipment cords and patch cords at both ends of the cabling channel will not exceed 10 m (33 ft). If stranded conductor equipment cords and stranded conductor patch cords with a combined length of more than 10 m (33 ft) are used, refer to the applicable cabling standards for maximum cord lengths.

14.9.7.4.2 Requirements

Manufacturers shall be consulted to confirm the attenuation characteristics of their stranded cables, equipment cords, and patch cords to help ensure that the installed cabling channels will perform to the applicable cabling standards.

Balanced twisted-pair equipment cords used in the context of zone outlets in the ZDA shall meet the minimum performance requirements provided in the cabling standard being followed.

The zone outlet shall be marked with the maximum allowable zone area cable length. One method to accomplish this is to evaluate cable length markings.

- **14.9.7.5 Horizontal Cabling Applications**

14.9.7.5.1 Requirements

For optical fiber, when designing individual optical fiber links or assessing existing cabling, the maximum allowable channel insertion loss for each application shall be considered.

14.9.7.5.2 Recommendations

For optical fiber and balanced twisted-pair cabling, application distances can be constrained by the cabling category or type. The compilation of application information detailed in applicable standards (e.g., TIA-568-C.0, CENELEC EN 50173-5, ISO/IEC 11801) provide the basic information to make informed decisions about optical fiber and balanced twisted-pair cabling usage and system design.

14.10 Cabling Installation

14.10.1 General Requirements

Cabling shall be installed and dressed neatly, taking care to adhere to minimum cable bend radii for cables. Take particular care not to leave excess optical fiber loops on the floor or in places where they can be damaged.

14.10.2 Cable Management

14.10.2.1 Introduction

Performance of cable and connecting hardware may become degraded if initial installation and ongoing cable management recommendations are not followed. Installation and maintenance practices for the pulling and placing of horizontal and backbone cabling differs greatly from that of the associated interconnections and cross-connections.

14.10.2.2 Requirements

While all transmission parameters are sensitive to transmission discontinuities caused by connector terminations, return loss, and all forms of crosstalk (e.g., near-end crosstalk [NEXT], attenuation-to-crosstalk ratio–far end [ACR–F], previously known as ELFEXT), performance of balanced twisted-pair systems are particularly sensitive to conductor untwisting and other installation practices that disturb pair balance and cause impedance variations. To prevent these problems, the installer shall adhere to the following practices:

- Remove only as much cable jacket as is required for termination and trimming.
- Follow the manufacturer's instructions for mounting, termination, and cable management.
- Minimize the amount of untwisting in a pair as a result of termination to connecting hardware. For untwisting cabling, maintain pair twists as close as possible to the termination point; the amount of untwisting must not exceed 13 mm (0.5 in) for Category 5e and higher cables.

NOTE: This requirement is intended to minimize untwisting of cable pairs and the separation of conductors within a pair. It is not intended as a twist specification for cable or jumper construction.

For termination fields that require frequent access (e.g., cross-connects used for configuring a network), one way to control termination consistency is by using factory-assembled equipment cords, patch cords, and patch panels that meet the appropriate performance requirements. Jumpers can provide comparable performance, but typically require a higher skill level to implement changes.

14.10.2.3 Recommendations

Telecommunications cabling should be placed in cabling pathways (containment) that provide sufficient space for placement of the media. Consider the following methods of containment for telecommunications cabling installed in dedicated routes:

- Enclosed raceway distribution (e.g., conduit systems)
- Zone distribution (e.g., enclosures)
- Cable trays (e.g., open top systems)

CAUTION: Refer to appropriate codes, standards, and regulations for compliance with flame spread and smoke index properties of cabling used in cabling pathway systems.

Connecting hardware should only be installed in the access floor space when the connecting hardware is one of the following:

- A TIA CP, ISO/CELENEC LDP, or TIA zone outlet in a zone distribution area (ZDA)
- EO in equipment distribution area (EDA) or workstation
- Building automation systems (BAS) horizontal connection point (HCP)

Cross-connections are designed for flexibility to allow for moves, adds, and changes. The structured cabling system user is typically responsible for altering cross-connections to implement network changes. Skill levels among users vary and should be taken into consideration when designing, providing training on, and performing ongoing management of the cross-connection facility. The following guidelines should be followed for appropriate management practices.

In cabling pathways and telecommunications spaces, use appropriate cable routing and dressing fixtures to organize and effectively manage the different cable types. The cable management precautions that should be followed include:

- For suspended cabling, limit the span between supports to 1.5 m (5 ft) or less.
- Cable ties should be installed so as not to deform cables beyond manufacturers' tolerances.
- Avoid twisting the cable jacket during installation as this may affect transmission performance.
- For balanced twisted pair cable, use of random spacing between cable ties to avoid return loss resonances.

NOTE: Uniformly placing cable ties has been shown to produce return loss resonance. However, a recommended minimum variation in the distances between cable ties necessary to avoid this effect has not been published.

WARNING: Never use staples or staple fastening tools to fasten telecommunications cabling in a data center.

The following are cross-connect facility management precautions that should be observed:

- Eliminate or minimize equipment cord, patch cord, and jumper slack in the management field after each cross-connection is completed.
- In cross-connections utilizing balanced twisted-pair or optical fiber equipment cords or patch cords, bend radius can become difficult to control; it is important to achieve desired manageability without loss of performance in a cabling channel by controlling the equipment cord and patch cord bend radii.
- Horizontal cables should be terminated on connecting hardware that is the same performance (Category) or higher. The installed transmission performance of cabling where components of different performance category requirements are used shall be classified by the least-performing component.
- Because horizontal and backbone cables are always terminated on separate connectors, use patch cords or jumpers to make connections between horizontal cables and backbone cables.

14.10.3 Bend Radius and Pulling Tension Guidelines

14.10.3.1 Introduction

Pay strict attention to the manufacturer's guidelines on bend radii and maximum pulling tension during installation. Notice that the recommended minimum bend radius for a cable during installation may be greater than the recommended bend radius after the cable is installed. This is to minimize tension and deformation as the cables pass around corners during installation.

Cable bend radius requirements minimize the effects of bends on the transmission performance of installed cabling links. These requirements are distinct from the bend radius specifications for conduits.

14.10.3.2 General Recommendations

If multiple cable types are used in any route, use the largest bend radius specified among the cable types used.

Consult the manufacturer's specifications for the minimum bend radius during installation. The minimum bend radius utilized should be the greater of the manufacturers' specifications and the specifications provided in this standard.

14.10.3.3 Balanced Twisted-Pair Cabling Bend Radius and Pulling Tension Requirements

The maximum pull force best practices for balanced twisted-pair cabling shall be established by the cabling products manufacturer. Consult with the applicable cabling products manufacturer for such best practices. See Table 14-9.

14.10.3.4 Optical Fiber Cable Bend Radius and Pulling Tension Requirements

The maximum pull force best practices for optical fiber cabling shall be established by the cabling products manufacturer. Consult with the applicable cabling products manufacturer for such best practices. See Table 14-10.

14.10.4 Abandoned Cable

14.10.4.1 Introduction

For the purpose of this standard, abandoned cable is described as installed telecommunications cabling that is not terminated at both ends at a connector or other equipment and not identified for future use with some form of labeling.

14.10.4.2 Requirements

Remove abandoned cable as required by the AHJ.

14.10.4.3 Recommendations

It is considered a best practice to remove abandoned cable in the data center.

Table 14-9 Balanced Twisted-Pair Cable Bend Radius and Pulling Tension

<i>Cabling/Cord Types</i>	<i>Required Minimum Inside Bend Radius Under No Load (No Stress)</i>	<i>Required Minimum Bend Radius Under Load (Stress)</i>	<i>Recommended Maximum Tensile Load Under Load (Stress)</i>
4-pair, balanced twisted-pair patch/equip cord	Four times the cord cable's outside diameter	Four times the cord cable's outside diameter	Follow manufacturer specifications
4-pair, balanced twisted-pair cables	Four times the cable's outside diameter	Four times the cable's outside diameter	110 N (25 lbf)
Multipair balanced twisted-pair cables	Follow manufacturer specifications	Follow manufacturer specifications	Follow manufacturer specifications

Table 14-10 Optical Fiber Cable Bend Radius and Pulling Tension

<i>Cable Type and Installation Details</i>	<i>Maximum Tensile Load During Installation</i>	<i>Minimum Bend Radii While Subjected to:</i>	
		<i>Maximum Tensile Load (During Installation)</i>	<i>No Tensile Load (After Installation)</i>
Inside plant horizontal cable with 2 or 4 fibers	220 N (50 lbf)	50 mm (2 in)	25 mm (1 in)
Inside plant cable with more than 4 fibers	Per manufacturer	20-times the cable outside diameter	10-times the cable outside diameter
Indoor/outdoor cable with up to 12 fibers	1335 N (300 lbf)	20-times the cable outside diameter	10-times the cable outside diameter
Indoor/outdoor cable with more than 12 fibers	2670 N (600 lbf)	20-times the cable outside diameter	10-times the cable outside diameter
Outside plant cable	2670 N (600 lbf)	20-times the cable outside diameter	10-times the cable outside diameter
Drop cable installed by pulling	1335 N (300 lbf)	20-times the cable outside diameter	10-times the cable outside diameter
Drop cable installed by directly buried, trenched, or blown into ducts	440 N (100 lbf)	20-times the cable outside diameter	10-times the cable outside diameter

NOTE: Non-circular cable bend diameter requirements are to be determined using the minor axis as the cable diameter and bending in the direction of the preferential bend.

14.11 Field Testing Data Center Telecommunications Cabling

14.11.1 Introduction

Field testing is an effective method of evaluating the transmission performance of installed telecommunications cabling. The field test measurement results of installed balanced twisted-pair or optical fiber telecommunications cabling depend on several factors, including the:

- Transmission performance of cable
- Transmission performance of connecting hardware
- Transmission performance of equipment cords, patch cords, and cross-connect cabling
- Total number of connections
- Installation practices and expertise of the installers
- Maintenance techniques that are used

Field testing conducted on balanced twisted-pair and optical fiber cabling shall be conducted in accordance with specified standards.

NOTE: Refer to the list of standards provided in Section 3 and Appendix H of this standard.

This section provides requirements and recommendations regarding channel and permanent link field-testing, including:

- Installation conformance
- Specifications for field test instruments
- Field test measurement methods
- Interpretation of test results

14.11.2 Installation Conformance

14.11.2.1 Introduction

Installation conformance ensures that field test measurements have been completed in accordance with the terms and conditions of a contract.

14.11.2.2 Requirements

The installation contract shall include field test measurement requirements of the installed cabling to specific industry standards as well as to visually inspect the cabling. Performance field test measurement documentation of the installed cabling shall be provided to the building tenant, building owner or agent per contract requirements, or, in lieu of contract requirements, in the format delivered by the certification test instrument. Visual inspection of installed cabling is performed by observing the following:

- The condition, workmanship, and finish are satisfactory, including no obvious damage to the cable (e.g., bend radius, tearing, and separation from sources of EMI).
- The marking (labeling) is legible and placed according to specification.
- Mechanical damage is absent, and there is no undesired movement or displacement of parts.
- Flaking of materials or finishes is absent.

Installation conformance to visual inspection requires that a form be submitted, indicating that a visual inspection has been conducted and the form shall document the results of the visual inspection.

14.11.3 100-ohm Balanced Twisted-Pair Cabling Field Testing

14.11.3.1 Introduction

Certification of the balanced twisted-pair cabling determines whether the cabling meets expected performance requirements such as those specified in one or more of the following Categories/Classes of cabling:

- TIA Category 3 cabling
- ISO Class C cabling
- TIA Category 5e cabling
- ISO Class D cabling using ISO Category 5 components
- TIA Category 6 cabling
- ISO Class E cabling using ISO Category 6 components
- TIA Category 6A cabling
- ISO Class E_A cabling using ISO Category 6_A components
- ISO Class F cabling using ISO Category 7 components
- ISO Class F_A cabling using ISO Category 7_A components

NOTE: Existing ISO Class E and TIA Category 6 cabling may support IEEE 10GBASE-T at limited distances but will require additional testing and mitigation strategies to ascertain what is achievable. For additional details, see TIA TSB-155-A and ISO/IEC TR 24750.

14.11.3.2 Balanced Twisted-Pair Cabling Field Test Configuration

14.11.3.2.1 Permanent Link Requirements

The permanent link test configuration shall be used to certify the performance of the permanently installed balanced twisted-pair cabling.

NOTE: A passing permanent link associated with compliant patch cords always guarantees a compliant channel.

The permanent link shall include:

- Up to 90 m (295 ft) of horizontal cable
- A connection at each end of the horizontal cabling
- Optionally, a consolidation point (CP) or local distribution point (ISO/IEC and CENELEC equivalent of CP in ZDA)

The permanent link configuration excludes the cable portion of the field test instrument cord and the connection to the field test instrument. See Figure 14-9 for an example of a permanent link.

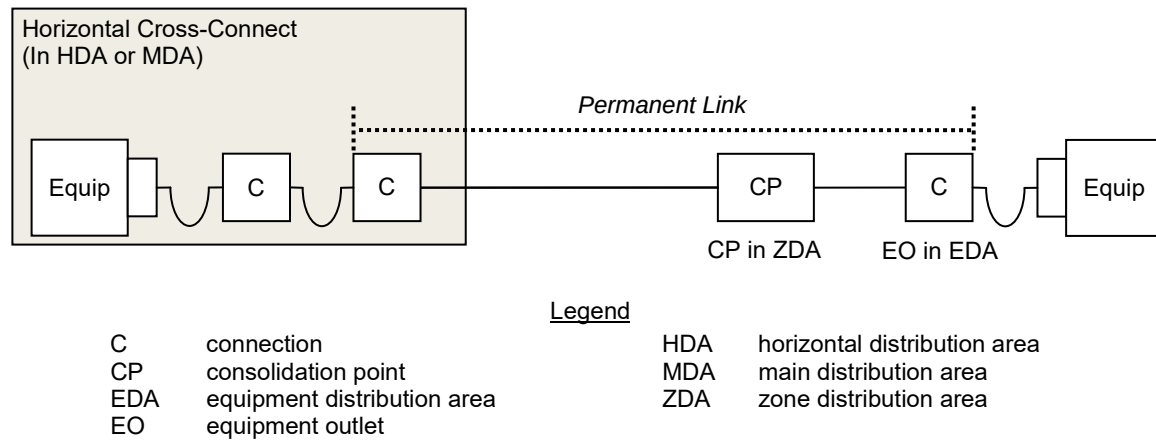


Figure 14-9
Permanent Link Example

14.11.3.2.2 Channel Requirements

If channel testing is performed, the channel test configuration shall be used to verify end-to-end channel performance of installed balanced twisted-pair cabling.

NOTE: This is generally used prior to connection of active equipment.

The channel includes:

- Horizontal cable
- Patch cords and equipment cords
- A telecommunications outlet/connector
- Optionally, a consolidation point (CP) or local distribution point (ISO/IEC and CENELEC equivalent of CP in ZDA)
- Up to two connections at the horizontal cross-connect

The channel configuration description does not apply to those cases where horizontal cabling is cross-connected to backbone cabling. See Figure 14-10 for an example of a channel.

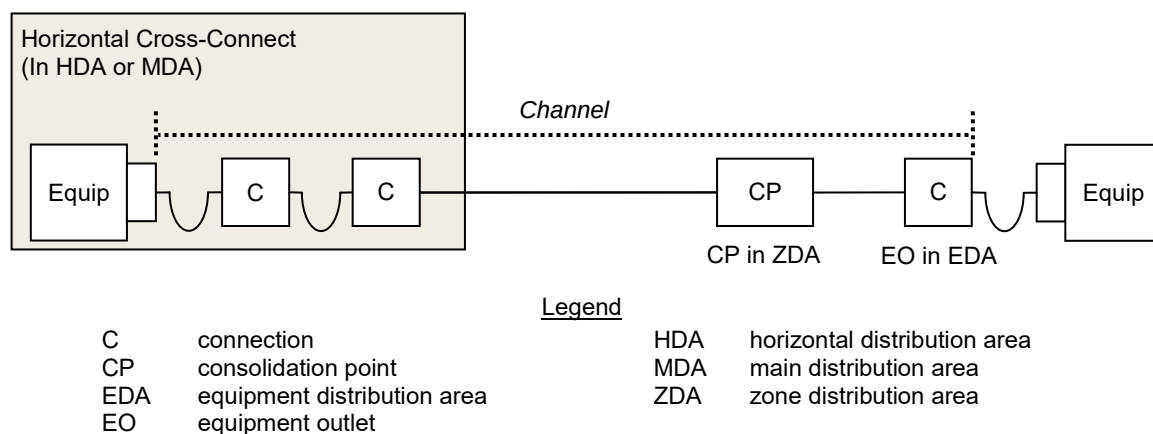


Figure 14-10
Channel Model Example

14.11.3.3 Balanced Twisted-Pair Cabling Field Test Parameters

14.11.3.3.1 Requirements

The field test parameters to be measured shall meet the requirements of the cabling standard being followed (e.g., TIA-1152, EN 50346). The field test instrument shall support all field test parameters specified by cabling standards.

A pass or fail result for each parameter shall be determined by the allowable limits for that parameter. The test result of a parameter shall be marked with an asterisk (*) when the result is closer to the test limit than the measurement accuracy.

Field test measurements shall be conducted at the temperature the cabling is intended to operate.

14.11.3.4 Balanced Twisted-Pair Cabling Field Test Instrument

14.11.3.4.1 Requirements

Field test instruments shall meet the accuracy requirements for the cabling Category or Class as defined in applicable standards (e.g., TIA-1152 or IEC 61935-1). Field test instruments shall:

- Be maintained following the equipment manufacturers guidelines.
- Have a valid calibration certificate, preferably from the equipment manufacturer.
- Be loaded with the latest revision of firmware and test limits.

Accuracy Level IIIe or higher (e.g., Level IV) field test instruments are required to measure the appropriate Category/Class of cabling to ensure accurate field test measurements. Table 14-11 provides information on the field testing configuration, frequency range, and minimum accuracy level of the test instrument for testing ISO Class E_A, TIA Category 6A, and higher Classes/Categories of cabling systems.

Field test results that are outside the uncertainty band of the field test instruments are reported as either “pass” or “fail.” Field test results that are inside the uncertainty band of the field test instruments are reported as either “*pass” or “*fail” as appropriate. Measurement results having an asterisk (*) shall be evaluated by the relevant cabling standard or as agreed upon in the contractual specification.

14.11.3.5 Balanced Twisted-Pair Field Test Connectors and Cords

14.11.3.5.1 Field Test Equipment Interfaces, Adapters, and Cords Requirements

Test equipment interfaces, adapters, and cords used as connecting hardware have a limited life cycle and shall be inspected periodically for wear. The field test equipment manufacturer shall provide information on the life cycle of these connectors. Test adapters, interfaces, and measurement quality test cords shall be replaced per manufacturer recommendations. Test adapters, interfaces, and cords shall meet the component requirements of the standards being followed.

Table 14-11 Balanced Twisted-Pair Field Testing

<i>Field Test Configurations</i>	<i>Frequency Range</i>	<i>Minimum Accuracy Level</i>
10GBASE-T Class E _A /Category 6A Permanent Link	1–500 MHz	IIIe
10GBASE-T Class E _A /Category 6A Channel	1–500 MHz	IIIe
Class F/Category 7 Permanent Link	1–600 MHz	IV
Class F/Category 7 Channel	1–600 MHz	IV
Class F _A /Category 7 _A Permanent Link	1–1000 MHz	IV
Class F _A /Category 7 _A Channel	1–1000 MHz	IV

14.11.3.5.2 User Cords Requirements

User cords are equipment cords, patch cords, or jumpers that are included as part of the channel. User cords shall be tested in place within a channel. A user cord may be verified by inserting the cord in the channel under test. If the channel conforms to the transmission requirements, the user cord may be approved for use in that channel only. The orientation of the user cords shall not be reversed.

14.11.3.6 Balanced Twisted-Pair Field Test Measurement Results

14.11.3.6.1 Requirements

Field test results shall be stored in the native format of the field test instrument. The measured results of all pairs shall be reported in graphical and table format with the specification limits shown on the graphs or in the table at the same frequencies as specified in the relevant cabling specifications. The reports shall explicitly note whether the measured results exceed the test limits. Additionally, the test results shall be carefully reviewed to ensure compliance to specified standards.

Any reconfiguration of cabling components after testing may change the performance, thereby invalidating previous test results. Such cabling shall require retesting to confirm conformance.

14.11.4 Optical Fiber Cabling Field Testing

14.11.4.1 General

14.11.4.1.1 Introduction

An optical fiber cabling link may consist of a fiber or concatenated fibers (spliced, cross-connected, or interconnected) with a connector or adapter on each end.

There are two approaches for establishing the limits against which to validate an optical fiber channel:

- Against the generic requirements set out in the cabling standard being followed for losses based on a predefined channel of a given distance
- Against the loss requirements for a specific optical fiber application

Factors that affect the attenuation measurements of installed and field tested optical fiber cabling include:

- Optical fiber type
- Link length
- Number and quality of terminations and splices
- Cable stresses
- Transmission wavelength

Link attenuation can be adversely influenced by:

- Severe cable bends
- Poorly installed connectors
- The presence of particulate matter (e.g., dirt or dust) on the endface of connectors

14.11.4.1.2 Requirements

Field testing optical fiber cabling shall be performed on length, optical attenuation, and polarity. An optical loss test set (OLTS), also referred to as a power meter and light source, shall be used to measure optical attenuation and length, if capable, and may be used to ensure correct polarity. An optical time domain reflectometer (OTDR) shall be used to characterize anomalies or damaged areas along the installed fiber and to evaluate uniformity of connections (connectors and splices). Optical fiber cabling field testing shall be conducted in accordance with the published standards for the cabling solution being used.

NOTE: A visible light source is a visible incandescent, LED or laser source used to trace fibers and may be used to verify polarity.

Measurement quality test cords and their connectors used for testing shall meet requirements for reference test cords (e.g., ISO/IEC 14763-3), which will provide accuracy and repeatability of the results obtained.

WARNING: All tests performed on optical fiber cabling that use a laser or light emitting diode (LED) in a test set are to be carried out with safety precautions in accordance with applicable standards (e.g., ANSI Z136.2).

14.11.4.1.3 Recommendations

An OTDR should be used to measure fiber length, reflectance, and optical return loss (ORL).

14.11.4.2 Optical Fiber Cabling Field Test Configuration**14.11.4.2.1 Introduction**

There are three test configurations available for use with an OLTS (see IEC 61280-4-1 and IEC 61280-4-2). These are:

- 1 jumper reference method
- 2 jumper reference method
- 3 jumper reference method

Used in conjunction with an OLTS, an optical fiber link may also be tested with an OTDR. This can be accomplished from one end of the fiber. However, a tail cord shall be placed at the far end of the link that is at least 100 m in length so that the far-end connector can be characterized.

14.11.4.2.2 Requirements

For multimode and single-mode cabling, the test jumper connectors and the connector ports under test shall be clean and free of damage in accordance with IEC-61300-3-35.

At the time of assembly or testing of optical fiber, the installer shall view the endfaces of the fiber with a microscope. Viewing the endface may indicate that the endface is damaged or that it is contaminated (e.g., dirt, oil from fingers). When needed, the connector shall be cleaned, repolished, or replaced before making connections.

Channel links shall be tested with an OLTS using a three jumper reference method. The set up and methods for using these are set out in the relevant cabling standards.

Permanent links shall be tested with an OLTS using a one jumper reference method. The set up and methods for using these are set out in the relevant cabling standards.

The OLTS measurements can be used to verify the requirements of the various applications needed. Some of the most common applications in the data center are listed in Table 14-12.

14.11.4.3 Optical Fiber Test Parameters**14.11.4.3.1 Requirements**

The field test parameters to be measured shall meet the requirements of the cabling standards being followed (e.g., TIA-568-C.0, EN 50346). Testing installed optical fiber cabling for attenuation with an optical loss test set (OLTS) as described in cabling standards verifying the cabling length and polarity constitutes the minimum degree of testing.

Each optical fiber link shall be measured for its attenuation with an OLTS in each direction and bi-directionally. Fiber length verification may be obtained from cable sheath markings or by use of the OLTS (if the OLTS has length measurement capability). Polarity can be verified with the OLTS while performing attenuation tests. A visible light source, such as a visual fault locator, can also be used to verify polarity.

The link attenuation allowance shall be calculated as follows:

$$\text{Link Attenuation Allowance (dB)} = \begin{aligned} &\text{Cable Attenuation Allowance (dB)} + \\ &\text{Connector Insertion Loss Allowance (dB)} + \\ &\text{Splice Insertion Loss Allowance (dB)} + \\ &\text{Reference jumper Repeatability Allowance (dB)} \end{aligned} \quad (14-3)$$

where:

Cable Attenuation Allowance (dB) = Maximum Cable Attenuation Coefficient (dB/km) * Length (km)

Connector Insertion Loss Allowance (dB) = Number of Connector Pairs * Connector Loss Allowance (dB)

Splice Insertion Loss Allowance (dB) = Number of Splices * Splice Loss Allowance (dB)

Reference jumper Repeatability Allowance (dB) = see Table 14-13

Table 14-12 Common Applications Using Optical Fiber Cabling

<i>Ethernet applications</i>				
<i>Application</i>		<i>Fiber Type</i>	<i>Maximum Distance</i>	<i>Maximum Channel Loss</i>
<i>2-core applications. Can function on cables connected with SC, LC or any other compliant duplex connectors</i>				
	1000BASE-SX	OM3/OM4	550m	2.6dB
	1000BASE-LX ¹	OM3/OM4	550m	2.35dB
	10GBASE-SR	OM3	300m	2.6dB
	10GBASE-SR	OM4	400m	2.6dB
<i>8-core applications. Need MPO type connectors with 12-core fiber cables</i>				
	40GBASE-SR4	OM3	100m	1.9dB
	40GBASE-SR4	OM4	150m	1.5dB
	100GBASE-SR4 ²	OM3	70m (objective)	1.8dB
	100GBASE-SR4 ²	OM4	100m (objective)	1.9dB
<i>20-core applications. Need two MPO type connectors with 12-core fiber cables each</i>				
	100GBASE-SR10	OM3	100m	1.9dB
	100GBASE-SR10	OM4	150m	1.5dB
<i>Fiber Channel Applications</i>				
<i>2-core applications. Can function on cables connected with SC, LC or any other compliant duplex connectors</i>				
	4Gbps	OM3	380m	2.88dB
	4Gbps	OM4	400m	3.02dB
	8Gbps	OM3	150m	2.19dB
	8Gbps	OM4	190m	2.22dB
	16Gbps	OM3	100m	1.95dB
	16Gbps	OM4	125m	1.97dB
	32Gbps ²	OM3	70m	N/A
	32Gbps ²	OM4	100m	N/A

NOTE 1: Mode conditioning cord required

NOTE 2: Not ratified at time of publication of this standard

Table 14-13 Reference Jumper Repeatability Allowance

<i>Termination 1</i>	<i>Termination 2</i>	<i>Reference Jumper Repeatability Allowance</i>
MM reference grade	MM reference grade	0.1 dB
MM reference grade	MM standard grade	0.3 dB
MM standard grade	MM standard grade	0.5 dB (see note 2)

NOTE 1: This table provides the reference jumper repeatability allowance using standard and reference grade terminations in accordance with IEC 60874-19-1.

NOTE 2: 97% of individual connections are required meet this attenuation limit. As a minimum of two connections are present within installed cabling, a value of 0.5 dB is quoted on a statistical basis

An OTDR trace characterizes the installed fiber link, resulting in an indication of fiber segment length, attenuation uniformity and attenuation rate, connector location and insertion loss, splice location and splice loss, and other power loss events such as a sharp bend that may have been incurred during cable installation.

NOTE: The optical lengths of certain cables (e.g., stranded loose tube) may be longer than the cable sheath because of the fiber lay within the cable sheath. However, the recorded length measurement is assumed to be the physical jacketed cable length.

An acceptable attenuation for optical fiber cabling shall be based on an attenuation allowance equation and then compared to the measured installed loss. The loss allowance equation is based on the component losses for each of the components in the permanent link or channel and includes optical fiber type, cable type, wavelength, link distance, number of connections (e.g., mated pairs), and number of splices. The mean insertion loss of each component shall be obtained from the manufacturer and used in the link attenuation allowance calculation.

14.11.4.3.2 Recommendations

Because the validity of the test depends on a proper reference setting, it is critical to follow step by step the proper procedures described in the standards for each OLTS test.

An OTDR may be used to measure reflectance and ORL.

NOTE: Reflectance is the return loss for individual events (i.e., the reflection above the fiber backscatter level, relative to the source pulse). ORL is the return loss for the entire fiber under test, including fiber backscatter and reflections and relative to the source pulse.

Reflectance measurements of each connection should be:

- $\leq -20\text{dB}$ for a multimode PC connection
- $\leq -26\text{dB}$ for a single-mode PC connection
- $\leq -40\text{ dB}$ for a multimode UPC connection
- $\leq -50\text{ dB}$ for a single-mode UPC connection
- $\leq -60\text{ dB}$ for a single-mode APC connection
- $\leq -60\text{ dB}$ for a fusion splice connection

ORL measurements should be better than:

- 20 dB for multimode
- 26 dB for single-mode

14.11.4.4 Optical Fiber Cabling Field Test Instrument

14.11.4.4.1 Requirements

Optical fiber field test instruments for multimode cabling shall meet the requirements of applicable standards (e.g., IEC 61280-4-1).

Optical fiber field test instruments for single-mode cabling shall meet the requirements of applicable standards (e.g., IEC 61280-4-2).

Field test instruments shall:

- Be maintained following the equipment manufacturer's guidelines
- Have a valid calibration certificate, preferably from the equipment manufacturer
- Be loaded with the latest revision of firmware and test limits

14.11.4.4.2 Additional Information

IEC 61280-4-1 has adopted the encircled flux metric for testing installed multimode optical fiber links. Field test instruments typically combine two wavelength sources through a single port. A single mandrel is typically placed on the launch cord to measure the two wavelengths, which reduces complexity and time. This two wavelength measurement procedure prevents alignment of each individual source wavelength to their separate encircled flux targets and requires a compromise alignment for each wavelength placement within the encircled flux template. Using a single mandrel, alignment performed for one wavelength to meet encircled flux (typically 850 nm) may result in the other wavelength (typically 1300 nm) to have some uncertainty. Additionally, the encircled flux limits do not account for enabling existing field test instruments that may meet outdated standards. The use of an external modal conditioner with existing field test instruments adds additional uncertainty. These cumulative uncertainties may cause variations outside the encircled flux limits, more so at one wavelength over another.

14.11.4.5 Optical Fiber Cabling Field Test Interfaces, Adapters, Connectors, and Cords

14.11.4.5.1 Requirements

Test equipment interfaces, adapters, connectors, and cords used as connecting hardware have a limited life cycle and shall be inspected periodically for wear. The field test equipment manufacturer shall provide information on the life cycle of these components. Test adapters, interfaces, connectors, and cords shall be replaced per manufacturer recommendations.

User cords are equipment cords, patch cords, or jumpers that are included as part of the channel. User cords shall be tested in place within a channel. A user cord may be verified by inserting the cord in the channel under test. If the channel conforms to the transmission requirements, the user cord may be approved for use in that channel only. The orientation of the user cords shall not be reversed.

Connector endfaces shall be inspected with a suitable microscope (minimum 100x magnification) and when necessary cleaned in accordance with manufacturer's instructions prior to mating.

14.11.4.5.2 Recommendations

Test equipment interfaces, adapters, connectors, and cords should be either colored or labeled differently from in-service counterparts (preferably a single color dedicated for 'test equipment') to easily distinguish them from in-service equipment.

The use of temporary index matching materials (gels and fluids) in mated connectors under test is not recommended where the introduction of such materials may invalidate any measurement or test result.

14.11.4.6 Optical Fiber Cabling Field Test Documentation

14.11.4.6.1 Requirements

Documenting the test results provides the information that demonstrates the acceptability of the cabling system or support of specific networking technologies. A permanent record of all tests should be retained together with:

- Details of the measurement procedure
- Details of the measurement type
- Serial number of field test instruments used
- Proof of up to date calibration of the field test equipment
- Details of the measurement quality test cords used

14.12 Telecommunications and Computer Cabinets and Racks

As with all other systems of the data center—power, HVAC, and flooring—cabinets and racking systems provide the vital services of proper structural and secure housing for data center equipment. Active and passive equipment have different requirements for mounting, power, ventilation, and cable management.

14.12.1 Requirements and Recommendations

14.12.1.1 General Requirements

Two post racks, four post racks, and cabinets shall be secured in accordance with AHJ, seismic requirements for the location, and the planned long-term loading. When access floor systems are used, any one of the following methods shall be permitted:

- Attachment to metal struts that are captured below the floor by two or more access floor stringers
- Attachment to metal struts below the access floor that are suitably attached to the permanent floor
- Attachment via threaded rod directly to the permanent floor
- Attachment to channel bases bolted to floor slab

Cabinets and racks shall be constructed of noncombustible materials.

Performance specifications and overall physical dimensions of cabinets and racks shall conform to applicable codes, standards, and regulations (e.g., ATIS 0600336, EIA/ECA-310-E, IEC 60917).

14.12.1.2 General Recommendations

If not already required by the AHJ, in locations where seismic activity could create a potential risk, cabinets and four-post racks in the computer room should be anchored at their base to the permanent floor and preferably braced at the top (the raceway or overhead auxiliary framing can be used for this).

14.12.1.3 Rack Requirements

The following criteria of racks shall conform to applicable codes, standards and regulations (e.g., EIA/ECA-310-E, IEC 60917):

- Channel dimensions and spacing
- Channel hole dimensions and thread systems
- Channel equipment mounting hole vertical spacing (U or RU)
- Panel opening and usable aperture opening

14.12.1.3.1 Rack Recommendations

Maximum height should not exceed 2.4 m (8 ft).

When in a row, multiple racks and their associated vertical cable managers should be bolted together.

14.12.1.4 Cabinet Requirements

The following criteria shall conform to applicable codes, standards, and regulations (e.g., EIA/ECA-310-E, IEC 60917):

- Equipment mounting rail dimensions and spacing
- Equipment mounting rail hole vertical spacing (U or RU)

Options for cable access into the cabinet shall be available from both the top and bottom.

Access floor openings beneath cabinets for cable entry shall offer:

- Protection against damage to the cables
- Restrictions against intrusion of dirt and debris
- Restriction of air passage

Cabinets shall be constructed of noncombustible materials.

14.12.1.5 Cabinet Recommendations

Maximum height should not exceed 2.4 m (8 ft). Width should conform to applicable codes, standards, and regulations (e.g., EIA/ECA-310-E, IEC 60917), allowing for the exceptions noted therein.

Top access ports should provide a means to be closed when not in use.

In seismically active areas, multiple cabinets in a row should be bolted together at the top to provide additional stability.

14.12.2 Cabinet and Rack Configurations

14.12.2.1 General Recommendations

Within EDAs, select cabinets, racks, and vertical cable managers whose design minimizes obstruction of exhaust air and recirculation of hot air from behind the equipment to air intakes in the front of the equipment. Within HDAs, IDAs, and MDAs, select cabinets, racks, and vertical managers whose design optimizes patch cord management, while minimizing air leakage between hot aisle and cold aisle.

In data centers that employ hot aisle/cold aisle orientation, ensure that the warm air is always exhausted toward the hot aisle. Optical fiber and balanced twisted-pair ports are located at the rear of many servers.

To simplify patching and maintenance, structured cabling patch panels should be mounted so that the ports face the same direction as the network ports on the equipment to which they are patched. These ports are commonly on the rear of servers and the front of network switches.

For equipment that is cooled side-to-side (e.g., certain networking equipment), cabinets, racks, and vertical cable managers should be selected that introduce the least disruption to the proper functioning of the hot and cold aisles and that minimize recirculation of hot air toward the air intakes.

Finishes should conform to applicable codes, standards, and regulations (e.g., ANSI/TIA-942-A, ATIS 0600336); conductive finishes are recommended to ensure a good bond between equipment and cabinet or rack ground and to prevent oxidation of the base metal. For painted racks, a supplementary bonding/grounding busbar system may be used to ensure a good bond between equipment and cabinet or rack ground. Cabinet and rack bonding and grounding should comply with applicable codes, standards, and regulations (e.g., NECA/BICSI-607, TIA-607-B, and ISO/IEC DIS 30129 currently in development).

Racks in entrance rooms, main distribution areas and horizontal distribution areas should have dimensions and cable management capacities in accordance with applicable codes, standards, and regulations (e.g., TIA-942-A).

A minimum of 1 rack unit of horizontal cable management should be provided for each rack unit of balanced twisted pair or coaxial patch panel unless a specific high density solution of managing the patch cords on the sides for every unit is chosen. Exceptions exist when a non-angled patch panel features an integrated horizontal management product design. Vertical cable management should always be provided unless patching is provided directly above or directly below mated passive patch panels (e.g., balanced twisted-pair, coaxial cabling, or optical fiber cabling) or between passive patch panels and active equipment that are installed directly above or below one another. In such cases, relatively short (typically less than 1 m [3 ft]) patch cord assemblies (or equipment cord assemblies) may be used. When angled patch panels are used, horizontal cable managers are typically not installed. Vertical cable managers should always be sized to accommodate the anticipated maximum cordage that may be deployed given the equipment requirements at the time of deployment.

Shorter power cords, equipment cords, patch cords, and keyboard-video-mouse (KVM) cabling should be specified to reduce the cable management density in the back of the cabinet or rack.

14.12.2.2 Rack Configuration Recommendations

Rack depth should meet the mounting and protection needs of the equipment they are to host and, as a minimum, conform to the criteria established in applicable standards (e.g., EIA/ECA-310-E, IEC 60917).

Each rack should have vertical cable managers sized for maximum rack capacity attached on both sides. Vertical cable managers between two racks should be sized to serve both racks simultaneously.

14.12.2.3 Cabinet Configuration Recommendations

Equipment mounting rails should be adjustable front-to-rear and should have rack unit number indications (with numbers starting at the bottom).

Equipment mounting rail dimensions should conform to applicable codes, standards, and regulations (e.g., EIA/ECA-310-E, IEC 60917).

Doors should be removable without tools. Door hinge orientation should be reversible or dual hinged.

Side panels should be removable and lockable without requiring intrusion into the equipment mounting area within the cabinet.

In applications where active equipment, patch panels, and horizontal cable distribution are mixed, floor-tile-width (e.g., 600 mm [24 in] width) cabinets may lack adequate vertical cable management space.

Blank panels should be installed in unused rack positions to maintain separation between hot aisles and cold aisles and prevent hot exhaust air from recirculating and mixing with chilled air at equipment in-takes. Blank panels also improve rigidity of cabinets.(see Figure 14-11)



Figure 14-11
Blank Panels Installed in Empty RUs

14.12.3 Cabinet Airflow and Cabling Capacity

14.12.3.1 Airflow

To ensure adequate airflow and to provide adequate space for power strips, telecommunications cabling, and safe access for work, the cabinet depth should be at least 150 mm (6 in) deeper than the deepest equipment to be housed if the cabinet is 700 mm (27.5 in) wide or larger. If the cabinet is less than 700 mm (27.5 in) wide, 11.5 mm (0.45 in) depth should be added for every 10 mm (0.4 in) reduction from 700 mm (27.6 in) width. (See Table 14-14)

Where mesh doors are used for ventilation, the doors should be a minimum 63% open to airflow for allowing chilled air entrance or evacuating heated exhaust air from the cabinet.

14.12.3.2 Calculating Cabinet Airflow Capacity

It is recommended that the following formulae be used to calculate door airflow capacity:

Airflow capacity (AFC) calculations:

$$AFC_D = \frac{S_D \times F_{EA}}{A_C \times H_{RMU} \times N_{RMU}} \quad (14-4)$$

Where:

AFC_D is airflow capacity for cabinets with doors

S_D is total surface area of the door panel inside the outer extreme boundaries of airflow openings (mesh, perforations, slots, etc.), in mm^2 (in^2)

F_{EA} is effective (open) area factor of the door mesh material (e.g., 0.65 [65%], 1 if mesh or screen is not used)

A_C is useable cabinet aperture opening at the door plane, in mm (in) (See Figure 14-12)

H_{RMU} is height of one rack unit (44.5 mm [1.75 in])

N_{RMU} is quantity of rack units in the cabinet.

Example: Network cabinet or server cabinet design with mesh doors

NOTE: The following parameters are for demonstration purposes and may not reflect actual properties of a specific cabinet or design requirements.

Given:

- 19-in equipment cabinet
- Height: 42 RMU
- Mesh door with $F_{EA} = 0.65$, 1,930 mm x 635 mm (76 in x 25 in)
- 1 RMU = 44.5 mm (1.75 in)
- Cabinet open aperture: 450.85 mm (17.75 in)

NOTE: Input data and criteria used in the examples above are provided as samples only. For actual parameters, please refer to the particular network cabinet or server cabinet design requirements.

Airflow capacity:

$$AFC_D = \left(\frac{S_D \times F_{EA}}{A_C \times H_{RMU} \times N_{RMU}} \right) = \left(\frac{1,930 \text{ mm} \times 635 \text{ mm} \times 0.65}{450.85 \text{ mm} \times 44.5 \text{ mm} \times 42} \right)$$

$$AFC_D = \frac{1,225,550 \text{ mm}^2 \times 0.65}{842,639 \text{ mm}^2} = 0.9454$$

Table 14-14 Example of Cabinet Depth Guidelines

Cabinet Width	Deeper than the Deepest Equipment Housed in the Cabinet	Additional Depth for Narrow Cabinets
600 mm (24 in)	150 mm (6 in)	115 mm (4.5 in)
700 mm (27.5 in)	150 mm (6 in)	N/A
750 mm (29.5 in)	150 mm (6 in)	N/A
800 mm (31.5 in)	150 mm (6 in)	N/A

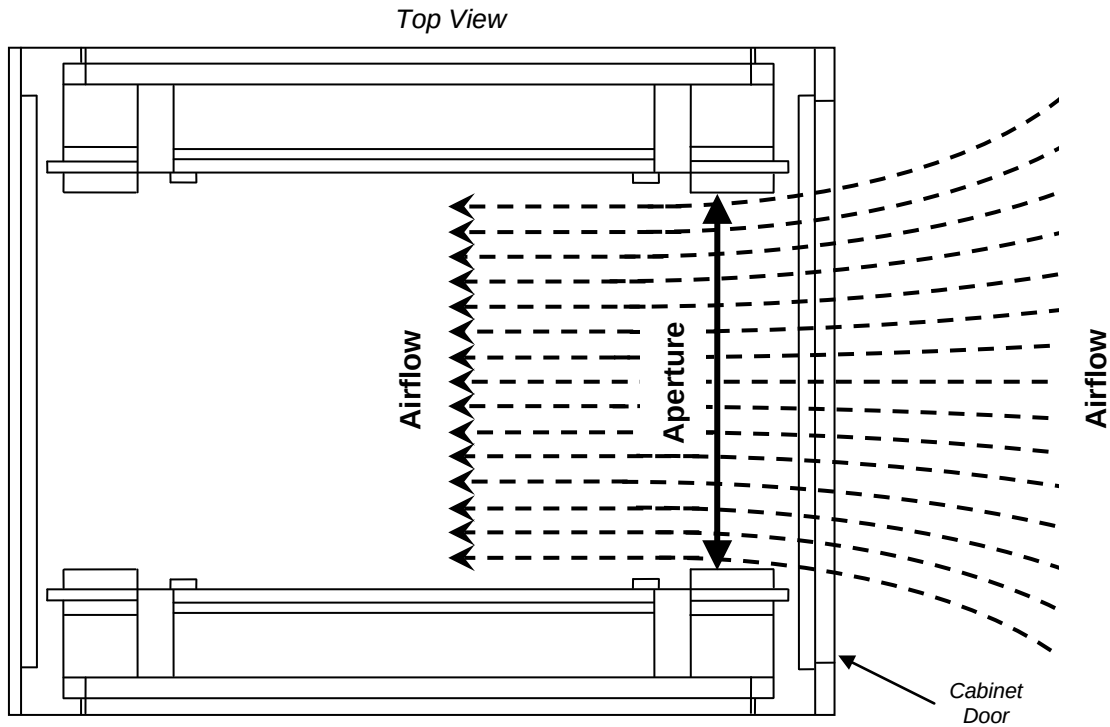


**Figure 14-12
Cabinet Aperture Opening**

$$AFC_D = \left(\frac{S_D \times F_{EA}}{A_C \times H_{RMU} \times N_{RMU}} \right) = \left(\frac{76 \text{ in} \times 25 \text{ in} \times 0.65}{17.75 \text{ in} \times 1.75 \text{ in} \times 42} \right)$$

$$AFC_D = \frac{1,900 \text{ in}^2 \times 0.65}{1,304.63 \text{ in}^2} = 0.9467$$

Conclusion: the cabinet mesh door open airflow capacity (ACF_D) falls within the recommended limits (e.g., 0.63-1.00 [63%-100%]).

When using Equation 14-4, any area within SD occupied by airflow impervious structures (e.g., such as door latches, door locks, access control panels), must be subtracted from the initial SD to establish the final SD for above calculations.

14.12.3.3 Cabinet Cable Capacity

14.12.3.3.1 Calculating Number of Cables

In order to estimate the number of cables the cabinet can accommodate, the following formulae can be used:

$$N = \frac{S_U}{S_{cable}} \times f_{fill} = \frac{S_I - S_E - S_O}{S_{cable}} \times f_{fill} \quad (14-5)$$

where:

N is the number of cables the cabinet can accommodate

S_U is the useful cabinet area, where cables can be installed, mm^2 (in^2)

S_{cable} is the cable cross-sectional area, mm^2 (in^2) (see Section 14.12.3.3.2)

f_{fill} is required or recommended cable pathway fill factor (e.g., 0.4 [i.e., 40 %])

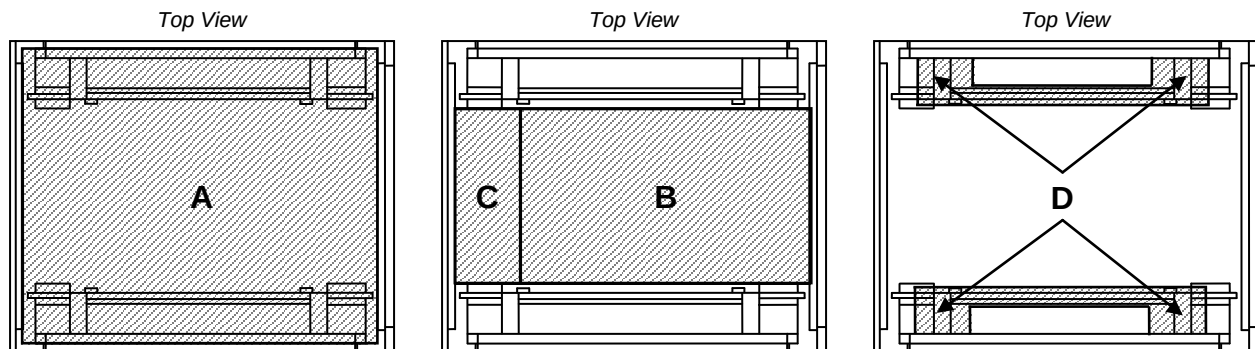
S_I is the cabinet internal area, mm^2 (in^2) (see Section 14.12.3.3.4)

S_E is the area allocated for active equipment and connecting hardware, mm^2 (in^2) (see Section 14.12.3.3.5)

S_O is the area occupied by various obstructing elements, such as rails, power strips, mm^2 (in^2) (see Section 14.12.3.3.6)

Illustrations of S_I , S_E , and S_O components are provided in Figure 14-13.

NOTE: Boundaries of areas shown in Figure 14-13 are for illustration purposes only; actual boundaries may vary depending on the cabinet design and layout.



Area A: S_I —cabinet internal area

Area B: S_E —area allocated for active equipment and connecting hardware including area C

Area C: “dead zone,” spare space behind active equipment and connecting hardware

Area D: S_O —area occupied by various obstructing elements, such as rails, power strips, etc.

Figure 14-13
Illustration of Components for Cable Capacity Formulae

14.12.3.3.2 Equation for Cable Cross Section Area (S_{cable})

The following equation for S_{cable} is used when the cables within the cabinet have a consistent diameter.

$$S_{cable} = \pi \times \frac{(d_{cable})^2}{4} = 3.14 \times \frac{(d_{cable})^2}{4} = 0.79 \times (d_{cable})^2 \quad (14-6)$$

where:

d_{cable} is the cable diameter, mm (in)

NOTE: See Section 14.12.3.3.3 for information on the calculation of d_{cable} when multiple cable diameters are expected or present.

14.12.3.3.3 Equation for Cable Diameter (d_{cable}) for Multiple Cable Diameters

When cables of differing diameters are to be deployed in a cabinet, because of differing media or performance characteristics (e.g., Category 5e and Category 6A), the cross sectional area can be approximated. This approximation is based on the diameters of the cables to be installed and the percentage of each cable type expected to be installed (e.g., 40% of the cable will be Category 5e and 60% will be Category 6A).

$$d_{cable} = \sqrt{\sum_{i=1}^n P_i \times D_i^2} \quad (14-7)$$

where:

d_{cable} is the cable diameter, mm (in)

n is the total number of different cable diameters

P_i is the percentage of the specific (indexed) cable

D_i is the diameter of the specific (indexed) cable

Example

Cable A has a diameter of 4.8 mm (0.19 in) and constitutes 8% of the total, Cable B has a diameter of 7.7 mm (0.30 in) and constitutes 32% of the total and a third cable has a diameter of 5.6 mm (0.22 in) and constitutes 60% of the total

$$d_{cable} = \sqrt{[(0.08 \times 4.8 \text{ mm} \times 4.8 \text{ mm}) + (0.32 \times 7.7 \text{ mm} \times 7.7 \text{ mm}) + (0.6 \times 5.6 \text{ mm} \times 5.6 \text{ mm})]}$$

$$d_{cable} = \sqrt{(1.843 \text{ mm}^2 + 18.973 \text{ mm}^2 + 18.816 \text{ mm}^2)}$$

$$d_{cable} = \sqrt{39.632 \text{ mm}^2}$$

$$d_{cable} = 6.30 \text{ mm}$$

or

$$d_{cable} = \sqrt{[(0.08 \times 0.19 \text{ in} \times 0.19 \text{ in}) + (0.32 \times 0.30 \text{ in} \times 0.30 \text{ in}) + (0.6 \times 0.22 \text{ in} \times 0.22 \text{ in})]}$$

$$d_{cable} = \sqrt{(0.003 \text{ in}^2 + 0.029 \text{ in}^2 + 0.029 \text{ in}^2)}$$

$$d_{cable} = \sqrt{0.061 \text{ in}^2}$$

$$d_{cable} = 0.247 \text{ in}$$

Once N , the number of cables for a specific cabinet, has been calculated (see Eq. 14-5), the specific number of each cable can be determined by multiplying N by the specific cable percentage.

14.12.3.3.4 Equation for Cabinet Internal Area (S_I)

$$S_I = (W_C \times f_D) \times (D_C \times f_D) = W_C \times D_C \times f_D^2 \quad (14-8)$$

where:

W_C is cabinet width, mm (in)

D_C is cabinet depth, mm (in)

f_D is dimensional de-rating factor for internal space (e.g., 0.95)

14.12.3.3.5 Equation for Area Allocated for Active Equipment and Connecting Hardware (S_E)

$$S_E = A_C \times (D_C \times f_D) \quad (14-9)$$

where:

A_C is useable cabinet aperture opening, mm (e.g., 450.85 mm [17.75 in])

D_C is cabinet depth, mm (in)

f_D is dimensional de-rating factor for internal space (e.g., 0.95)

14.12.3.3.6 Equation for Area Occupied by Obstructing Elements (S_O)

$$S_O = (S_I - S_E) \times f_O \quad (14-10)$$

where:

f_O is de-rating factor taking into account the obstructing elements (e.g., 0.3)

S_I is the cabinet internal area, mm² (in²) (see Section 14.12.3.3.4)

S_E is the area allocated for active equipment and connecting hardware, mm² (in²) (see Section 14.12.3.3.5)

14.12.3.3.7 Alternative Equation for Calculating Cabinet Cabling Capacity

As an alternative to separate calculations of each component provided above (which may be required for detailed design analysis), the following reduced formula (14-11) may be used:

$$N = \frac{\{[(D_C - D_E) \times f_D] \times [(W_C - A_C) \times f_D \times (1 - f_O)]\} \times f_{fill}}{0.79 \times (d_{cable})^2} \quad (14-11)$$

where:

D_C = cabinet depth, mm (in)
 D_E = maximum equipment depth, mm (in)
 f_D = dimensional de-rating factor for internal space (e.g., 0.95)
 f_{fill} = required or recommended cable pathway fill factor (e.g., 0.4 [i.e., 40 %])
 W_C = cabinet width, mm (in)
 A_C = useable cabinet aperture opening, mm (e.g., 450.85 mm [17.75 in])
 f_O = de-rating factor taking into account the obstructing elements (e.g., 0.3)
 d_{cable} = cable diameter, mm (in)

Where available, vendor cable manager calculators should be used to specify a correctly sized cabinet. Where such calculators are not available, Table 14-15 provides cable capacity estimates based on total available space outside of the equipment mounting area and between the rear equipment mounting rail (located at 762 mm [30 in] behind the front frame piece) and the rear frame and allowing 152 mm² (0.24 in²) for vertical power strips, regardless of the presence or lack of vertical cable management accessories.

Cabinets should have adequate width and depth to avoid routing of cabling behind equipment exhausts where they may obstruct proper airflow.

Cable management capacity requirements should be calculated prior to either specifying a cabinet or even specifying a cabinet footprint.

Vertical cable management should be available and should be deployable in either the zero U space or, in deeper, more cabling intensive applications, in the equipment mounting space behind the mounted equipment.

Cabinets should include integral features for attaching any sort of external bracing structures.

Front and rear clearances around cabinets should conform to applicable codes, standards and regulations (e.g., NFPA 70; see also Section 6.6). Minimum clearances should be optimized with either 150° or larger door swing, or split doors with hinges on both sides and latching in the center.

NOTE: Use the cross sectional values from Table 14-15 to calculate the cable capacity of a cabinet per the following procedure:

$$N = \text{round\_down} (A_{cable \text{ management space}} \div A_{cable}) \times f \quad (14-12)$$

Where:

N = Number of cables
 $A_{cable \text{ management space}}$ = cross sectional space from Table 14-15 in mm² (in²)
 A_{cable} = cross sectional area of cable, mm² (in²)
 f = fill rate

For example, a 1050 mm (41.3 in) deep and 700 mm (27.5 in) wide cabinet with one power strip and 8 mm (0.31 in) diameter cable would be calculated as follows for a 40% fill rate:

$$\begin{aligned} A_{cable \text{ management space}} &= 89600 \text{ mm}^2 \\ A_{cable} &= \pi \times 4^2 = 50.24 \text{ mm}^2 \\ N &= (89600/50.24) \times 0.4 = 713.3758 = 713 \end{aligned}$$

Table 14-15 assumes cables are managed outside the space used for ventilation of equipment. The rows with “a” following the cabinet depth are for one vertically mounted power strip. The rows for “b” following the cabinet depth are for two vertically mounted power strips.

Table 14-15 Available Space for Calculating Cabinet Vertical Cable Capacity

Cross-sectional values in mm² (in²) for noted cabinet depths and widths

Cabinet Frame Depth (mm)	Cabinet Width (mm)			
	600 mm	700 mm	750 mm	800 mm
900	15700 (24)	45300 (70)	58400 (90)	71400 (111)
900a ³	10500 (16)	40100 (62)	53200 (82)	66300 (103)
900b ⁴	5400 (8)	35000 (54)	48000(74)	61100 (95)
950	21500 (33)	62100 (96)	80000 (124)	97900 (152)
950a ³	16300 (25)	56900 (88)	74800 (116)	92700 (144)
950b ⁴	11200 (17)	51700 (80)	69600 (108)	87500 (136)
1000	27300 (42)	78800 (122)	124300 (157)	124300 (193)
1000a ³	22100 (34)	73700 (114)	119200 (149)	119200 (185)
1000b ⁴	17000 (26)	68500 (106)	91300 (141)	114000 (177)
1050	32800 (51)	94800 (147)	122100 (189)	149500 (232)
1050a ³	27600 (43)	89600 (139)	117000 (181)	144300 (224)
1050b ⁴	22500 (35)	84500 (131)	111800 (173)	139100 (216)
1100	38600 (60)	111500 (173)	143700 (223)	175900 (273)
1100a ³	33500 (52)	106400 (165)	138600 (215)	170700 (265)
1100b ⁴	28300 (44)	101200 (157)	133400 (207)	165600 (257)
1150	44400 (69)	128300 (199)	165300 (256)	202400 (314)
1150a ³	39300 (61)	123200 (191)	160200 (248)	197200 (306)
1150b ⁴	34100 (53)	118000 (183)	155000 (232)	192000 (298)
1200	49900 (77)	144300 (224)	185900 (288)	227500 (353)
1200a ³	44800 (69)	139100 (216)	180700 (280)	222300 (344)
1200b ⁴	39600 (61)	133900 (208)	175500 (272)	217200 (337)

NOTE 1: Standard front-to-rear mounting rail spacing = 750 mm (29.5 in)

NOTE 2: Front rail is set back 25 mm (1 in) from cabinet frame

NOTE 3: Capacity de-rated for one vertically mounted power strip

NOTE 4: Capacity de-rated for two vertically mounted power strips

NOTE 5: IMPORTANT: Capacities are calculated on available space. Vendor specifications need to be referenced to determine actual cable management capacity

14.12.4 Cabinet and Rack Installations

14.12.4.1 General Requirements

Where the cabinets and racks are on an access floor, they shall be placed so that there are liftable tiles in front and behind each cabinet and rack. This typically means placing the rows of cabinets and racks parallel (rather than at an angle) to the rows of floor tiles and placing the front edge of the cabinets along the edge of the floor tiles to lock down the minimum number of tiles under the cabinets.

All overhead cable management (e.g., ladder racks, cable tray, etc) shall remain free of obstructions such as sprinklers, lighting, and electrical outlets.

The designer shall anticipate the weight of the equipment in the cabinets and racks; ensure that the cabinets, racks and floors (both access floors and slabs) are rated to handle the expected weight.

Adequate power shall be available to all cabinets and racks that will hold active equipment and must be installed in accordance with applicable codes and the AHJ.

Each cabinet and rack shall be labeled on the front and back with its identifier. All patch panels, cables, equipment cords, and patch cords shall be properly labeled per applicable standards (e.g., TIA-606-B, ISO 14763-2-1). (See Figure 14-14 and Figure 14-15).



Figure 14-14
Cabinets Are Identified and Labeled



Figure 14-15
Example of Labeled Termination Ports and Equipment Cords

14.12.4.2 General Recommendations

Cabinet and rack layout designs should be harmonized with lighting (luminaire) delivery layout designs.

Anticipate growth and leave room for expansion when/if possible.

Power strips should be labeled with power distribution unit or electrical panelboard identifier and circuit breaker number.

Power cords should not be installed under equipment, mats, or covering other than access floor tiles. The mounting surface for cabinet and racks should be prepared for the specific anchors required for the application. Refer to manufacturer's recommended practice and verify those practices are acceptable to the local AHJ. Cabinets in a line-up where they are properly attached together may require fewer anchors per cabinet than those installed as standalone units. When drilling into the mounting surface use proper technique to ensure that dust or particles do not get airborne. Using a drill with attached vacuum is an effective way to prevent dust or particles while drilling in floors or walls.

14.12.4.3 Rack Installation Recommendations

Equipment in the computer room should be mounted to cabinet or rack rails rather than placed on shelves as equipment on shelves provides a return path for air between the rear and front of the cabinet or rack.

Floor tile openings under cabinets and racks should be no larger than required for entry of cabling to minimize loss of underfloor pressure through openings.

Consider using openings with gaskets or brush grommets to satisfy requirements to minimize air pressure loss and short-circuiting of cold aisle/hot aisle air circulation and subsequent reduction in cooling efficiency. See Figure 14-16 and Figure 14-17 for examples of air recirculation and Figure 14-18 and Figure 14-19 for gaskets and brush grommets.

A dedicated pathway should be provided for equipment cords or patch cords within an MDA, IDA, or HDA that is separate from those used for horizontal and backbone cabling.

Ensure all active devices are properly supported and securely mounted to the rack to prevent equipment damage from improper installation.

In seismically active areas, it is recommended that the design of the attachment methods and the installation be reviewed by a licensed structural engineer. Many jurisdictions will require a seismic certification report signed by a professional engineer.

Sharp edges at the top of the threaded rods should be capped (using plastic covers, domed nuts, or other means). The exposed threads under the access floor should be covered using split tubing or other method to avoid abrading cable.

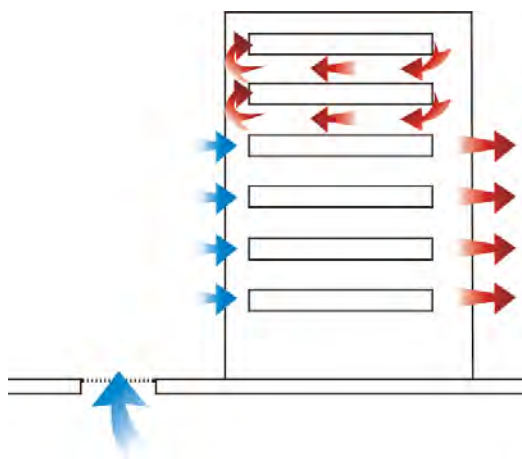


Figure 14-16
Effect Of Internal Hot Air Recirculation

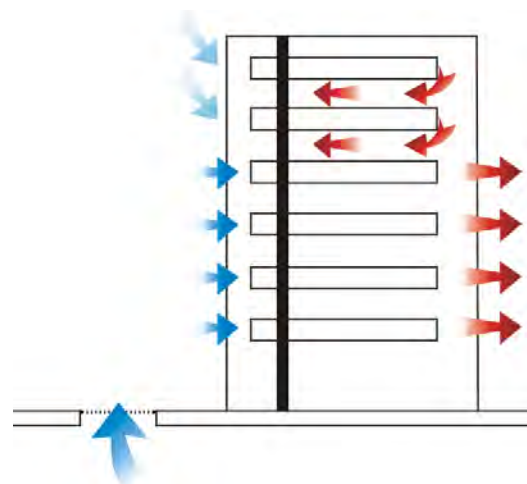


Figure 14-17
How Reducing Internal Hot Air Recirculation Reduces Input Air Temperature



Figure 14-18
Gasket Seals Off Access Floor Tile Cutout In
Vertical Cable Manager

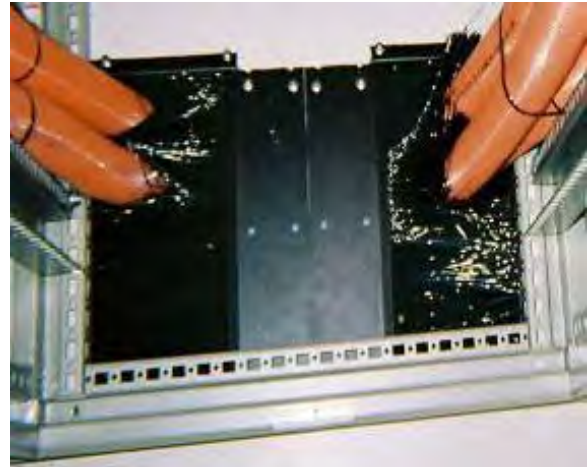


Figure 14-19
Brush Grommet Seals Access Floor Tile Cutout

Racks should be set in place and leveled throughout the line-up. Shimming of any anchoring point should not exceed 13 mm (0.5 in) unless specified by the project engineer. If racks require more than 13 mm (0.5 in) of shimming, an engineered solution should be used to ensure rack line-ups are properly supported. Adjacent racks in the line-up should be ganged together before anchors are installed. Install anchors per manufacturer specification, making sure all shims are properly located.

Some line-ups require additional bracing to meet customer specifications or local codes. Required bracing may be based on rack style, equipment, and location. Bracing should be installed as a system to ensure proper fit and support. Install all parts hand tight and then tighten fasteners in a series to prevent stress on rack lineup. All bracing should be installed before racks are populated.

14.12.4.4 Cabinet Installation Recommendations

Avoid empty cabinet or rack positions in rows. Replace removed cabinets or frames and fill any gaps in a row of cabinets with a substitute blanking panel of the same height as the cabinet or frames to either side to avoid recirculation of air between hot and cold aisles. For the same reason, cabinets and racks should be installed with no blank spaces between them. In the case of vacant cabinets and racks and where blank spaces exist in populated cabinets and racks, install blanking panels. Vertical cable managers can provide cable management and block recirculation of air between racks. Cabinets should be butted up against each other. Where possible, bayed cabinets should still share a side panel or include other means to seal the rear-to-front airflow path along the side of rack-mounted equipment.

Given a choice, where placing one edge of the cabinet creates unequal aisle sizes, the front aisle should be the larger one as it provides more working space for installation of equipment into cabinets and a greater area for providing cool air to cabinets.

In order to meet the requirement to restrict air passage through all openings outside the cold aisle on access floors, floor tile openings under cabinets and racks should be no larger than required for entry of cabling to minimize loss of underfloor pressure through openings taking into account anticipated growth.

Furthermore, consider using openings with gaskets or brush grommets to minimize air pressure loss and short-circuiting of cold aisle/hot aisle air circulation and subsequent reduction in cooling efficiency. See Figure 14-16 through Figure 14-19 for examples.

- Ensure that all active devices are properly supported and securely mounted to the cabinet to prevent equipment damage from improper installation.

Plan equipment, power strip, cable manager, and cabling layouts in cabinets before making a major purchase. Either create detailed drawings or preferably create a mock up to ensure that:

- All equipment and cable managers fit properly
- There is adequate space and access to power strips
- There is adequate access to cabinet floor and top openings
- There is adequate space for cable management
- Equipment can properly slide in and out as required
- Equipment intakes and exhausts are not blocked by cabling, cable management, or cabinet structure so that air can flow freely within the rack and to exit out the hot side
- Cabinets, racks, and vertical management do not have large openings for recirculation of air from hot to cold aisles

- Temporarily remove any doors and panels that may interfere with the cabinet installation.

On solid or slab floors, cabinets should be set in place and leveled throughout the line-up. Most cabinets are equipped with leveling feet. If leveling feet are not provided, consult manufacturer for proper shimming hardware.

On access floors, cabinets and racks should be secured to the concrete subfloor. If cabinets in the line-up are to be ganged, attachment hardware should be installed before anchors are installed. Install anchors per manufacturer's specification, making sure all shimming hardware is properly located. (See Figure 14-20).

In seismically active areas, it is recommended that the design of the cabinets and their installation be reviewed by a licensed structural engineer as many jurisdictions require a seismic certification report signed by a professional engineer.

Sharp edges at the top of the threaded rods should be capped (using plastic covers, domed nuts, or other means). The exposed threads under the access floor should be covered using split tubing or other method to avoid abrading cable.

Floor tile panels should have correctly sized and placed cutouts for the cabinet or equipment placed over them. The cutout should be under the cabinet/equipment cord opening and properly sized for the quantity and type of cables to be routed through the opening.



NOTE: Threaded rods are uncovered for illustration purposes; exposed threads should be covered.

Figure 14-20
Illustration of Securing Cabinets and Racks on an Access Floor to a Concrete Slab Using Threaded Rod and Steel Channel

14.12.5 Thermal Management in Cabinets

14.12.5.1 Recommendations

There is no one thermal management configuration that works best in every instance. Each may be optimal, depending upon different factors unique to the customer, application, and environment. Serious consideration should be given to understanding the upfront installed costs as well as ongoing operation cost from an energy efficiency and maintenance perspective. At a minimum, equipment should be installed in cabinets with the air intake oriented toward the front of the cabinet or rack and the air exhaust oriented toward the rear of the cabinet or rack, when possible, with the cabinet rows oriented in a “hot aisle/cold aisle” configuration—rears of cabinets facing each other and fronts of cabinets facing each other.

Use of any supplementary cooling mechanisms on a cabinet must take into consideration its effect on the overall fluid dynamics of the air space and how other equipment will be affected.

Considerations of supplemental cooling systems need to include criticality and required levels of redundant backup. Cabinets with good passive air management systems in well-designed rooms remove concerns about single points of failure and can support heat loads of twenty kW and higher.

Cabinet fans for cabinets specially designed to handle high heat loads should be on UPS power and have redundant power cords or be on transfer switches to ensure continuous operation.

Cabinet fans should be on separate circuits from the equipment in the cabinet as fans are susceptible to ground faults.

The perimeter of the equipment mounting area is also a path for cold air bypass or hot air recirculation and should be blocked accordingly.

Careful planning is needed for capacities, heat loads, and redundancies required for desired availability and reliability. See Appendix B.

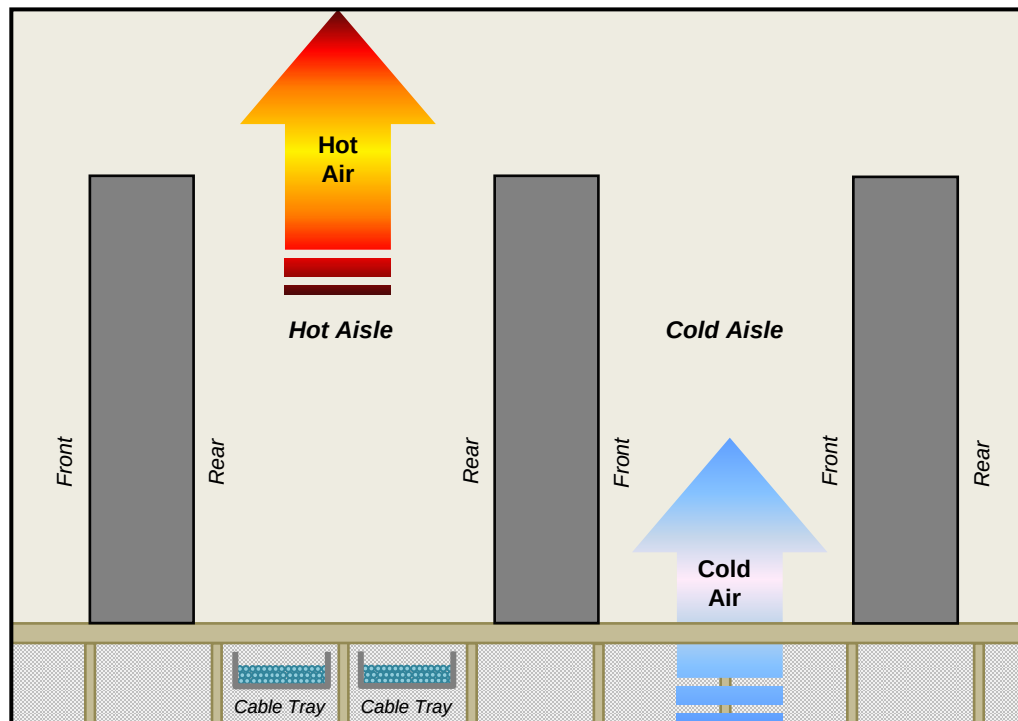


Figure 14-21
Hot Aisle/Cold Aisle Cabinet Layout

14.12.5.2 Additional Information

Specify/purchase the highest quality racks and rack components the budget will allow. They hold up better in the long run through numerous changes.

Over tightening mounting screws will strip out threads in the racks (especially the poorer quality racks). Minimum torque setting on drill/driver is usually sufficient to secure anything in the rack. Refer to manufacturer's specifications for recommended hardware. Specify toolless construction wherever possible.

ITE original equipment manufacturers (OEM) cabinets may provide insufficient space to meet operational cable management requirements or cabling architecture.

Current generation servers will operate with, and high availability environments require, multiple network connections. For example, a single server might typically have two production LAN connections, one or two clustering or virtualization LAN connections, an out-of-band software management LAN connection, a hardware lights out management (LOM) LAN connection, and two (primary and secondary) SAN network connections. Additionally, there may be redundant power supplies requiring two or more power cords per server. Therefore, in a server cabinet that houses twelve servers, the application could potentially encounter seventy-two (72) balanced twisted-pair equipment cords, twenty-four (24) duplex optical fiber equipment cords, and twenty-four (24) power cords for a total of one hundred twenty (120) individual cords, plus any KVM cabling.

Some line-ups require additional bracing to meet customer specifications or local codes. All bracing should be installed before cabinet doors or panels are installed and before the cabinet is populated. Required bracing may be based on cabinet style, equipment, and location. Bracing should be installed as a system to ensure proper fit and support. Install all parts hand tight and then tighten fasteners in a series to prevent stress on cabinet line-up.

Changes in floor tile cuts can be disruptive and time-consuming. To mitigate the change of reworks, floor tile panel cuts should be carefully planned, taking into account current and anticipated power and data cabling requirements as well as all necessary route diversity considerations.

Cabinet roof fans and fan trays generally offer little benefit and can actually be counterproductive, creating hot spots within a cabinet, particularly when used in conjunction with high airflow mesh front doors. Additionally, these fans may disrupt the proper function of hot and cold aisles. Caution should be applied to any use of cabinet fans to assure they will enhance rather than disrupt the proper functioning of hot and cold aisle separation. Rear door fans can be used as long as the actual delivered fan capacity is not less than the cumulative throughput of the equipment fans in the cabinet.

In suboptimized spaces, hot aisle containment or cold aisle containment may compensate for otherwise inadequate cooling by isolating source air from return air.

NOTE: As an installation tip, make a floor cut template on cardboard or directly on the floor panel from the access opening in the cabinet being placed.

14.13 Telecommunications Cabling, Pathways, and Spaces Administration

14.13.1 General

14.13.1.1 Introduction

Documentation, labeling, and administration of data center components are critical to proper operation and maintenance of a data center. Administration systems may be manually operated or utilize an automated system. However, physical labeling of all items should be undertaken irrespective of the system being implemented. The following guidelines and recommendations contained in this section are for the administration of a data center.

14.13.1.2 Requirements

Data centers shall be provided with an identification/administration system following the hierarchical requirements of an approved standard (e.g., TIA-606-B or ISO/IEC TR 14763-2-1). The administration system must include identification and labeling requirements for:

- Campus or site
- Building
- Indoor telecommunications space
- Outdoor telecommunications spaces such as maintenance holes, handholes, joining chambers, pedestals, or outdoor cabinets
- Cabinet, frame, or wall segment

<List continues on next page>

- Closure
- Port or termination on closure
- Backbone cable or cable between cabinets, frames, or wall sections
- Pair/port within backbone cable or cable within distributor, telecommunications room, equipment room, or computer room
- Splice - pair in splice on backbone cable or horizontal cable to outlets mounted in a cabinet, frame, or wall section in distributor, telecommunications room, or data center
- CP port in ZDA or LDP
- Horizontal cable to telecommunications outlet not mounted in a cabinet, frame, or wall section in distributor, telecommunications room, or data center
- Telecommunications outlets not mounted in a cabinet, frame, or wall section in distributor, telecommunications room, or data center
- Splice - pair in splice on horizontal link to telecommunications outlets not mounted in a cabinet, frame, or wall section in distributor, telecommunications room, or data center
- Patch cord or jumper
- Outdoor pathway system
- Campus or building entrance pathway system
- Pathway system within a building
- Firestop in building pathway system
- Data center pathway system
- Bonding conductor for cabinet or frame
- Cabinets, racks, and frames
- Patch panels
- Patch panel and equipment outlet ports
- Cables
- Patch cords and equipment cords

14.13.1.3 Recommendations

Supplies for labeling and administration should be part of an inventory system. Cable label makers, labels, markers, spare batteries, and other supplies are often overlooked and should be readily available. This will help ensure proper marking.

14.13.2 Identification Conventions for Data Center Components

14.13.2.1 Spaces

14.13.2.1.1 Introduction

Spaces in the data center need to be identified and recorded to ensure operational efficiencies. Space identification is traditionally user specified. Additionally, architectural concerns could determine the labeling methods for spaces. Data center spaces are also defined in the various cabling standards.

14.13.2.1.2 Requirements

All spaces shall have a unique identifier and be labeled.

14.13.2.1.3 Recommendations

A space summary report should be available listing all spaces, including their types and locations.

A space with access floor should track the computer room grid. Most computer rooms will use at least two letters and two numeric digits to identify every 600 mm × 600 mm (24 in × 24 in) floor tile. In such computer rooms, the letters will be AA, AB, AC, ..., AZ, BA, BB, BC, and so on (See Figure 14-22). For example, a floor tile located in the seventh row (AG) in the twelfth (12) column should be called AG12.

If the computer room is comprised of multiple spaces, the space identifier should be incorporated at the beginning of the floor space identifiers. Therefore, the cabinet at AG05 in room 4DC should be named 4DC-AG05.

In general, space identifiers should be formatted as fs-XXYY, where:

- fs is the optional space identifier.
- XX is floor tile grid row.
- YY is floor tile grid column.

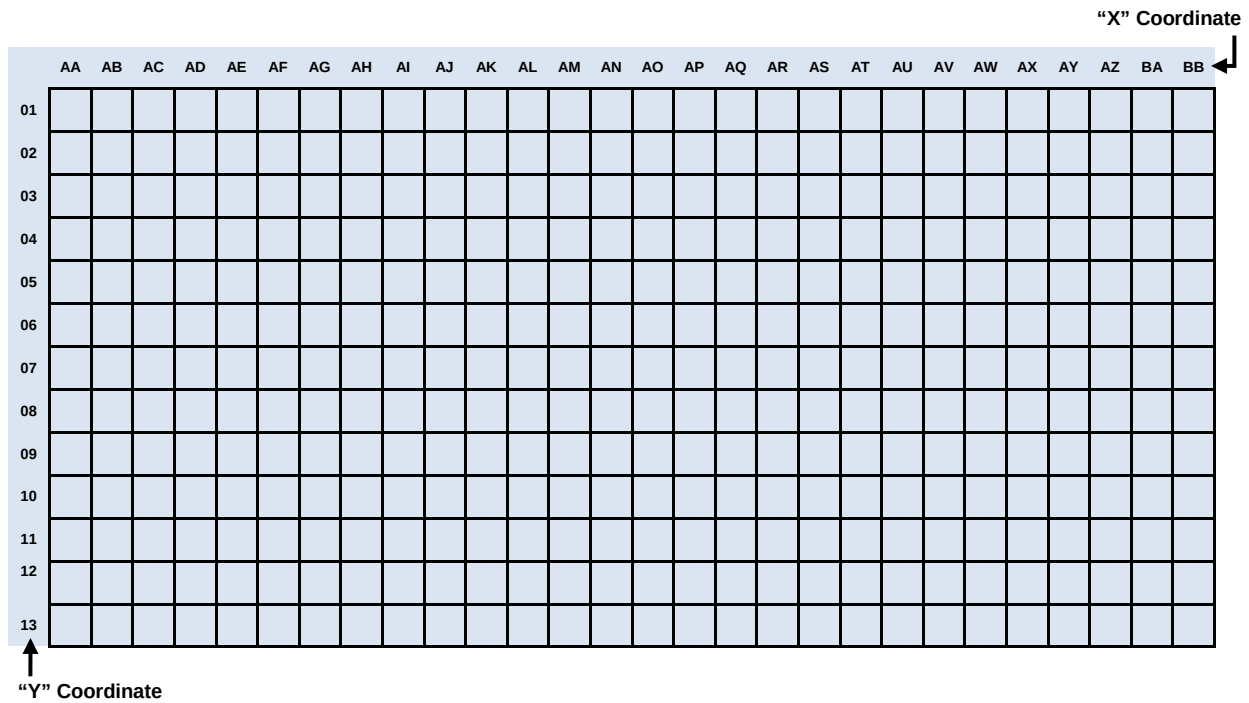


Figure 14-22
Room Grid Coordinate System Example

14.13.2.2 Cabinets and Racks

14.13.2.2.1 Requirements

In facilities with 600 mm × 600 mm (24 in × 24 in) floor tiles, many cabinets and racks will extend over more than one floor tile. In these facilities, each cabinet and rack shall be identified with a tile identifier, using the same location on every cabinet or rack to determine the grid location. This location shall be some point on the front of the cabinet or rack. The location may be the left front corner, right front corner, or front center as long as the same location is used for all cabinets and racks in the facility.

In rooms without a grid identifier, cabinets and racks may be identified by their row number and location within the row. The quantity of characters used for each identifier shall be the same throughout the facility. The numbering shall begin at the same end of each row in the facility, selecting an end that is not at risk of future cabinet or rack growth, such as adjacent to a wall.

The location identifier shall be labeled in plain view on the front and rear of each cabinet and rack. Preferred locations for labels are the top and bottom on a permanent part of the cabinet or rack. Text on the labels shall be upper case and large enough to be easily read from a standing eye-level vantage point near the cabinet or rack. The label text shall be machine printed, and the label color shall contrast with the surface upon which it is affixed (e.g., white on a dark surface, black on a light surface).

14.13.2.3 Pathways

14.13.2.3.1 Introduction

Pathways may include conduit, cable tray systems, or other elements in the data center used to support and convey telecommunications cabling.

14.13.2.3.2 Requirements

All entrance pathways and pathways between rooms shall have a unique identifier per applicable standards (e.g., TIA-606-B or ISO/IEC TR 14763-2-1).

All entrance pathways and pathways between rooms shall be labeled at all endpoints.

14.13.2.3.3 Recommendations

Additional labeling should be provided at:

- Intermediate points such as pull boxes and joined cable tray segments
- Regularly spaced intervals in closed loop pathways such as cable tray rings
- Partitioned pathways such as partition duct or innerduct. Unique identifiers shall be provided for each segment

A pathways summary report should be available listing all pathways, including their types, origins, destinations, total capacities, and present fill conditions.

14.13.2.4 Records

14.13.2.4.1 Recommendations

A cabinet, rack and frame summary report should be available listing all racks, cabinets, and frames, including their types, locations, sizes, capacities, and current usage status.

A cabling summary report should be available listing all cabling, including their types, uses, pair/strand/port counts, sources, destinations, current pair/strand/port usage, backbone and horizontal cabling port/pair/strand assignments on termination hardware, patching/cross-connection assignments, connected equipment, and unterminated or damaged pairs/strands.

It is also recommended that the database source for the cabling reports be able to provide end-to-end circuit trace connectivity reports from either end or from any intermediate point along the circuit.

A cross-connect summary report should be available listing all cross-connects, including their types, uses, pair/strand/port counts, sources, destinations, current pair/strand/port usage, backbone and horizontal cabling port/pair/strand assignments on termination hardware, and connected equipment.

14.13.2.5 Active Equipment

14.13.2.5.1 Introduction

Active equipment includes switches, routers, hubs, firewalls, multiplexers, servers, external storage devices, and other equipment designed to support data center LANs, WANs, SANs, and computing infrastructure.

14.13.2.5.2 Requirements

All pieces of installed equipment shall have a unique identifier.

All active equipment shall be labeled on the front and back with their identifiers. These labels shall be machine generated and legible.

14.13.2.5.3 Recommendations

• An active equipment summary report should be available listing all pieces of equipment, including their types, uses, location, connected backbone and horizontal cabling port/pair/strand assignments on termination hardware and other connected equipment.

14.13.2.5.4 Additional Information

A two-digit counter or rack unit location can delineate the active equipment in each cabinet, rack, or frame. The equipment is typically designated by the RU at the top of the active equipment. Rack unit numbering should start from the bottom of the usable space in the cabinet or rack.

14.13.2.6 Bonding and Grounding System

14.13.2.6.1 Requirements

The bonding and grounding system and all components of the bonding and grounding system shall be labeled and identified on all “as-built” documentation in accordance with applicable cabling standards being followed and, if applicable, with manufacturer-recommended labeling systems.

14.13.2.6.2 Recommendations

Bonding and grounding system records should:

- Include next scheduled maintenance information. At a minimum, maintenance should include an inspection and test all bonding and ground connections.
- All bonding and grounding system records should be retained and available for review. This should include the maintenance schedule.

14.13.2.7 Electronic Documents**14.13.2.7.1 Recommendations**

Specifications for electronic documentation for the data center should be defined during the design phase and may be contingent on the size and type of the data center.

- Base building—Provide drawings in AutoCAD or similar electronic format.
- Data center—Provide drawings in AutoCAD or similar electronic format.
- Data center utilities – Provide all test results for the data center utilities, including, but not limited to, power, HVAC, and fire detection and suppression systems, in electronic format. These files should be retained.
- Balanced twisted-pair, coaxial, and optical fiber cabling—Provide all balanced twisted-pair, coaxial, and optical fiber cabling schedules and test results in electronic format. The cabling schedule should include the “to-from” information that identifies the connection to each piece of equipment or corresponding connecting hardware. These files should be retained.
- Power cabling—Provide all power cabling schedules in electronic format. The power cabling schedule should include the “to-from” information that identifies the connection to each piece of equipment or corresponding connecting hardware. These files should be retained.
- Cabinet and rack elevations—Provide drawings identifying rack layout and equipment placement in AutoCAD or similar electronic format.
- Active equipment inventory—Provide inventory list of all active equipment in spreadsheets, database(s), drawings, or other approved electronic format.

14.13.2.8 Firestopping**14.13.2.8.1 Recommendations**

A firestopping system should be labeled and should include digital pictures.

Fire detection and suppression systems should be identified on all as-built documents.

Firestop submittals, including manufacturer cutsheets and installation instructions, should be retained and available for review.

14.13.2.9 Alternate Power Systems**14.13.2.9.1 Recommendations**

The data center may contain various emergency power systems necessary for redundancy. These should be identified and be labeled.

All components of the alternate power system shall be labeled and identified on all as-built documentation.

All alternate power system records should be retained and available for review. This should include the maintenance schedule.

14.13.2.10 Change Control**14.13.2.10.1 Introduction**

Access and change control policies and procedures are important elements to consider during the design.

Administration of the data center components is integral to the access and change control policies.

14.13.2.10.2 Requirements

Change control procedures shall be posted and be part of the access requirements. Work shall only be performed after proper approvals.

Change control process shall identify the proper work in progress practices.

Change control process shall include trouble ticket procedures and identify the proper site access as part of the resolution.

Change control procedures shall identify and include all required safety practices.

14.13.3 Intelligent Infrastructure Management

14.13.3.1 Introduction

Intelligent infrastructure management features cabling records updating automatically upon changes of equipment cord or patch cord positions in a given intelligent patching field. The system may be implemented with the addition of an analyzer or scanner able to monitor all the cabling connections within a given distributor or patching field and update the system database.

The intelligent infrastructure management system is composed of patch panels, patch cords, analyzers or scanners, additional cables for connections between analyzers or scanners and the patch panels, and management software usually installed in a dedicated server. Monitored patch panel ports are connected to the analyzer or scanner so that when an equipment cord or patch cord is removed or inserted, the system will detect it and update the software database. Therefore the network administrator will have access to the up-to-date information about the cabling system at any time.

Some benefits of intelligent infrastructure management:

- Physical connections between switch ports and patch panel ports can be monitored in real-time.
- Equipment cord and patch cord connections are stored in a software database.
- Communication with network devices can be implemented through SNMP (Simple Network Management Protocol).

If SNMP is implemented, several network management features can be implemented in the intelligent patching system, such as alarm configurations, messages through e-mail, in case of unauthorized access to the network and other actions according to prior configuration.

- Permits planning of work orders (moves, additions, and changes).

Some potential disadvantages of intelligent infrastructure management:

- Difficult or impossible to retrofit into an existing infrastructure
- Higher cost than an equivalent nonintelligent infrastructure
- May consume additional rack units at locations wherever patching is managed
- Depending on the product selected, manufacturer specific equipment cords or patch cords may be required

The current existing technologies for the hardware of intelligent infrastructure are:

- Micro switches imbedded in the ports of the patch panels. They detect the connection of an equipment cord or patch cord.
- Physical contact between a sensor on the patch panel and an extra contact on the equipment cord or patch cord.
- RFID detection between a sensor on the patch panel and a tag fixed on the equipment cord or patch cord.

Intelligent infrastructure management systems may be implemented using two configurations:

- Interconnection
- Cross-connection

Interconnection configuration is implemented by using sensor strips installed on the Ethernet switch ports to provide them with a means for detection of equipment cord or patch cord connections. Figure 14-23 depicts the interconnection configuration.

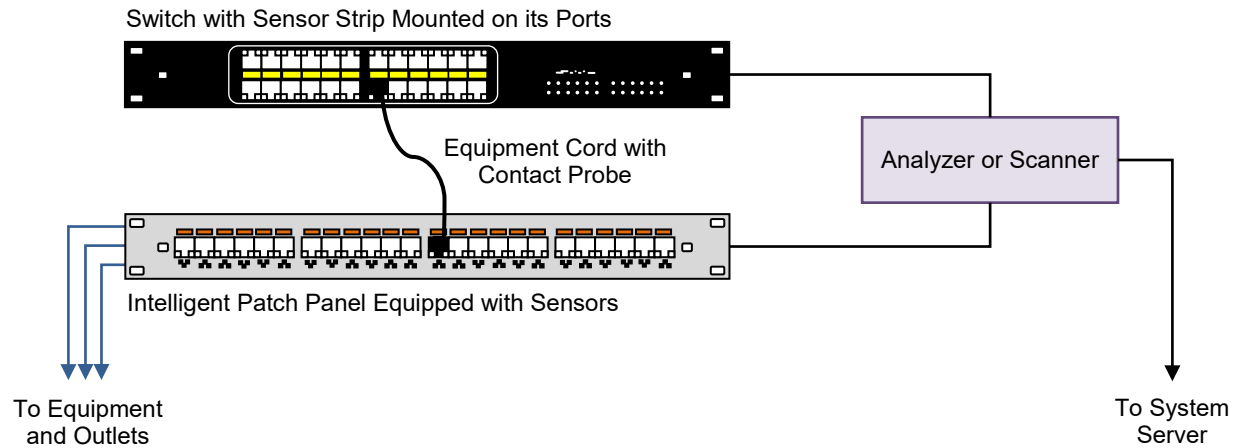


Figure 14-23
Intelligent Infrastructure Management Interconnection Configuration Example

Cross-connection configuration is implemented through a “mirror” patch panel between the Ethernet switch and the horizontal distribution. Switch ports are mirrored in the intelligent patch panel, so connections will be made between patch panel ports only and not between switch ports and patch panel ports. This configuration is especially suitable for systems that operate with sensors or micro-switches for detection of equipment cord or patch cord connections. Figure 14-24 depicts the cross-connection configuration.

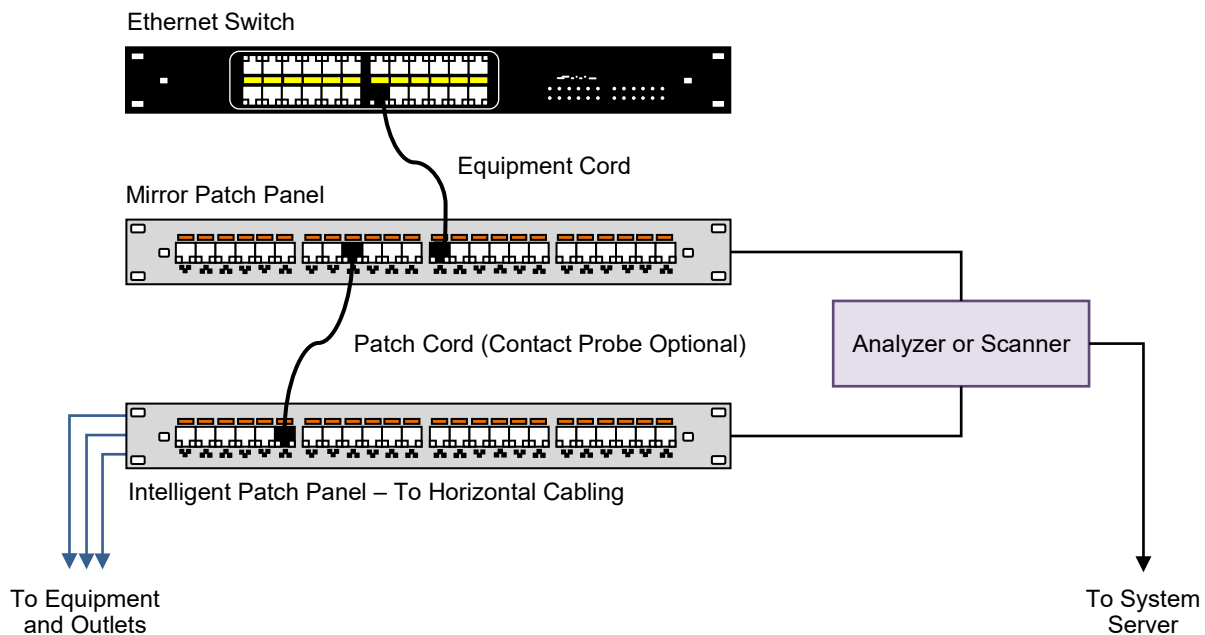


Figure 14-24
Intelligent Infrastructure Management Cross-Connection Configuration Example

15 Information Technology

15.1 Disaster Recovery

15.1.1 Introduction

There are several considerations when developing a disaster recovery plan. Some of the considerations are:

- Offsite data storage
- Colocation facility
- Onsite data storage
- HVAC failure
- Power failure
- Distance between data centers

15.1.2 Offsite Data Storage

15.1.2.1 Cold Site (Recovery Ranging From 24 Hours to 5 Days)

A cold site is typically a leased or company owned disaster recovery facility providing only the physical space for recovery operations. Clients provide their own hardware, software, and network. Depending on the level of services contracted, equipment is either “cold” (stored at the site) or “cool” (powered up but not in service). Clients transfer data on physical media like tape and optical media. The clients can also transfer data over point-to-point communication lines or via secure VPN tunnels directly to the site. Backup data may be transferred to a second off-site facility as well for remote storage of critical data. The “cold” or “cool” site method provides the replication machines, operating systems, and applications required for disaster recovery at significantly less cost than having a full backup data center. However, recovery time may be unacceptable. The cool disaster recovery site should be tested regularly.

15.1.2.2 Warm Site (Recovery Ranging From 30 Minutes to 8 Hours)

A warm site is a backup site having some, but not all, of the components necessary to immediately restore all business functions. During a disaster, obtaining additional hardware and software will delay recovery to some degree. A warm site can function as a second production data center until needed for disaster recovery. Because the warm site must be able to assume the primary site workload, data must be replicated and transferred to the warm site periodically. Generally, the data replication routine can occur anywhere from once every 24 hours to once a week. The data transfer often takes place through a high-speed data connection. In the event of a disaster, the warm site would run on one day or older data unless real-time mirroring of production data occurs. Real-time mirroring is expensive and requires data synchronization management.

15.1.2.3 Hot Site (Recovery Ranging From 1 Minute to 20 Minutes)

A hot site is a fully operational offsite data processing facility equipped with both the hardware and software systems that can very quickly assume the disaster recovery workload. A hot standby site can be used as an active/active data center for certain applications. This can be achieved by replicating the data in a synchronized fashion between the data centers in real time.

A hot standby site can also be used as an active/standby data center for certain applications. To achieve that, the data should be saved in a synchronized fashion but not necessarily in real time.

15.1.3 Colocation Facility

A colocation facility is a data center in which multiple clients lease small portions of the computer room for their computer and network equipment. Companies typically lease anywhere from one cabinet or rack to several cabinets or racks enclosed in a secured fence or by walls. The equipment may be for backup recovery, for remote storage, or even the primary data center for that client. The advantage to the client is having a secured and controlled computer room environment without having to build and maintain a data center. The colocation owner is typically responsible for moving equipment into the spaces (often called cages or suites), setting up customer-provided cabinets or racks, configuring communications equipment, and creating physical security access lists.

The colocation facility owner provides power as required by the client, circuit delivery facilities, and various levels of support. Colocation facilities generally offer high security, including cameras, fire detection and extinguishing systems, multiple connection feeds, filtered power, backup power generators, and other items to ensure high availability, which is mandatory for all web-based, virtual businesses.

15.1.4 Onsite Data Center Redundancy

Redundant pathways are typically designed to eliminate or reduce single points of failure in the cabling infrastructure.

Network equipment redundancy includes redundant routers, core, distribution, service appliances, service modules, access layer LAN/SAN switches, hot-swappable port cards, spare wireless antennas, and power supplies.

15.1.4.1 Requirements

Backup equipment cabinets, racks, and associated hardware are required for recovery of campus area networks and metropolitan area networks; long-haul fiber optic emergency facilities are provisioned for high-bandwidth connectivity to critical sites during disasters.

15.1.4.2 Recommendations

Equipment should be in cabinets supported by branch circuits from different electrical panels or power distribution units. Equipment with multiple power supplies and power cords should be plugged into different branch circuits for power redundancy. For equipment with one power cord, consider plugging the equipment into a rack-mount switch or power strip that is fed from two different branch circuits.

15.1.5 HVAC Failure

Refer to Section 9, *Electrical Systems*, Section 10, *Mechanical* and Section 13, *Data Center Management and Building Systems* for coordination of disaster recovery procedures.

15.1.5.1 Recommendations

Every facility should have a portable HVAC unit and an adequate number of large fans in storage to provide temporary service to critical equipment. Special considerations must be made in advance to ensure that power is available with the correct type of power receptacle. Additional advanced consideration is required for hot air exhaust from portable air conditioning units and properly sized exhaust tubes, including correct lengths. Exhaust tubes and ceiling grid connectors are not necessarily included with portable unit purchases but may be purchased separately.

15.1.6 Power Failure

In general, the power disaster recovery efforts should include a consideration for redundant external power sources, alternate power supply methods, and dedicated UPS units per equipment, equipment rack, or cabinet (see Section 9).

15.1.6.1 Recommendations

Power strips within the equipment cabinets or racks should be IP capable to allow for SNMP monitoring and reactive reporting of power consumption, spikes, dips, and preaction alerts.

Communications devices should support multiple power supplies and be capable of continuous operation in the event that one supply fails, loses power, or requires hot swap.

Ensure that equipment that has dual power supplies is plugged into the upstream electrical distribution. (See Section 9.3.14)

15.1.7 Mirroring

Mirroring is the copying of data from the host system to a second system in real time. Because the data is copied in real time, the information stored on the second system is the same as the information on the host system. Data mirroring is critical for the speedy recovery of critical data after a disaster. Data mirroring can be implemented locally or offsite at a remote data center or colocation facility. When copying data offsite, it is important to consider the form of transmission used, as bandwidth and delay affect the performance and capacity of the mirroring or replication. Transmission methods such as ISDN PRI, T-1, T-3, E-1, E-3, ATM, Gigabit Ethernet, SONET, SDH, and DWDM are commonly employed.

15.1.8 Location of Real-Time Redundant Storage Device

The location of the redundant storage devices is critical. Possible locations include housing the equipment in the same room, the same building, on campus, or off-site. Considerations include the need to have quick access to the backup equipment for maintenance, disaster recovery timelines and policies, and security levels of protection of the stored information. Other considerations include the financial and criticality aspects of maintaining real time, redundant databases.

15.1.8.1 Recommendations

It is generally desirable for redundant storage to be located off-site in a location far away enough to avoid losing both copies during a single disaster. It should be noted, however, that many data replication methods have distance limitations.

15.1.9 Physical Connectivity Methods and Devices

Physical connectivity can take many forms (e.g., conventional copper, optical, satellite). Conventional methods include copper connections between devices within the same cabinet, rack, row, or room. While this is the most economical, equipment must be located within a limited distance not to exceed constraints that may limit bandwidth. Other methods can increase the distance and speed of replication; however, there is an inherent increase in costs associated with these methods, which include, but are not limited to, long-haul Ethernet, carrier MPLS networks, ATM, SONET, and DWDM.

15.1.10 RAID

Short for redundant array of independent (or inexpensive) disks, a category of disk drives that employs two or more drives in combination for fault tolerance and performance. RAID disk drives are used frequently on servers but are not generally necessary for personal computers.

There are number of different RAID levels:

- Level 0: striped disk array without fault tolerance—provides data striping (spreading out blocks of each file across multiple disk drives) but no redundancy; this improves performance but does not deliver fault tolerance. If one drive fails, then all data in the array is lost.
- Level 1: mirroring and duplexing—provides disk mirroring. Level 1 provides twice the read transaction rate of single disks and the same write transaction rate as single disks.
- Level 2: error-correcting coding—not a typical implementation and rarely used, Level 2 stripes data at the bit level rather than the block level.
- Level 3: bit-interleaved parity—provides byte-level striping with a dedicated parity disk. Level 3, which cannot service simultaneous multiple requests, also is rarely used.
- Level 4: dedicated parity drive—a commonly used implementation of RAID, Level 4 provides block-level striping (like Level 0) with a parity disk; if a data disk fails, the parity data is used to create a replacement disk. A disadvantage to Level 4 is that the parity disk can create write bottlenecks.
- Level 5: block interleaved distributed parity—provides data striping at the byte level and stripe error correction information; this results in excellent performance and good fault tolerance. Level 5 is one of the most popular implementations of RAID.
- Level 6: independent data disks with double parity—provides block-level striping with parity data distributed across all disks.
- Level 7: A trademark of Storage Computer Corporation that adds caching to Levels 3 or 4.
- Level 0 + 1: a mirror of stripes—not one of the original RAID levels, two RAID 0 stripes are created, and a RAID 1 mirror is created over them; used for both replicating and sharing data among disks.
- Level 10: a stripe of mirrors—not one of the original RAID levels, multiple RAID 1 mirrors are created, and a RAID 0 stripe is created over these.

15.1.11 Distance Between Data Centers

The synchronous replication of data and accessing of that data by applications between two or more data centers is dependent on the distance between the data centers. The latency increases as the distance increases. The latency should be limited so that application or the data replication write functions can show acceptable performance.

15.2 Channel and Console Cabling

15.2.1 Introduction

System consoles should be networked over private IP address space and accessible from the operations center. Providing this type of architecture enables a 'lights-out' operation in that personnel do not need to be in the computer room, except when human intervention is necessary.

15.2.2 Mainframe Channel Cabling

15.2.2.1 FICON

Fiber Connection (FICON) is a high-performance protocol. FICON channels enable 100-Mbps of bidirectional link rates at distances up to 20 km over optical fiber cables. In addition, an I/O interface for mainframes supports the characteristics of existing and evolving higher speed access and storage devices.

In summary, FICON products—from IBM—use a mapping layer that is based on the existing ANSI standard, Fibre Channel-Physical and Signaling Interface (FC-PH). FC-PH specifies the physical signaling, cabling, and transmission speeds for Fibre Channel.

Each FICON channel is capable of supporting more than 4,000 I/O operations per second, which allows each channel to support the same capacity as up to eight Enterprise Systems Connection (ESCON) channels.

Disaster recovery functions, such as tape vaulting, remote disk copy and geographically dispersed parallel Sysplex (which are multiple mainframes strapped together as a single unit) benefit from the large distance supported by FICON channels. Although direct links between FICON devices of 10 kilometers are supported, 20-kilometer links are possible under certain conditions. The FICON protocol also permits additional end-to-end error checking above that provided by the FC-PH transport.

FICON is also designed to support a mixed workload. Small data transfers, typical for transactions, do not have to wait for large data transfers to complete.

Instead, they are multiplexed on the link with the long running operations. This helps to simplify configurations and removes one of the inhibitors to having a single database for transaction processing and business intelligence workloads.

15.2.2.2 ESCON

Enterprise System Connection (ESCON) is an IBM optical fiber channel connection technology that provides 17-MB/sec throughput. ESCON provides direct channel-to-channel connections between mainframe systems and peripherals over optical fiber links at distances up to 60 kilometers (36 miles). It also provides a way for communication controllers and other devices to share a single channel to a mainframe.

Compared to the copper-based parallel bus and tag channels, ESCON provides greater speeds and uses a serial interface. An ESCON Director is a hub-and-spoke coupling device that provides 8-16 ports (Model 1) or 28-60 ports (Model 2).

15.2.2.3 Small Computer System Interface (SCSI) Channel Cabling

The term "SCSI cable" usually refers to a complete cable, including the wire, connectors, and possibly a terminator as well. A number of different types of cables are available with various connector types to create specific cable implementations.

SCSI cables come in two distinct varieties: external and internal. External cables are used to connect SCSI devices that do not reside inside the PC; rather, they have their own enclosures and power supplies. Internal cables connect SCSI devices installed within the system enclosure. These cables are different in construction, primarily because the external environment represents much more of a risk to data corruption. This means external cables must be designed to protect the data traveling on the cable. Internal cables do not have this problem because the metal case of the cabinet shields the components inside from most of the electromagnetic and radio frequency noise and interference from the "outside world." Thus, internal cables can be made more simply and cheaply than external ones.

External cables are commonly called shielded cables because they are made specifically to protect the data they carry from outside interference. They have a very specific design in order to ensure that data traveling on the cable is secured, including the following properties:

- **Twisted-pair wiring**—All the wires in the cable are formed into pairs, consisting of a data signal paired with its complement. For single-ended signaling each signal is paired with a signal return or ground wire. For differential signaling each "positive" signal is paired with its corresponding negative signal. The two wires in each pair are twisted together. The twisting improves signal integrity compared to running all the wires in parallel to each other. A cable with 50 wires actually contains 25 pairs, and a 68-wire cable contains 34 pairs. This type of wiring is also commonly used in other applications, such as network cabling, for the same reason.
- **Shielding**—The entire cable is wrapped with a metallic shield, such as aluminum or copper foil or braid, to block out noise and interference.
- **Layered structure**—The pairs of wires are arranged in layers. The core layer of the cable contains the pairs carrying the most important control signals, REQ and ACK (request and acknowledge). Around the core pairs, other control signals are arranged in a middle layer. The outer layer of the cable contains the data and other signals. The purpose of this three-layer structure is to further insulate the most important signals to improve data integrity.

External cables have a round cross-section, reflecting the circular layers mentioned just above. These cables are not simple to manufacture, and external SCSI cables are generally quite expensive. For internal cables, special steps are not required to protect the data in the wires from external interference. Therefore, instead of special shielded multiple-layer construction, internal devices use unshielded cables. The internal device unshielded cables are flat ribbon cables similar to those used for floppy drives and IDE/ATA devices. These are much cheaper than external cables to make.

Even with internal cables, there are differences in construction (beyond the width issue, 50 wires for narrow SCSI or 68 wires for wide SCSI). One issue is the thickness of the wires used; another is the insulation that goes over the wires. Better cables generally use Teflon as a wire insulation material, while cheaper ones may use PVC. Regular flat cables are typically used for single-ended SCSI applications.

For Ultra2 or faster internal cables using LVD signaling, the poor electrical characteristics of flat ribbon cables begin to become an issue in terms of signal integrity, even within the PC. Therefore, a new type of internal ribbon cable was created that combines some of the characteristics of regular internal and external cables. Pairs are twisted between the connectors on the cable as with external cables, but the ribbon remains flat near the connectors for easier attachment. Ultra2 pair twisting improves performance for high-speed SCSI applications. While pair twisting increases cost, Ultra2 cables are not as expensive as external cables. This technology is sometimes called "twist-n-flat cable" since it is a partially flat and partially twisted pair.

There are several variations of the SCSI cable, each with its own limitations:

- **Single-ended (SE) SCSI**—Most SCSI devices use SE SCSI signaling. In SE SCSI, each signal is carried by a single wire. SE SCSI is very susceptible to noise and has a rather short distance limitation, a maximum of 6 m (20 ft).
- **Differential SCSI (also called high-voltage differential [HVD] SCSI)**—Differential SCSI is incompatible with SE SCSI above because it uses differential signaling rather than single-ended signaling. The benefit of using differential SCSI is that it works well in noisy areas and can reach up to 25 m (82 ft) in distance.
- **Low-voltage differential (LVD) SCSI**—LVD is the newest type of SCSI cabling. LVD SCSI specifications offer distances up to 12 m (39 ft) and legacy support of LVD/SE which offer LVD mode or SE mode. Most LVD SCSI devices are LVD/SE. However, the link can only run in SE mode or LVD mode. If one device on the SCSI bus is SE, all devices will be limited to SE limitations. All devices must be set to LVD to achieve LVD distance and speed capabilities. Note that LVD SCSI cabling requires twist and flat ribbon cable and a LVD/SE terminator or a twist and flat ribbon cable with built-in LVD termination.

15.2.2.4 Serial Console Cabling in the Computer Room and Operations Center

15.2.2.4.1 Recommendations

The following recommended maximum distances for serial console connections using EIA/TIA-232-F and EIA/TIA-561/562 are as follows:

The recommended maximum distances for EIA/TIA-232-F and EIA/TIA-561/562 console connections up to 20 kb/s are approximately:

- 23 m (76 ft) over Category 3/Class C balanced twisted-pair cabling.
- 27 m (90 ft) over category 5e/class D or category 6/class E balanced twisted-pair cabling.

The recommended maximum distances for EIA/TIA-232-F and EIA/TIA-561/562 console connections up to 64 kb/s are:

- 8 m (27 ft) over Category 3/Class C balanced twisted-pair cabling.
- 10 m (31 ft) over category 5e/class D, category 6/class E or higher balanced twisted-pair cabling.

15.2.2.5 KVM Switches

15.2.2.5.1 Introduction

A keyboard, video, mouse (KVM) switch allows a single keyboard, video display monitor, and mouse to be switched to any of a number of computers when typically a single person interacts with all the computers but only one at a time. The switch provides more table space in addition to saving the cost of multiple keyboards and monitors. KVM switches are commonly used at Web and other server locations with multiple computers but usually by a single administrator or Webmaster.

IP protocols are also advancing into KVM switching systems that are used to access server consoles remotely. IP KVMs allow users to remotely control server screens via Web browsers. Wireless KVM solutions are also available. The systems encapsulate KVM signals into Ethernet packets for wireless transmission over the 802.11 wireless LANs. For large data centers, this means saving on KVM cabling and cable management as well as more flexible server control. Security is provided through wireless LAN encryption or by using proprietary protocols.

15.2.2.5.2 Recommendations

Consider using integrated KVM or console consolidation systems to avoid the need for keyboards, monitors, and mice for every system or rack. IP-based systems allow servers to be managed over the network, allowing support staff to be located away from the data center. However, these systems should incorporate security to ensure that only authorized personnel have console access to the servers.

15.3 Communications

15.3.1 Wired/Wireless/Hands-Free Voice Communications

15.3.1.1 Introduction

Data center employees spend a lot of time during the day working on multiple systems within multiple cabinets or locations in the data center or adjoining facility. Efficient voice communications is a critical consideration when designing the data center. During critical down times, employees working to repair the system should not need to worry about where the nearest telephone is.

The communications industry provides several methods of technology to consider for this situation, including:

- Wired:
 - Desktop
 - Wall mounted
 - Rack mounted
 - Intercom devices
- Wireless:
 - Analog
 - Cellular
 - VoIP
 - Hands free

Advancements in wireless data technology and digital voice systems permit voice and data systems to share the same wireless system.

An intercom device can be designed in conjunction with overhead speakers and ceiling mounted microphones to provide hands-free communication between the data center staff and support space. The intercom system can also be a very effective form of access control and can be integrated with video and the appropriate door release hardware.

Wireless equipment may not work well in a shielded computer room.

15.3.1.2 Recommendations

When using a wireless VoIP system, one of the more important tasks to perform prior to designing a wireless deployment is to conduct a wireless site survey. This survey will verify that wireless antenna coverage is adequate to provide appropriate Quality of Service (QoS) for voice and data applications.

- One note of caution when considering 2-way radios within the data center; some fire suppression systems contain blasting caps that are used to “fire” the release pin on the suppression media tank in the event of a fire. Construction sites use similar explosive caps. Signs are often posted when approaching road construction, which provides warning to turn off two-way radios and cell phones. These caps can be triggered by certain frequencies. Therefore, it is advised that prior to using two-way radio communications in the data center that the fire suppression provider be contacted. The manufacturer or installation contractor will be able to specify if two-way radios can be used in or near the data center. It is further recommended that a NO RADIO ZONE be established of a size as determined by the manufacturer if the data center is using a blasting cap type system (see Figure 15-1).

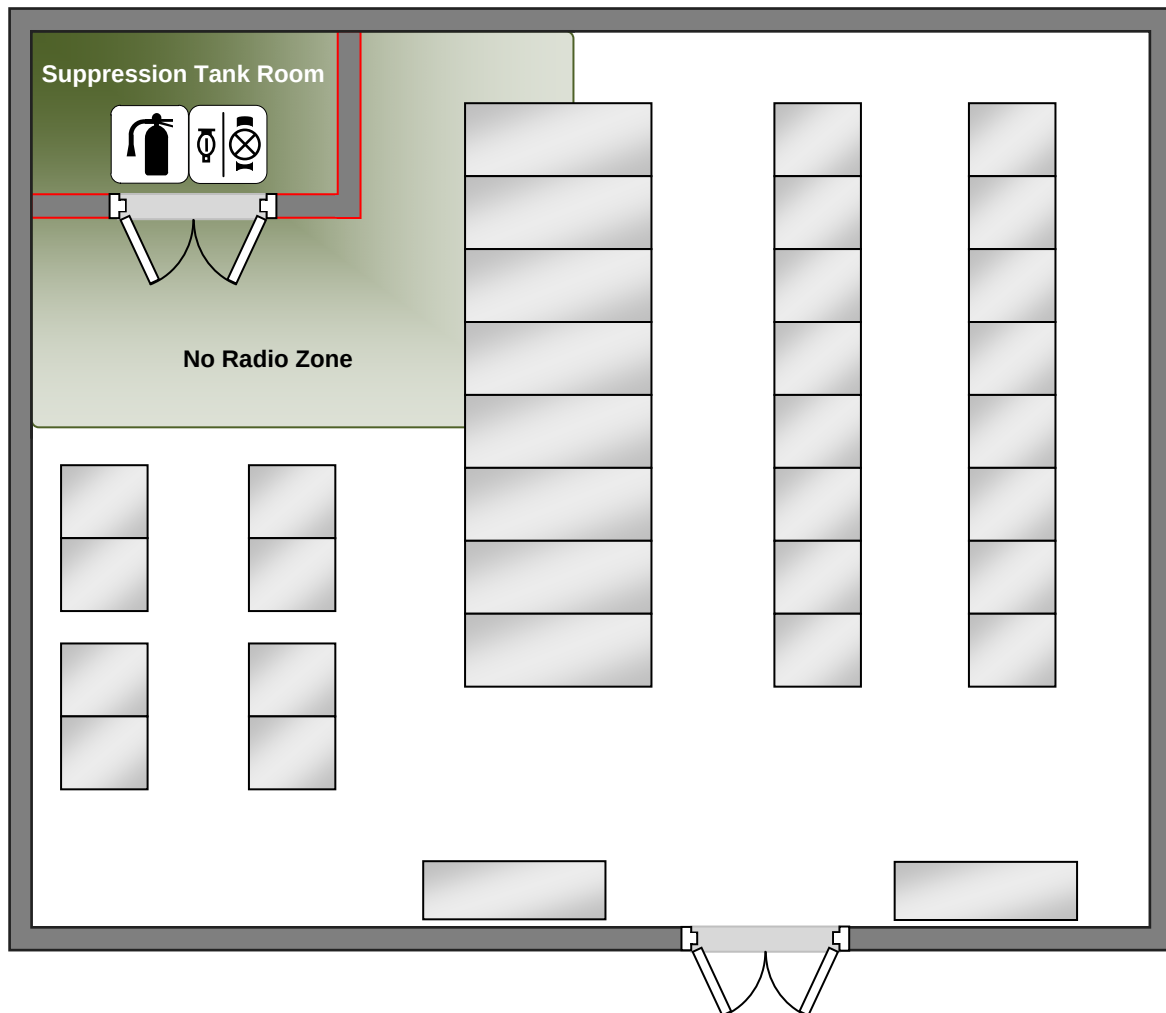


Figure 15-1
No Radio Zone Around Suppression Tank Room

15.3.2 Wireless Network for Portable Maintenance Equipment

15.3.2.1 Recommendations

With the growing size and complexities of today's data centers, the designer should take advantage of the advancements in wireless technology to potentially provide a redundant maintenance network:

- Personal digital assistant (PDA)
- Tablets
- Scanners—asset tracking

15.3.3 Zone Paging

15.3.3.1 Introduction

While overhead paging can be one of the more primitive forms of communication, it can still be very effective for regionalized voice contact in such areas as:

- Network operations center
- Support space
- Computer room

15.4 Computer Room Layout

15.4.1 Introduction

Computer room layout is affected by cable length restrictions for channel cabling, console cabling, LAN, SAN, and WAN cabling.

15.4.2 Equipment Configuration for Efficiency

15.4.2.1 Recommendations

- Hot and cold aisles:
 - Minimize the reintroduction of hot air into rack and equipment cold air intake vents by using blanking panels.
 - Minimize the loss of the necessary static pressure under the access floor by means of dampers, brushes, or other means to seal cable cutouts and other openings in access floor tiles.
- Dedicated application rows
- Dedicated equipment type areas:
 - The concept of rows containing the same type equipment is a best practice method for both connectivity and airflow. From a connectivity perspective, some equipment is inherently fiber-connected, some copper connected, and some equipment uses proprietary cabling and share proprietary peripherals. By aligning same type equipment, the designer may be able to limit the use of proprietary cabling in cable pathways.
 - From an airflow perspective, having the same type of equipment cabinets or racks in rows helps keep a consistent airflow around equipment, allows for ease of hot/cold aisle design, and better prepares the computer room for portable cooling if necessary.
 - Consider separate areas of the computer room for rack-mounted and floor-standing systems to simplify cabling and the management of cabinets and racks.
 - Develop a small number of standard cabinet and rack cabling configurations for the computer room to simplify cable installation and administration.

15.4.3 Connectivity Panel Distribution

15.4.3.1 Introduction

Refer to the most recent version of the relevant standards and reference manuals (e.g., BICSI *TDMM*, TIA-942-A, ISO/IEC 11801) for information on standards-based cabling distance limitations:

- Copper and fiber panel distribution
- Dedicated network connectivity rack area
- Distributed connectivity racks:
 - Standards-based rack
 - Standards-based cabinet
 - Underfloor
- Dedicated panels for each equipment cabinet or storage device

15.4.3.2 Recommendations

Figure 15-2 is a representation of simple connection topography for a data center. The connections shown can be copper or optical fiber so long as standards are not violated. Points to remember:

- Stay within recommended lengths.
- Check the AHJ on plenum issues for computer rooms.
- If running above the floor, watch for distance limitations from fire suppression elements (check with AHJ).
- If running under the floor, stay under aisle ways and do not run media under static equipment.
- Keep all runs at 90° turns (not violating bend radius); do not run media on an angle across the room.
- Map out all pathways and provide updated copies to computer room managers.
- If using underfloor cable tray, check with the floor and cable tray manufacturer for best practices regarding stanchion attachment.

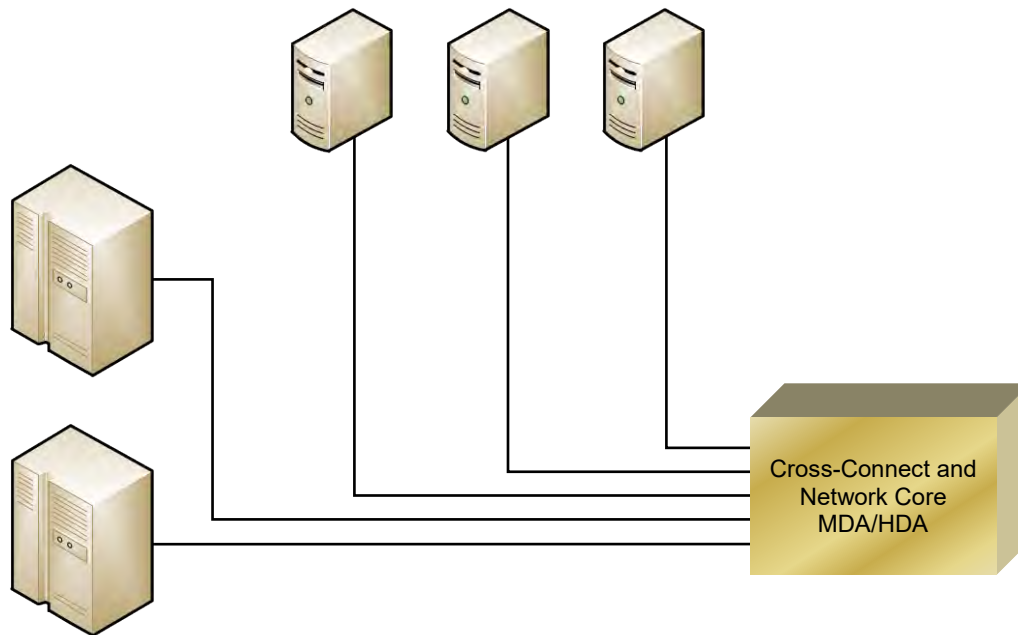


Figure 15-2
Simple Connection Topology

Figure 15-3 shows the basic representation of zone distribution. A zone distribution area can be housed above the floor in an equipment rack or below the floor in an access box. Each method has both advantages and disadvantages. When housed above floor, the connections are easier to access for connection and maintenance. However, the above floor methods use floor space that would otherwise be available for equipment. Below floor methods provide better security and maximize above floor space. However, installing zone boxes under the floor requires proper planning. The network team and the data center management need to agree on long-term commitments regarding placement of the remote distribution units as moving them is difficult in terms of the organization allowing for the necessary downtime. In addition, data center space planners need to understand that equipment cannot be placed on top of underfloor zone distribution areas.

Figure 15-4 represents a redundant topology using redundant zone distribution areas. Notice that two totally separate pathways are used to keep maximum separation of the cabling from each ZDA.

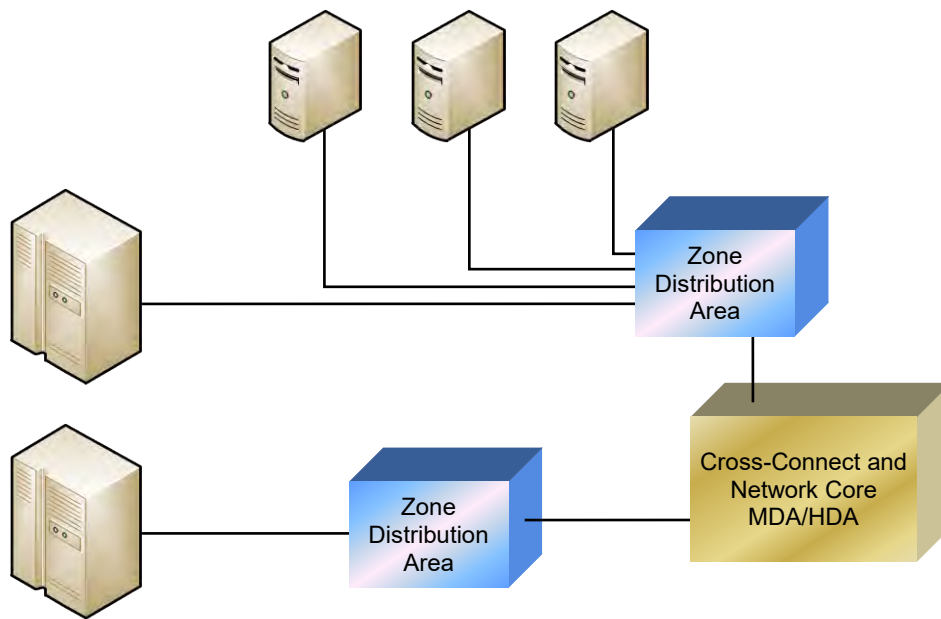


Figure 15-3
Sample Zone Distribution Topology

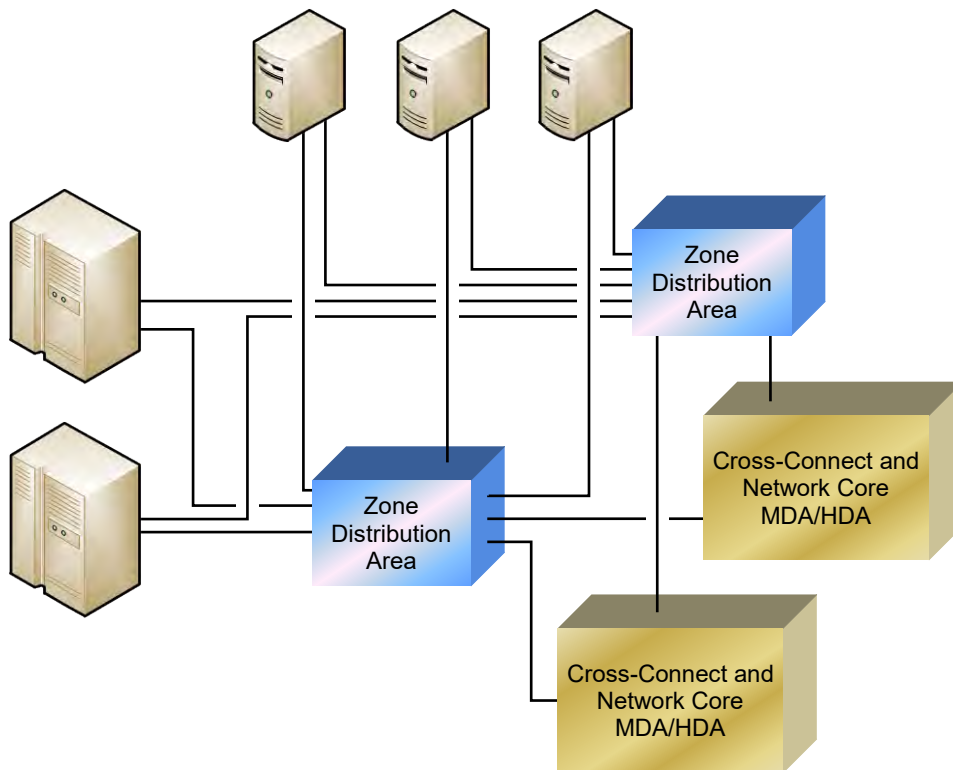


Figure 15-4
Sample Redundant Topology

15.4.3.3 Adequate Material Storage

15.4.3.3.1 Recommendations

The planner should account for enough storage for emergency parts and equipment to minimally maintain the data center in an event. Items could be stored in the following areas:

- Network operations center
- Computer room
- Tape drives
- Hot swappable devices
- Patch cords
- Test equipment
- In row
- Off-site or out of room staging area

15.4.4 Aisle Sizing and Workflow Analyses for Proper Walkways and Egress Pathways

15.4.4.1 Recommendations

It is suggested that the walkways be designed to accommodate the following requirements:

- Cabinet portability
- HVAC maintenance
- Accessibility and emergency egress—refer to Section 7

15.5 Operations Center

15.5.1 Monitoring of Building Systems

15.5.1.1 Introduction

Refer to Section 10 and Section 13 for coordination. In general, monitoring systems should be available within the operations control center.

For more information about the monitoring of security cameras and access control devices, refer to Section 12.

15.5.2 Location

15.5.2.1 Recommendations

System consoles should be networked over private IP address space and accessible from the operations center, so operations personnel do not have to be in the computer room except in cases when human intervention is necessary.

The operations center should be located adjacent to the computer room with a viewing window if possible to provide visual communications.

The center should be equipped with large screen displays for system/network tools (e.g., power consumption, computer room humidity, temperature).

15.6 Network Infrastructure Reliability

15.6.1 Overview

The network architecture data center services layer is a critical system supporting the critical business applications. The network architecture must not only be designed to support all the applications and anticipated bandwidth requirements in a scalable manner to accommodate future growth in applications, hosts, and data storage, but also accommodate all these requirements with the level of redundancy that is in alignment with the business objectives. The level of redundancy must be maintained from the initial day-one requirements to the ultimate port counts and bandwidth requirements in a scalable manner.

The level of redundancy must also be aligned across the enterprise. Data centers implemented with single path networks on non-redundant chassis within the data center LAN (representing multiple single point of failure), while connecting to multiple redundant WAN service providers with redundant access circuits. This misalignment either results in excessive WAN service provider recurring costs not required for lower performance objectives or a higher than acceptable risk associated with single points of failure within a data center LAN with higher performance objectives, depending on the targeted overall data center class objective.

The network architecture service layer consists of:

- Internet: The internet network services layer ranges from single link internet access from one service provider to redundant internet access across two or more service providers.
- Wide Area Network (WAN): The WAN network services layer provides network connectivity from the data center to secondary data center(s), other corporate office locations, and possibly key remote partner or customer locations. Services range from a single link from a service provider to redundant circuits/networks from multiple service providers.
- Metropolitan Area Network (MAN): The MAN network services layer provides network connectivity from the data center to secondary data center(s), other corporate office locations, and possibly key remote partner or customer locations, all within a common metropolitan area. MAN services can be implemented using a service provider's network services, leasing dark fiber from vendors or customer-owned fiber optic outside plant distributed throughout the MAN. Services range from a single link to redundant circuits/networks from multiple service providers, leased dark fiber vendors, or customer-owned fiber optic outside plant.
- Local Area Network (LAN): The LAN network services layer consists of the network connectivity within the data center interconnecting the processing systems to the Internet, WAN, and MAN network services. LAN services range from single link connectivity throughout the LAN to redundant connections from the processing systems to the Internet, WAN, and MAN.
- Storage Area Network (SAN): The SAN network services layer consists of the network connectivity within the data center interconnecting the data storage systems to the processing systems and WAN and MAN network services for off-site replication. SAN services range from single link connectivity throughout the SAN to redundant connections from the data storage systems to the processing systems and to the WAN and MAN. For converged SAN/LAN systems, the level of redundancy must meet the minimum requirements of either the LAN or SAN network services.

NOTE: All redundant internet, WAN or MAN network services provisioned over a collapsed ring, common sheath, common pathway, or any other implementation resulting in common modes of failure between the redundant network services are considered "single link". An example is a ringed topology network implemented with full or partial collapsed rings.

For the network architecture reliability classes, the corresponding class designation is prefaced with an "N" to identify it represents the "Network" reliability criteria.

15.6.2 Network Infrastructure Availability Classes

15.6.2.1 Introduction

The following network architecture examples merely represent one example. Any network architecture that meets the intent of, and can validate the performance characteristics of, any network reliability Class would achieve that particular Class rating. While there are generally a few industry accepted, commonly applied redundant LAN/SAN network topologies that meet the higher levels of reliability Class, there are many WAN/MAN network topologies that can meet the higher levels of reliability Class. Options exist such as redundant services across multiple access provider vendors or provisioned across redundant services from one access provider vendor. It is important that the data center designer validate that the redundant systems or services meet the performance characteristics defined by the network reliability Class. This would include validating logical and physical diversity from the data center throughout the WAN/MAN or to the Internet backbone, not simply to the nearest Central Office (CO).

15.6.2.2 Availability Class N0 and N1

Downtime will result from planned and unplanned events. Downtime of several days has minimum impact on the enterprise. Network services are single link from one service provider.

Table 15-1 provides tactics for Class N0 and N1, and Figure 15-5 shows an example of a Class N0 and N1 infrastructure.

Table 15-1 Tactics for Class N0 and N1

Internet:	Internet access from one service provider via single link.
WAN/MAN:	Single link connection from one service provider.
LAN/SAN:	Single link connections throughout network.

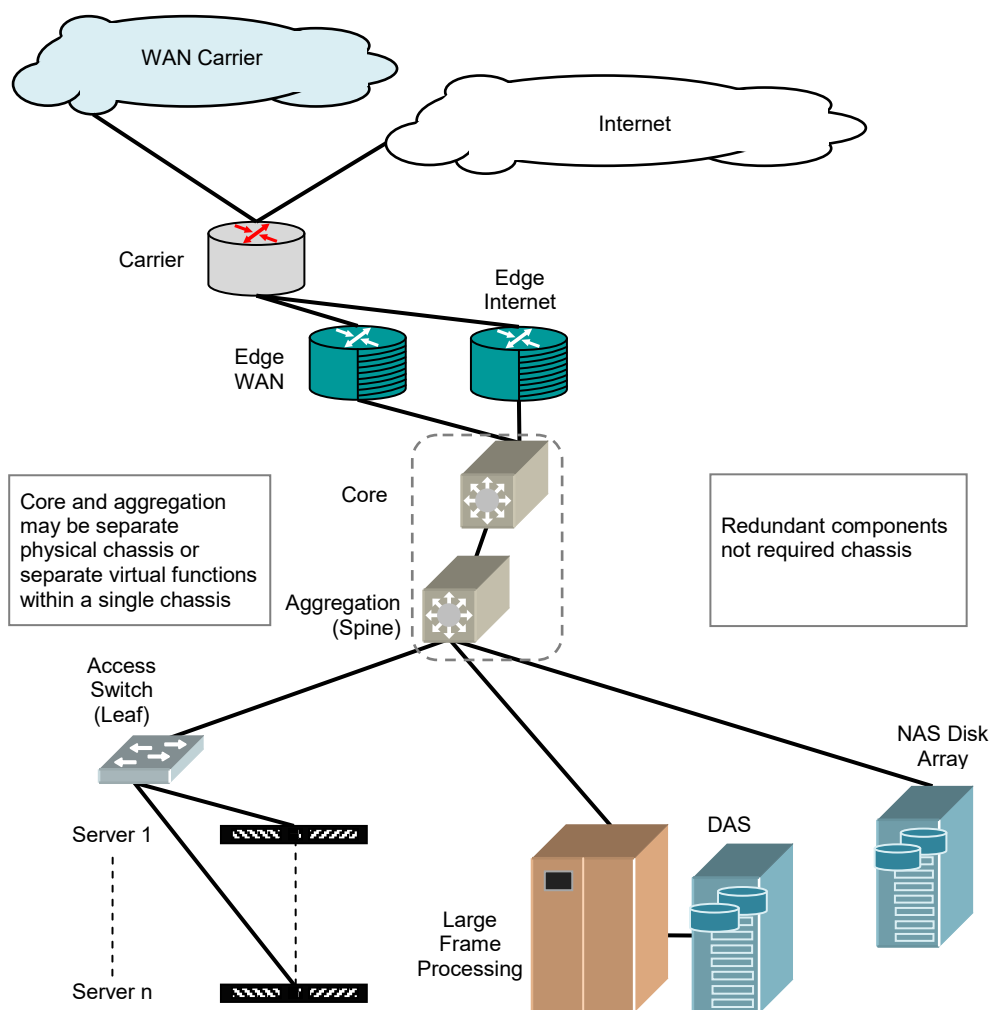


Figure 15-5
Class N0 and N1 Network Infrastructure

15.6.2.3 Availability Class N2

Class N2 provides a higher level of redundancy to reduce risk of downtime because of failure of critical components with low MTBF. Downtime may result from planned and unplanned events. Downtime of several hours or a couple of days has minimum impact on the enterprise. Network services are single link throughout the LAN/SAN but multi-path from core network to the WAN/MAN.

Table 15-2 provides tactics for Class N2, and Figure 15-6 shows an example of a Class N2 infrastructure.

Table 15-2 Tactics for Class N2

Internet:	Two Internet service providers each with a single local access circuit or a single Internet service provider with either a protected or redundant local access circuits.
WAN/MAN:	Non-redundant circuits from two service providers or a redundant or protected circuit from one service provider.
LAN/SAN:	Single link connections throughout network with redundant critical components such as power supplies, supervisors, or NIC teaming for failover.

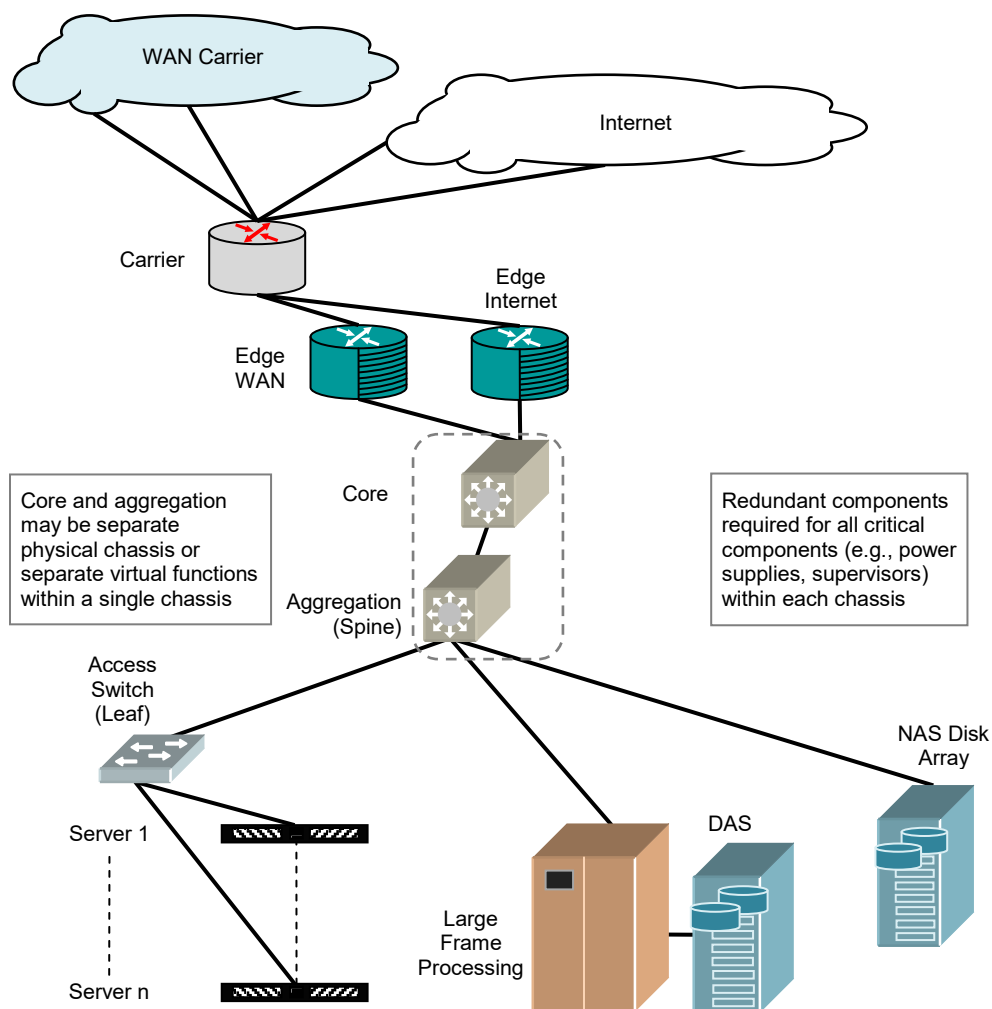


Figure 15-6
Class N2 Network Infrastructure

15.6.2.4 Availability Class N3

Additional redundancy is provided to reduce the risk of downtime due to human-error, natural disasters, planned maintenance, and repair activities. Network services are provided with redundant links throughout the network from the processing systems to all upstream network devices and network services.

Table 15-3 provides tactics for Class N3, and Figure 15-7 shows an example of a Class N3 infrastructure.

Table 15-3 Tactics for Class N3

Internet:	Two Internet service providers each with a single local access circuit or a single Internet service provider with either a protected or redundant local access circuits.
WAN/MAN:	Non-redundant circuits from more than two service providers or redundant or protected circuits from two service providers. Leased fiber or customer owned fiber optic outside plant can be implemented in lieu of network services from service provider.
LAN/SAN:	Redundant links and chassis in network from access switches to all upstream network devices; redundant components not required for links and chassis with redundant systems.

15.6.2.5 Availability Class N4

Redundancy is provided throughout the data center network and external network services to reduce the risk of downtime as a result of human-error, natural disasters, planned maintenance, and repair activities. Network services are provided with redundant links throughout the network from the processing systems to all upstream network devices and network services. Redundant critical components provided within critical links and systems.

Table 15-4 provides tactics for Class N4, and Figure 15-8 shows an example of a Class N4 infrastructure.

Table 15-4 Tactics for Class N4

Internet:	Two Internet service providers both with redundant or protected local access circuits.
WAN/MAN:	Multiple circuits from multiple service providers each utilizing redundant or protected local loops. Leased fiber or customer-owned fiber optic outside plant can be implemented in lieu of network services from service provider.
LAN/SAN:	Redundant links, components, and chassis in network from access switches to all upstream network devices.

In reality, there may be very little difference in cost between Class 3 and Class 4 Network architectures. Adding redundant components such as power supplies, supervisors, etc. to implement a Class 4 solution does not normally represent a significant cost increase. However, we are presenting an example of the minimum requirements to meet the performance characteristics of each given Class.

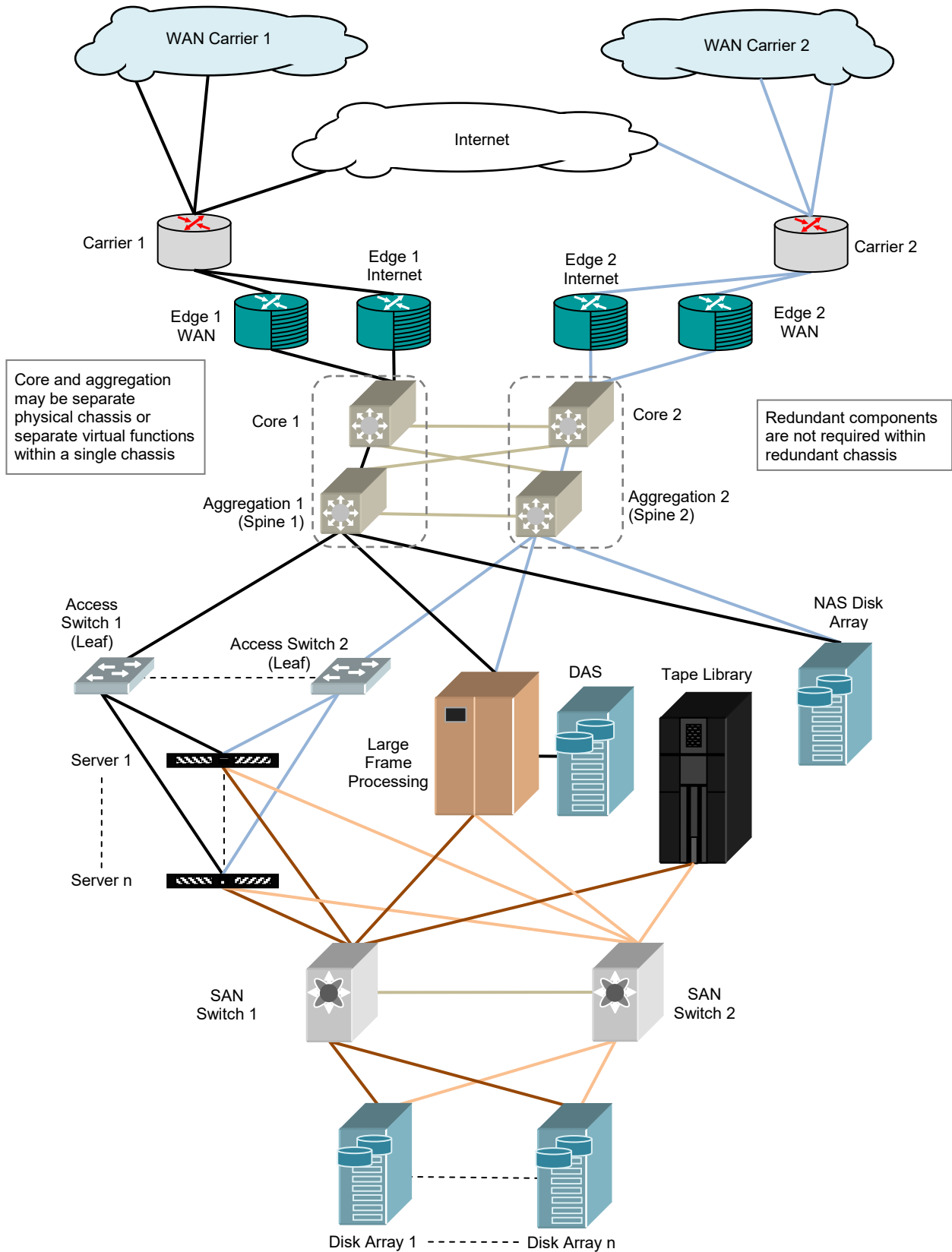


Figure 15-7
Class N3 Network Infrastructure

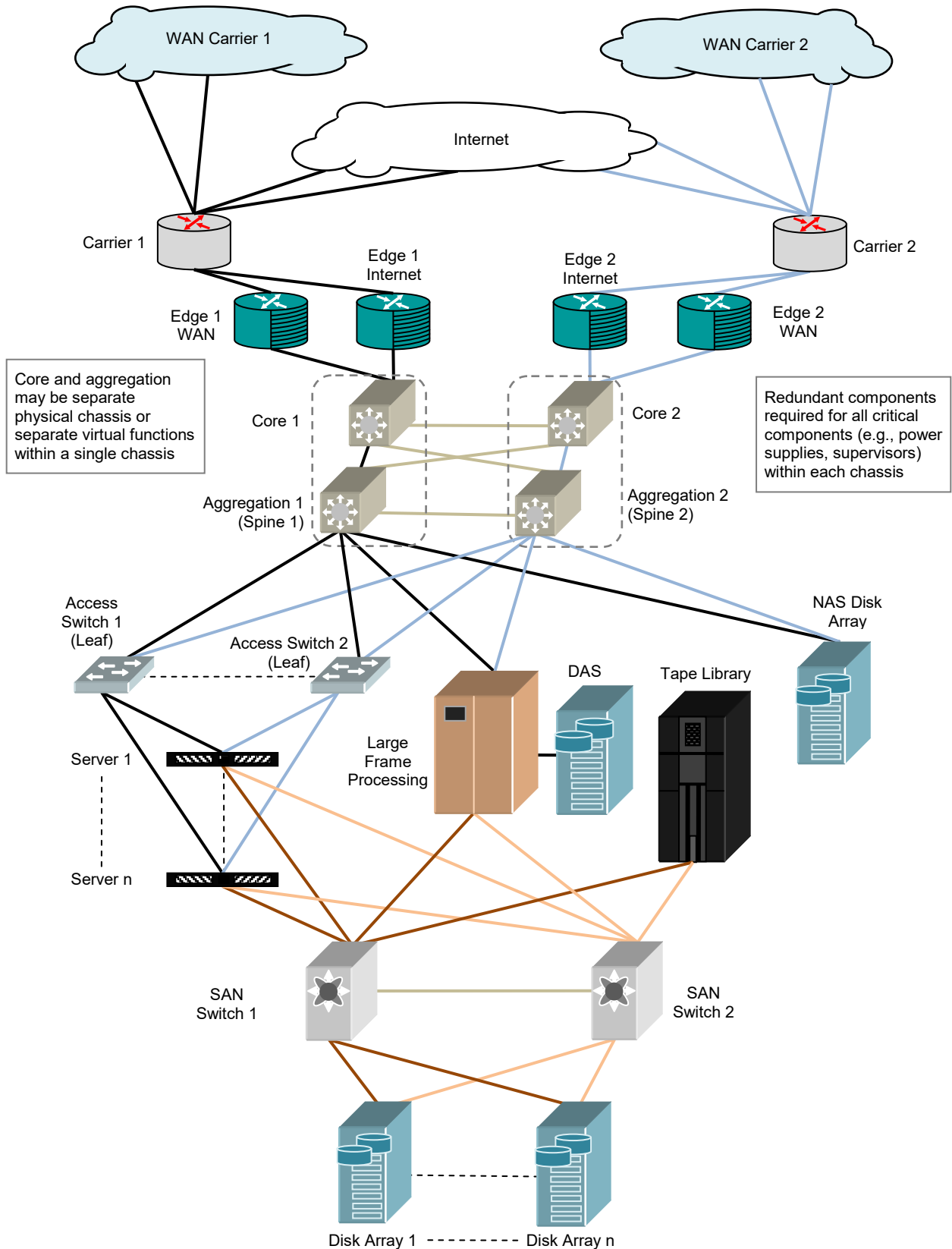


Figure 15-8
Class N4 Network Infrastructure

15.7 Network Security for Facility and IT Networks

15.7.1 Overview

There are several networks within the data center beyond the core computer room Ethernet local area or Fiber Channel storage area network. Networks within the data center are made up of discrete IT and facility system networks. Often, the implementation of these networks are planned, designed, installed, and managed by individual departments with little or no communication between the groups, resulting in a lack of coordination and a common set of guidelines or standards.

The networks can be categorized into three main systems:

- Computer Room Networks:
 - Server and NAS Ethernet LAN
 - Storage Fiber Channel SAN
- Building Desktop Networks:
 - Desktop PCs
 - VoIP Telephones
- Facility Building Automation System (BAS) Networks:
 - HVAC Controls
 - Fire Alarm
 - Physical Security
 - Computer Room Power Monitoring
 - Electrical Distribution Control
 - Lighting

Although these network categories are discrete in their topology, they do interface through BMS or DCIM tools to provide key management functionality for data center facility managers, computer operators, and network administrators. It is important that these networks are planned and designed in a coordinated effort to ensure:

- It is clearly understood which staffing roles require access to each network
- Who is responsible to manage each network
- Who is responsible to manage the interfaces between the networks and what levels of security are required at each network interface
- Who is responsible to manage each network, hardware platforms, and operating systems
- Who is responsible to install each network cabling infrastructure pathways

Once these questions have been answered the data center designer can begin to identify where the hardware and core network components should be located, how they are interconnected (if required), and how logical security will be provided.

NOTE: See Section 13 for further information on DCIM and building systems.

15.7.2 Requirements

The configuration of the non-computer room networks shall have logical security that isolates each of these non-computer room networks from each other and from the critical and data sensitive computer room network.

15.7.3 Recommendations

Each of the discrete systems may have server based control logic which raises the question, “Where should non-IT servers be physically located?” If the non-IT servers are not managed by the IT department, it is not recommended that they be located within the computer room. A separate secure room, or area, within the data center should be provided for non-IT servers. It is recommended that these non-IT servers be supported by a dedicated facility UPS, separate from the UPS that supports the computer room, which meets the Class redundancy of the data center.

The IT network team should be engaged early in the facility design process so that each of these non-computer room networks are clearly understood by the IT network administrators enabling them to plan a suitable firewall design to isolate and protect each of the networks.

15.7.4 Additional Information

Figure 15-9 shows an example of a facility & IT network topology with these types of systems.

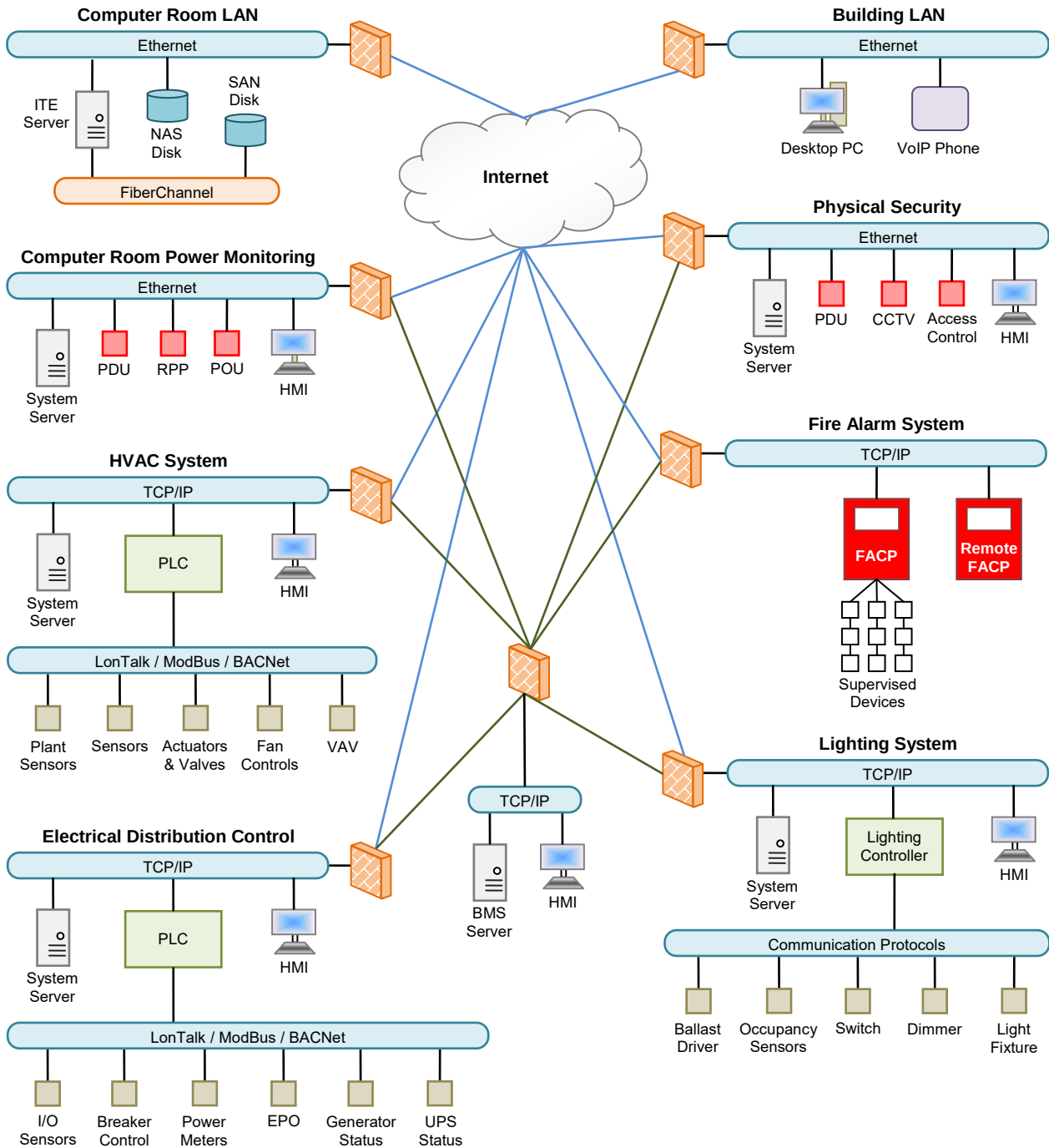


Figure 15-9
Example of Facility & IT Network Topology

This page intentionally left blank

16 Commissioning

16.1 General

16.1.1 Introduction

Commissioning is the process of ensuring systems are designed, installed, functionally tested, and capable of being operated and maintained according to the owner's design intent and operational needs. Commissioning also provides testing of failure modes and operational procedures that cannot be performed once the data center is in production.

Historically, commissioning has been associated with the HVAC systems. Today, commissioning has become an important quality control process that encompasses the entire building or data center.

Because of its unique facilities requirements and systems, a data center should be commissioned according to industry guidelines and requirements.

16.1.2 Recommendations

The following systems should be considered for inclusion in the commissioning plan for a data center:

- Electrical systems
- HVAC systems
- Control systems (e.g., BAS)
- Monitoring systems (e.g., BMS)
- Fire protection and suppression systems
- Security systems
- IT infrastructure components and cabling, including LAN, SAN, WAN, management, and BAS/BMS networks
- Grounding systems
- Fuel oil pumping systems
- Inventory monitoring systems
- Leak detection systems
- Systems required by codes or local ordinance to be commissioned
- Critical exhaust and ventilation
- Life safety system

16.2 Phases of the Commissioning Process

16.2.1 Overview

The commissioning process is not isolated to one discrete phase of a data center's construction. Rather, the commissioning process has elements in all of a data center constructions phases, including the:

- Program phase
- Design phase
- Construction phase
- Acceptance phase
- Post-Acceptance phase

Elements of commissioning for each phase are described in the following sections.

16.2.2 Program Phase

The program phase establishes the foundation for the other phases and determines the scope of work and systems to be commissioned. Objectives in the program phase include:

- Establishing the:
 - Design's intent
 - Project owner's requirements
 - Necessary funding and budgets
- Identifying the:
 - Team
 - Systems to be commissioned
 - Performance reliability requirements or BICSI 002 availability Class rating
 - Required approvals for all phases and receiving those required for the program phase
 - Requirements for training
- Developing the:
 - Commissioning plan
 - Commissioning issues log procedures

Decisions made in the program phase are crucial to the overall success of the commissioning of a data center.

16.2.3 Design Phase

During the design phase, the design of the data center components and systems is completed. Contract documents, specification documents, and system documents are completed. The commissioning agent should review all documents to ensure compliance with the design intent. Objectives in the design phase include:

- Architectural review of the room or building
- Review of the IT and facilities systems
- Execution of a needs assessment and inventorying of IT requirements
- Submission of design intent documentation
- Review of scope of work for all participants, including contractors and vendors
- Review of systems for maintainability in critical environments

16.2.4 Construction Phase

As the building or data center is constructed, the commissioning authority monitors the progress to ensure the design intent is being followed. Objectives in the construction phase include:

- Performance of milestone monitoring
- Completion of prefunctional testing as required
- Submission of field inspections and progress reports
- Monitoring of the change order process and approval authority
- Documentation and approval of any modification of the design intent

16.2.5 Acceptance Phase

During the acceptance phase, functional performance testing is performed on all the integrated systems. System calibration, manufacturers testing guidelines, and other requirements established during the design intent are completed and documented. Nonperforming systems are identified and corrected prior to startup. Objectives in the acceptance phase include:

- Base line performance documentation
- Functional performance testing
- Site audit
- Warranty audit
- Submission of the final documentation and all test reports

16.2.6 Post-Acceptance Phase

During the post-acceptance phase, operations and maintenance procedures are defined and monitored. As an extension of the acceptance phase, the documentation of new systems, changes in the facility, and a process for verification that the design intent is still being met should be clearly documented. Objectives in the post-acceptance phase include:

- Establishment of operations and maintenance (O&M) procedures
- Documents storage and modifications to documents defined
- Training the personnel
- Establishment of moves, adds, and changes (MAC) procedures
- Implementation of change control procedures and policies

16.3 Types of Commissioning

16.3.1 New Building

Four types of new building commissioning can be employed, depending on the project scope, client budgets and the design intent as well as existing building commissioning activities.

16.3.1.1 Continuous Commissioning

- Commissioning authority is engaged at the start of project.
- Performance information is gathered and reviewed throughout the life of the facilities.
- Ensures the design intent is maintained through project.

16.3.1.2 Milestone Commissioning

- Defines design milestones procedures.
- Performs testing, component validation, and verification of design intent at agreed upon intervals.

16.3.1.3 Acceptance Phase Commissioning

- Conducts required test on the integrated systems only.
- Reviews all test and maintenance criteria prior to turnover.
- Validates operational performance and correct deficiencies.

16.3.1.4 Network Operability Commissioning

- Performs validation of IT systems before turnover.
- Utilizes documented observed performance to establish baseline criteria.

16.3.2 Existing Building

16.3.2.1 Overview

There is considerable reported value in performing commissioning activities to existing buildings or systems. For existing buildings, this may take one of two forms:

- Retrocommissioning—the application of the commissioning process to a building that has not undergone commissioning and is initiated at some point after operations have already commenced.
- Recommissioning—the performance of the commissioning process to existing installations that had at least an initial commissioning performed, typically to reassess performance because of to modifications in operations, system changes or other concerns.

The goal of either commissioning form is to insure system operation and performance is in alignment with the operation's current use or needs.

16.3.2.2 Recommendations

A plan for recommissioning should be established as part of a new building's original commissioning process or during an existing building's retrocommissioning process.

16.4 Testing

16.4.1 Introduction

As a quality assurance process, commissioning requires testing at various intervals and in conjunction with the design intent of the project. Functional performance testing is the basis for the commissioning process. The main objective of functional performance tests is to ensure that all systems and equipment are operating efficiently and in accordance with the design intent.

16.4.2 Functional Testing Components

- Equipment description
- Purpose of the test
- Required personnel, tools, and instruments needed to perform the tests
- Design information pertinent to the equipment or system under test
- Detailed sequence of operation, including any operating set points
- Scheduling requirements
- Special instructions or warnings
- Description of expected results
- Sampling strategies

16.4.3 Functional Testing Procedures

- Inspection of equipment for manufacturing and installation defects
- Conditions of test
- Integrated systems test
- What was done to the system to cause a response
- Verification of response
- Comparison of actual response to acceptance criteria

16.4.4 Testing Equipment

16.4.4.1 Requirements

Equipment shall be calibrated according to the manufacturer's recommendations and whenever suspected of being damaged. Calibration certification shall be kept on record, and copies for each tester provided in turnover documents.

16.4.4.2 Recommendations

Test equipment should be of an accuracy required to test system performance within the tolerances specified by the construction and manufacturer's documents. Generally, the accuracy of any sensor should be at least twice that of the device being tested.

16.4.5 System Testing

16.4.5.1 Preinstallation Testing

Some subsystems may have components that have been pretested prior to installation. Some components (e.g., video cameras) should have quick functional test performed prior to installation.

Preinstallation tests may:

- Reveal components that have been damaged in shipment and need to be replaced
- Provide the option to calibrate or adjust systems in the shop

16.4.5.2 Preliminary Testing and Calibration

Systems and subsystems should be thoroughly tested and all adjustments and calibrations completed prior to the start of final acceptance testing. This includes the testing of each individual device or component for proper operation and system response.

For example, preliminary testing and calibration of a data center's ESS systems may include testing:

- Each access control device for door prop alarms, forced door alarms, and valid and invalid card reads
- Each alarm point for intrusion detection and video camera call-up and recording
- Video cameras for resolution, light sensitivity, focus, and where applicable, PTZ control
- The functionality and response of the systems' graphical user interface (GUI) system
- Intercom and notification systems for proper operation, sound quality, and intelligibility

16.4.5.3 Burn-in Period

Prior to scheduling the final acceptance test, the commissioning technician should power up and operate each of the systems during a burn-in period. During this burn-in period, each system should be powered and operated for an entire day. A burn-in period could be 2-14 consecutive days or based on client requirements.

Any faults, errors, and noncompliance issues should be corrected prior to beginning the final acceptance testing. Any components or systems that are replaced should also be subject to a burn-in period.

16.4.6 Acceptance Testing

16.4.6.1 Overview

Acceptance testing should be performed after the completion of a successful and complete system burn-in period. As with preliminary testing, acceptance testing should include testing individual devices for proper operation and proper system responses. Acceptance testing is to be complete and test documentation approved by the client prior to the project completion.

16.4.6.2 Plan

Clear acceptance testing guidelines should be provided in the construction specification documents. Those guidelines provided shall define the performance requirements for the system as the acceptance testing plan will be used by the client during the final acceptance test as part of the turnover documentation. The plan should include checklists and procedures with specific areas for recording and documenting all tests and inspections and a summary statement and signature block at the end of the plan.

16.4.6.3 Documentation

16.4.6.3.1 Requirements

Testing documentation shall include full details of all commissioning tests as well as factory testing reports provided by the manufacturer with the equipment.

16.4.6.3.2 Recommendations

The test plan forms and checklists should list any deficiencies and fully document the test results of each acceptance test performed. The client should also document all observed tests and create a punch list of deficiencies that need to be corrected and retested.

16.4.6.4 Retesting Equipment and Systems

16.4.6.4.1 Requirements

The commissioning technician shall correct any deficiencies identified by the client. Upon completion of all corrections, the equipment shall be retested to demonstrate proper operation, integration, and performance.

16.4.6.4.2 Recommendations

Verification of proper system operation and performance should be completed during the preliminary testing stage to avoid retesting. The construction documents should identify who is responsible for labor, materials, and other required support for the supervision and observation of any retesting of failed components or systems.

16.4.7 Electrical System Testing Example

NOTE: See Appendix F for specific examples of PDU, UPS, and generator testing.

For electrical systems, testing typically occurs during the construction and acceptance phases. The following is a typical sequence of testing, though each phase may have a time interval between the completion of one phase prior to the start of the next.

- Level 1—Equipment subject to in-factory testing and certification prior to delivery to the project location.
- Level 2—Equipment installation has been completed and start-up activities are satisfactorily completed by the factory technicians.
- Level 3—Component-level testing.

Individual electrical system components, like a single generator or UPS power modules are tested. This commissioning step would precede the assembled parallel or complete electrical system testing.

- Level 4

- Electrical System Functional Testing

This system-level testing where paralleled or cooperating systems like multiple generators or UPS power modules are tested together as a single unit. This commissioning step would be for electrical systems under a single control system or activity and would precede the complete electrical system testing.

- Electrical System Operational Testing

The completed electrical system is tested as a complete and interconnected utility. Unlike electrical system functional testing, this phase of testing examines the entire electrical system to verify the interaction of the various electrical subsystems and to ensure that the electrical system works as a single, coordinated entity. This commissioning step would precede the complete building system testing in Level 5.

Level 4 should include training and participation of all personnel who will be responsible for any activities during any change of state in the facility power and mechanical systems.

- Level 5—Whole Building Testing.

Subsequent to the successful functional and operational testing of both the individual or complete electrical and mechanical systems, the entire building's utility infrastructure is examined as a complete system. The goal of this is to validate that the all building utility systems are operating as intended and to verify the proper and expected interactions of those systems (e.g., how the mechanical system responds to a change of state in the electrical system) and to ensure that they work as a single, coordinated entity.

The building is subjected to the design maximum loads for electrical supply and mechanical cooling/heating. Like previous steps, normal, failure, and maintenance modes of operations are demonstrated. Load response and profiles are typically developed during this phase of the work.

16.5 Commissioning Documents

16.5.1 Introduction

Documentation is one of the primary differentiating aspects for implementing a commissioning process. Thorough documentation prevents random quality control and assurance that often leads to system inefficiencies. Documentation also provides uniform testing protocols for on-going testing procedures and performance analysis.

16.5.2 Design Documents

Design documents shall include the following, as applicable:

- Design intent
- Basis of design
- Building drawings
- General equipment specifications
- System submittals
- Architectural requirements
- Project owner's requirements
- Change orders
- Sequence of operation

16.5.3 Process Documents

Process documents shall include the following, as applicable:

- Commissioning plan
- Reporting forms
- Schedules and timelines
- Meeting minutes and progress reporting
- Conflict and resolution records
- Startup and testing plans and schedule
- Training program

16.5.4 Verification Documents

Verification documents shall include the following, as applicable:

- Construction observation reports
- Commissioning issues log
- Test reports from:
 - Manufacturers
 - Contractor
 - Commissioning agent
- Final commissioning report

16.5.5 Operation and Maintenance Documents

Operation and maintenance documents shall include the following, as applicable:

- Warranties
- Equipment operation and maintenance (O&M) manuals
- As-builts
- Control drawings

16.5.5.1 Equipment O&M Manuals

16.5.5.1.1 Requirements

O&M manuals shall include:

- Detailed installation, operating, troubleshooting, and maintenance procedures
- Certifications provided by the manufacturer that indicate compliance with any regulatory requirements, codes, or standards

16.5.5.1.2 Recommendations

O&M manuals should contain:

- Site-specific instructions for routine and emergency operations and maintenance
- Complete warranty information, including the client's responsibilities for maintaining the warranty

16.6 System Training for Client Staff

16.6.1 Recommendations

At least two separate instruction sessions should be provided for training the client's operating staff.

The first session is conducted during acceptance testing to provide the initial training needed to operate and maintain the system. The first training session should include:

- General familiarization and operating instructions for each specialty system
- Routine maintenance procedures
- User level programming of software and systems

Instruction on complicated systems and components should be provided by factory-trained technicians.

The second training session should be conducted after the final acceptance to fill in gaps and answer questions that develop once the staff has become familiar with the system.

Each training session should provide all the necessary training materials, including:

- An overview of the implementation and commissioning program
- A description of how the training is to be conducted
- The date, time, and location of the training
- The names and company affiliations of instructors
- A summary of the content
- Recommended reference material

The training sessions should be recorded and archived for repeat training and reference for additional staff. Requirements for system training, training materials, and recordings should be included within the construction documents.

16.7 Final Commissioning Report

The following is an outline of the information that should be included in the final commissioning report:

- Project name
- Name, address, firm, and telephone number of commissioning authority
- Description of the building:
 - Size
 - Location
 - Use
 - Construction
- HVAC and other installed systems
- List and description of commissioning tasks
- Commissioning plan
- Complete documents
- Completed design intent document
- Completed prefunctional test checklists
- Completed functional performance testing reports
- Any outstanding seasonal testing needs
- All noncompliance forms
- Summary of commissioning findings
- Recommendations for system recommissioning
- Recommendations for monitoring the ongoing performance of the system
- Recommendations for system improvements
- Recommendations for establishing trending settings and monitoring activities for ongoing system performance management

17 Data Center Maintenance

17.1 Introduction

Insufficient maintenance and maintenance spaces within the data center can result in extended downtime and potential damage to the supported systems. Given that the availability of a system or data center itself is expected to be at least 99% systems maintenance or lack thereof can either positively or negatively affect the achievement of the target availability.

Reducing scheduled downtime is not the same as eliminating time required for maintenance as all systems of a data center will require maintenance to reduce the risk of premature replacement. Therefore, maintenance requirements should be utilized within the design, planning, and operational stages of the data center.

The terms *predictive maintenance* and *just-in-time maintenance* come from a philosophy that is gaining popularity. It suggests that because human intervention is as often causative as it is preventive, anything that can be done to minimize human error increases availability.

This section provides general guidelines for all types of maintenance considerations within a data center. Sources of information for maintaining data center systems will vary from codes and standards applicable to telecommunication and electrical systems to manufacturer requirements for specific equipment and specialized systems (e.g., CRAC, access flooring, lock hardware).

17.2 System Maintenance General Requirements and Recommendations

17.2.1 Requirements

Manufacturer's specifications and the applicable AHJ requirements for the system shall be followed for applicable maintenance, at a minimum.

17.2.2 Recommendations

All maintenance activities should be carefully planned and performed by personnel familiar with the entire system to be maintained as well as with all of its interdependencies. As part of the operational maintenance strategy, a plan should be drafted determining the order and sequence of all annual maintenance and testing procedures.

All electrical and mechanical equipment should be initially tested after installation and then periodically throughout the life of the equipment. Testing should be performed on the equipment individually and as an integrated system to ensure compatibility and proper interaction between equipment in accordance with the design intent. Frequency of testing shall conform to manufacturer's recommendation as a minimum. Equipment or devices susceptible to significant wear resulting from testing, such as (but not limited to) batteries, should not be subjected to more testing than is recommended by the manufacturer. Testing of equipment or devices performed at high risk should be limited to the recommendation of the manufacturer.

Backup system testing should be scheduled during off hours, even if the electrical systems are designed to keep all critical loads running when one or more electrical service feeds are shut down as the testing may uncover a defect that causes a system outage.

For data centers designed with redundant components or systems (Class 2 or higher), it is especially important not to plan work on primary and secondary components of the same system or mirrored components simultaneously.

To minimize the need for unscheduled maintenance, all components of a system should be designed for high reliability. Where possible, components should provide a minimal requirement of downtime for service, whether it is preventive or remedial.

System maintenance should include periodic testing of the systems to ensure that they are operating properly.

17.3 Maintenance Plans

17.3.1 Recommendations

The following should be addressed in the creation of a system maintenance plan:

- Identify the maintenance requirements of each system, and ensure that they are conducted as required
- Develop a detailed checklist that tracks maintenance activities as they occur as well as the results of these ongoing checks
- Develop a preventative maintenance program for sensitive systems, devices, or certain restricted areas that may contain sensitive or valuable assets
- Develop effective maintenance contracts that serve both the security contractor and the client
- Develop an ROI that outlines how a nonperforming system may impact the viability of the organization as well as an ROI that details cost savings that occur when the system is able to operate at optimal efficiency
- Utilize intelligence data to justify maintenance and sustainment efforts to management, demonstrating any correlation that might exist that links the available statistics and intelligence data
- Perform a risk analysis that focuses on the organization's potential exposure and how best to mitigate these exposures with the existing systems

Additional items that may be addressed in a maintenance plan are:

- Personnel availability and skill set requirements
- Product training, including hands-on familiarization with new products
- Codes, standards, and safety training to maintain skill levels to minimize substandard or unsafe work habits
- Current documentation with detailed records of circuits, optical fibers, and cables
- Cable records maintained for staff to identify potential issues that affect service
- Up-to-date pathway segment records
- Installed equipment baseline—This includes the current version of installed equipment, documented option settings, port configurations, and other information needed for the repair or restoration of individual circuits
- Storage and availability of repair materials—This includes the procedures and process necessary for replenishing materials as they are used. Some quantity of materials must be available to the restoration teams on a 24/7 basis. The maintenance plan must address how this material is to be obtained by the restoration team outside the normal working hours of the support center.
- Initial and sustaining training—The maintenance plan must establish guidelines for training of the initial skill sets necessary for normal operations as well as provide a method for ensuring continued development of the workforce needed. Backup personnel must be available for long-term support and operations.
- Restoration procedures—The maintenance plan must establish policies and practices for the routine maintenance and support of the system and demand maintenance response to requirements driven by public demand or natural events. In the event of unplanned system outages along with the policies and practices for routine and demand maintenance, special procedures and policies must be established for emergency or quick system recovery.
- Maintenance schedule for all equipment, including periodic testing and calibration.
- Management escalation procedures with contact information for emergency call out of the workforce.

17.4 Cabling Systems Maintenance

17.4.1 Introduction

Cabling systems, once installed, will normally require very little maintenance, provided the structured cabling system is designed and installed to comply with appropriate codes and standards of the data center location. Properly built cabling systems do not generally break under normal usage without some external force causing breakage. Cable pathways and spaces are designed and built in compliance with applicable standards and follow the recommended cable fill ratios. There should be sufficient space for moves, adds, and changes that will normally occur as changes and reconfigurations take place in the data center. This is particularly important in a new data center where growth is expected. Cable access is the single most important factor for maintenance of structured cabling systems in the data center.

Cabling systems should be inspected periodically for cable degradation, cracks, abrasions, heat, deformation, brittleness, movement, corrosion, or other indications of abuse and age.

17.4.2 Recommendations

Only qualified personnel should be performing moves, adds, and changes.

Personnel performing changes should be trained in the data center standards and policies for:

- Cabinet, rack, equipment, cable, patch cable, power strip, and power receptacle labeling
- Cable and patch cord color scheme (if used)
- Routing and dressing of cables and patch cords
- Proper equipment installation (air intakes in the front, exhaust out back, preferably not on rail, labeling, routing of cables)
- Connecting equipment to the proper power strips and receptacles to provide the desired redundancy

During the annual inspection or when moves, adds, and changes performed by cabling technicians occur:

- Inspect/repair/replace worn, cut, pinched cabling entering cabinets and at stress points in the cable management systems
- Inspect/repair secure mounting of all cable management systems
- Inspect/repair cable congestion points within telecommunications switches and or servers
- Inspect/repair floor, wall, and ceiling cable penetrations for correct fire stop and or cable damage
- Inspect/repair any loose cable that could be snagged, cut, or tripped over
- Remove any/all unused/abandoned cable whenever possible. (especially important at cross connections)
- Ensure any unused terminated optical fiber is capped to prevent dust contamination or scratches on fiber ends
- Ensure that cabinets, racks, and raceways are properly grounded and that bonding conductors are secure. Grounding connections should be inspected regularly (annually at minimum) to ensure that they have not been damaged, corroded, or come loose.
- Ensure that all cabinets, racks, patch panels, cables, and patch cables are properly labeled

17.5 Electrical Systems Maintenance

17.5.1 Introduction

Many electrical systems are required to support a working data center. Some of these systems will require more maintenance than others. Generators, batteries, and UPS systems will require periodic maintenance at manufacturer-specified or industry standard intervals.

Standards such as NFPA 70B illustrate the importance of Effective Electrical Preventive Maintenance (EPM), and its economic benefits as well as increased availability.

Technicians must also follow applicable safety codes, standards, and applicable local and federal guidelines.

NOTE: Appendix H contains a listing of many commonly encountered standards from NFPA, IEEE, and other standards organization for electrical system maintenance.

17.5.2 Requirements

The most important factor regarding electrical systems maintenance is safety. Consequently, all electrical work shall be performed by fully qualified, licensed/bonded/insured electricians/technicians who have been trained (and certified when such certification is available) on the specific type of equipment. All electrical work shall be accomplished in accordance with all applicable codes and regulations as mandated by the AHJ. Certain maintenance functions, such as replacement of hot swappable elements, shall be permitted to be performed by trained operators when the equipment has been so designed and procedures have been specified.

Perform inspections as required by the AHJ, and may include:

- UPS and power generation systems periodic maintenance inspections performed in accordance with manufacturer's specifications and the AHJ
NOTE: NFPA 70B recommends routine maintenance on a semiannual basis for UPS systems. It also suggests what should be inspected, measured, and possibly tested.
- Emergency lighting operational check as required by AHJ
- BAS and fire alarm systems operational check as required by AHJ

Ensure complete compliance with all mandated safety regulations of the applicable AHJ.

17.5.3 General Recommendations

Safe performance of electrical maintenance and testing should conform to the manufacturers' procedures. Additionally, perform inspections as specified by the equipment manufacturers.

Inspections and recommendations that are in addition to those that may be required by the AHJ include:

- All power connections secure
- IR thermography scanning is recommended once per year to identify loose or poor connections and unbalanced electrical loads, all characterized by increased resistance or temperature rise
- All receptacles and power strips properly labeled
- All safety features in place and operational
- Doors and cover plates on panelboards and power distribution units in place and operating properly
- Consider battery monitoring in UPS systems
- Lighting systems checked and bulbs replaced as required
- Check fuel quality for generators annually

17.5.4 Battery Recommendations

Inspections should be performed on batteries as recommended by IEEE standards. The following is a summary of recommendations for common battery types.

17.5.4.1 VRLA Battery Recommendations

IEEE 1188 provides details for maintenance, testing, and replacement of stationary valve-regulated lead-acid (VRLA) batteries, including:

- Monthly:
 - Visually inspect for evidence of corrosion, container distortion, and dirt
 - Check overall battery float voltages at regular intervals (at least monthly if performed manually; continuous monitoring is recommended)
- Quarterly:
 - Measure and record cell/unit internal ohmic value, temperature, and voltage
- Annually:
 - Measure and record cell-to-cell and terminal connection resistance and measure AC ripple current
 - Compare measurements to base line data, monitor trends, and identify units that fall outside of predicted range (per manufacturer's recommendation)
 - Replace battery units or strings as necessary
 - If UPS is designed with continuously monitored modular battery cartridges, replace when notified by alarm

17.5.4.2 Vented (Flooded) Lead Acid Battery Recommendations

IEEE 450 details the recommended maintenance, testing, and replacement practices for vented, stationary, and lead acid batteries:

- Monthly
 - Visually inspect for evidence of corrosion, container distortion or damage, and dirt
 - Check overall battery float voltages and charger float current
 - Inspect electrolyte levels; add water as required
 - Check pilot cell voltage and electrolyte temperature
 - Check for unintentional grounds
- Quarterly:
 - Measure and record cell/unit voltage
 - Measure and record specific gravity and temperature of 10% of cells
- Annually:
 - Measure and record cell-to-cell and terminal connection resistance
 - Measure and record specific gravity and temperature of each cell
 - Inspect structural integrity of battery cabinet or rack
 - Compare measurements to base line data, monitor trends, and identify units that fall outside of predicted range (per manufacturer's recommendation)
 - Replace battery units or strings as necessary

17.5.4.3 Vented Nickel-Cadmium (Ni-Cd) Battery Recommendations

IEEE 1106 provides details for maintenance, testing, and replacement of stationary vented Ni-Cd batteries, including:

- Monthly:
 - Visually inspect for evidence of corrosion, container distortion, dirt
 - Check overall battery float voltages at regular intervals
 - Measure charger output current and voltage
 - Visually inspect electrolyte levels; replenish as required
- Quarterly:
 - Measure and record pilot-cell electrolyte temperature
- Semiannually:
 - Measure and record voltage of each cell
- Annually:
 - Measure intercell connection torque
 - Measure and record cell-to-cell and terminal connection resistance
 - Inspect structural integrity of battery cabinet or rack

NOTE: See IEEE 1184 for more information.

17.5.5 Additional Information

The following is an example of one manufacturer's specified service intervals for electrical systems and components:

- 3-phase UPS—2 preventive maintenances (PMs) per year
- VRLA batteries associated with 3-phase UPS—4 PMs per year
- Wet cell batteries associated with 3-phase UPS—12 PMs per year
- 1-phase UPS—1 PM per year
- VRLA batteries associated with 1-phase UPS—1 PM per year
- Power distribution units (PDU) —1 PM per year
- Static transfer switches—2 PMs year
- DC power plants—2 PMs per year
- VRLA batteries associated with DC power pants—4 PMs per year
- Wet cell batteries associated with DC power plants—4 PMs per year
- Remote monitoring systems—1 PM per year
- Surge suppression devices—inspect condition of item—no PM
- IR thermography scanning—1 per year

17.5.5.1 Generator Testing

Regular testing is required to maintain the generator per manufacturers' instructions and code requirements.

Testing under a load bank will prevent the potential of jeopardizing the critical load. However, local code may require testing under live load. Class F1 and F2 generator systems should have an extra breaker with lugs for connection of a portable load bank. Class F3 and F4 should have a permanent load bank for regular testing.

NOTE: Standards such as NFPA 110 contain further recommendations for maintenance and testing of generators.

17.6 HVAC Systems Maintenance

17.6.1 Introduction

HVAC systems in data centers are a critical component in the operation of the center. All IT and telecommunications system operating within the data center have temperature and relative humidity operating ranges that must be maintained to prevent overheating and damage to critical system components.

Numerous commercially available environmental monitoring tools run on LANs and provide computer room environment reporting to the operations center. Operations personnel can then take preventative measures if computer room conditions begin to approach threshold levels.

It is very important that HVAC systems operate at optimal performance. To do so, these systems must be maintained according to manufacturer's specifications.

Data center HVAC systems should always be maintained by qualified HVAC technicians that are available for service twenty-four hours a day, seven days a week.

17.6.2 Recommendations

Recommended preventive maintenance for computer room air conditioning (CRAC) systems includes:

- Monthly:
 - Environment:
 - o Verify that each module is maintaining temperature and humidity set points
 - o Record room temperature and humidity near the return vent of each module
 - o Inspect for visible damage to module (dents, scratches)
 - o Inspect for environmental damage (dirt, dust, debris, liquid stains) around the module installation area
 - o Inspect belts (if applicable) for wear and tightness
 - o Record past month's alarm history—cause and response
 - Cleanliness:
 - o Check condition of return air filters; replace if necessary
 - o Check condition of drain pan and remove any accumulation of debris

<List continues on next page>

- Mechanical:
 - o Ensure that all components of the blower and its motor are moving freely with no signs of binding or damage
 - o Inspect the set-screws on fan blades and bushings to make sure that they are tight
 - o Verify that condensate line is flowing freely
 - o Verify that the humidification system does not have leaks at the fill and drain valves and that these modes of operation are functional
 - o Ensure that there are no kinks in the steam delivery system (where applicable) from the cylinder top to the steam distributor
 - o Check for build-up in cleanable cylinders (where applicable) and clean as required
 - o Replace disposable humidifier cylinders if necessary (where applicable)
 - o Verify chilled water supply temperature (where applicable)
- Electrical:
 - o Confirm that the incoming main power is within tolerance listed on the module's nameplate
 - o Verify that the control voltage is within manufacturer's recommended tolerance
- Quarterly:
 - Mechanical:
 - o Check water lines for leaks
 - o Verify tightness of blower and its motor hardware
 - Electrical:
 - o Conduct an infrared (IR) scan of electrical panels and connection points. If hot spots are identified, schedule shutdown, deenergize the equipment, and tighten any loose connections
 - o Record amperages for critical components (such as cooling coil fan motors, reheater, and humidifier)
- Semiannually:
 - Cleanliness:
 - o Check cleanliness of chilled water coil
 - Electrical:
 - o Verify that contactors and relays are operating correctly
 - o Check the main power wiring for critical components such as reheat elements, evaporator motors, and humidifiers
 - Functional tests:
 - o Verify operation of the coil fluid (water regulating) valves and record pressure
 - o Check the operation of all system alarms

17.7 IT and Telecommunications Systems Maintenance

17.7.1 Introduction

17.7.1.1 IT Systems

IT systems for data centers come in many configurations from small servers that fit in a single rack unit or blade server chassis module to very large multiple processor systems that consume several cabinets and can require a footprint of 1.7 m² (18 ft²) or more. The one thing all servers and associated peripherals have in common is that they all will require maintenance at some time.

All IT systems manufacturers should provide the necessary maintenance documentation or web-based technical support for their particular systems. Most will offer maintenance programs ranging from defective component mail-in replacement to on-site maintenance technicians.

The key to maintaining IT and telecommunication systems is to provide sufficient space for qualified technicians to perform the required maintenance actions.

Telecommunications systems have advanced as rapidly as today's new generation of servers and are just as sophisticated. Systems can be ordered with redundant "hot swappable" components that make it possible to run virtually forever without taking a system offline for hardware maintenance.

Maintenance spaces are very important for telecommunications systems because of cable congestion that often happens with large configurations installed in cabinets or racks.

17.7.1.2 Telecommunication Systems

Like IT systems, telecommunications system manufacturers should provide the necessary maintenance documentation and web based technical support for their particular systems. Most will offer maintenance programs ranging from defective component mail-in replacement to on-site maintenance technicians. The key to telecommunications systems maintenance is to provide sufficient space for qualified technicians to perform the required maintenance actions.

Maintenance on a small switch usually consists of whole unit removal and replacement when failure is detected. In contrast, a large enterprise class switch will consist of a chassis with multiple “blades” and redundant power supplies. Maintenance on a large switch like this requires removal and replacement of the individual defective “blade” or power supply.

Some devices require front access for maintenance and others will require rear access for maintenance. It is wise to plan for both front and rear maintenance access. Some specialty peripheral equipment, such as robotic tape storage systems, can require front, rear and side maintenance access because of the complexity and size of the internal subsystems and components.

All equipment and systems proposed for installation in the data center will have manufacturer-recommended installation specifications that must be reviewed in advance by planners, configuration managers and facilities managers to help determine the maintenance space required for each respective system installed in the data center.

Planning for and allocating adequate maintenance space ensures expedient and safe maintenance activities on installed IT and telecommunications systems.

Ethernet switches, commonly used to provide network connectivity to servers within the data center, range in size from one rack space unit for a small office Ethernet distribution switch with eight to forty eight connectivity ports (see Figure 17-1) to large enterprise class distribution switches that will take up half (or more) of a standard 42U cabinet or rack and can contain four hundred or more connectivity ports (see Figure 17-2).



Figure 17-1
One Rack Unit (1 RU) 48 Port Ethernet Switch



Figure 17-2
Twenty Rack Unit (20 RU) Network Switch
Chassis with Installed Switches

17.7.2 Recommendations

17.7.2.1 General

Some IT systems must be maintained by factory-authorized service technicians because of their proprietary nature or complexity, and some IT systems can be maintained by competent onsite personnel. Most checks, such as those listed below, would be performed during periodic maintenance inspections occurring monthly, quarterly, or annually:

- Cleaning of cooling fans in all equipment
- Check/replace inoperative or noisy cooling fans in all equipment
- Cleaning or replacement of air filters where applicable
- Checking for failing/failed power supplies in equipment fitted with redundant power supplies
- Checking exposed cabling (power or data) for possible damage
- Confirming all computer and telecommunications equipment is properly labeled

Whether maintenance activities are performed by factory-authorized technicians or trained competent on-site personnel, it is critical to adhere to the manufacturer's recommended maintenance plan for proper operation of IT and telecommunications systems.

17.7.2.2 Cabinets

With high port density switches, such as those shown in Figure 17-1 and Figure 17-2, the use of careful and neat cable management is recommended in order to avoid patch cable congestion that will make maintenance (component removal or changes) difficult to perform without affecting connected users, particularly when the switch is installed in an enclosed cabinet.

Manufacturer specifications for maintenance space should always be followed as a minimum requirement. When manufacturer specifications are not available, one meter maintenance access space in front and rear is sufficient in most cases.

Cabinets can be configured with left side hinges in front and right side hinges in the rear or vice versa or doors that are split in the middle and, therefore, hinged on both sides in front and rear. Some manufacturers offer cabinets with removable side skins that allow like cabinets to be fastened together. Not all cabinets will be offered with an anti tip rail in the bottom, but this is an important safety feature to look for in tall cabinets with a full complement of slide-out servers if the cabinet is not secured to the floor; however, it is recommended that such cabinets be secured to the floor.

Liquid-cooled cabinets will require special procedures for access and maintenance because of high heat loads being generated in these cabinets. Any door open time will need careful planning to reduce the impact of cooling loss on the equipment contained in them.

Removing front and rear cabinet doors is not recommended for:

- Cabinets that rely on ventilation fans installed in the doors
- Cabinets that require the presence of these doors for proper air circulation
- Data centers that rely on lockable/locked cabinet doors to prevent untrained/unauthorized personnel from accessing cabinet contents
- Data centers that require a high aesthetic (e.g., client tours, data center "showcase")

NOTE: It is common in high-density server cabinets to have multiple network connections required per server. Therefore, careful and neat power and network cable routing and management is critical in these cabinets to prevent cable damage when servers are extended for maintenance service as well as observing power and data cable separation requirements.

17.8 Access Floor System Maintenance

17.8.1 Introduction

As IT, telecommunications, structured cable, and power distribution systems are installed in and moved around the data center, wear and tear of the access floor system will occur. Over time, dust and debris will accumulate in the sub floor, presenting the potential for dirt infiltration into systems receiving conditioned air from under the access floor. Consequently maintenance inspections/actions and cleaning will be necessary to maintain the integrity/cleanliness of the floor system. The failure or collapse of an access floor system will result in extended down time. An unstable floor system is dangerous and can lead to serious injuries or equipment damage. Failure to maintain the access floor system may result in violation of AHJ codes or standards.

17.8.2 Recommendations

There are two categories of maintenance concerns for access floor systems: Structural and Environmental.

17.8.2.1 Access Floor Structural Maintenance

17.8.2.1.1 Lateral Instability

Lateral instability occurs when the floor system becomes loose and unstable. There are gaps between panels. Panels shift laterally when weight is applied.

Causes are:

- Missing edge trim
- Lateral braces loose or untied
- User abuse
- Incorrect cutouts
- Leaving panels out
- Poor installation
- Drastic temperature changes
- Multiphase installations

Consequences are:

- Structural damage to other floor components
- Equipment subject to shifting
- Personnel hazard
- Allows debris to drop on stringers causing vertical instability
- Reduction in plenum pressure from air conditioning
- Allows water/chemicals used in cleaning to corrode understructure
- Safety hazard

17.8.2.1.2 Vertical Instability

Vertical instability occurs when floor panels do not rest securely on the pedestal head or grid system. This allows the floor panels to rock and panels to move up and down when weight is applied.

Causes are:

- Missing gaskets
- Missing stringers
- Missing pedestal pads
- Dirt/debris on pedestal/grid caused by lateral instability
- Subfloor dirt/particulates forced on grid by air conditioning
- Removing stringers, not replacing properly
- Removing panels, not replacing properly
- Swollen wood core panels
- Warped panels
- Moving equipment on floor too soon after installation
- Tipped pedestal

Consequences are:

- Reduction in plenum pressure from air conditioning
- Tripping hazard for personnel
- Edge trim is exposed, subject to breaking (if edge trim is broken, laminate surface is exposed to chipping)
- Dirt/debris drops into subfloor
- Permanent panel damage

17.8.2.1.3 Missing Edge Trim

Missing edge means that edge trim has been removed, misplaced, or broken from panel edge.

Causes are:

- Neglectfully not reinstalling after underfloor access
- User abuse
- Vertical instability
- Lateral instability

Consequences are:

- Chipping of high-pressure laminate
- Panel surface detachment
- Safety hazard (tripping)
- Lateral instability
- Reduction of plenum pressure
- Collection of dirt/dust on grid and subfloor
- Allows cleaning chemicals to reach steel components
- Rapid aging of floor system

17.8.2.1.4 Overloaded Panels

Overloaded panels subject to weights exceeding load rating of floor system.

Causes are:

- Heavy permanent loads (equipment, racks)
- Heavy loads repetitively rolled over the floor panels

Consequences are:

- Floor system failure
- Permanent panel damage
- Rapid aging of floor system

17.8.2.1.5 Perimeter Tipping

Perimeter tipping occurs when the outside edge of floor is not level or in accordance with access floor specification.

Causes are:

- Improper interface between perimeter panel and pedestal head
- Stringers not cut and bolted to the perimeter pedestal head
- Improper reinstallation (after removal for underfloor access)
- Missing understructure

Consequences are:

- Safety hazard to personnel
- Lateral instability
- Dangerous to rolling equipment

17.8.2.1.6 Panel Surface Detachment

Panel surface detachment occurs when panel surface (e.g., laminate, vinyl) becomes loose or detached.

Causes are:

- Breakdown of glue from using improper cleaning chemicals
- Improper maintenance (flooding the floor)
- Missing edge trim (if vertical instability is present)
- Freezing (0 °C [32 °F])
- Rapid increase or decrease in temperature

Consequences are:

- Irreversible panel surface damage
- Tripping hazard
- Absence of surface leaves steel surface exposed to cleaning chemicals/water followed by rust

17.8.2.1.7 Deformed Panel Surface

Panel surface deformations are individual or multiple indentations in the panel surface.

Causes are:

- Dropping heavy objects on floor
- Rolling heavy loads with small caster wheels

Consequences are:

- Loss of static dissipative qualities of surface
- Rapid aging of floor system
- Unsightly appearance

17.8.2.1.8 Chipped Laminate

Laminate surrounding the outer edge of panel may become chipped or cracked.

Causes are:

- Missing edge trim that causes exposure with vertical instability
- Unsealed cutouts
- Scratching

Consequences are:

- Irreversible surface damages

17.8.2.1.9 Brittle Edge Trim

Edge trim surrounding the panel may become brittle and unstable.

Causes are:

- Repeated uses of acrylic/polymer chemicals (wax)

Consequences are:

- Breaking of edge trim leaves laminate surface open to chemicals that can detach surface covering
- Leaves laminate surface exposed to chipping
- Lateral instability
- Allows water/chemicals used in cleaning to corrode understructure
- Safety hazard from personnel tripping

17.8.2.1.10 Missing Components

Components may be removed or broken when panels are removed or replaced.

Causes are:

- Not installing components properly after underfloor access
- Improper reinstallation of components

Consequences are:

- Improper access floor performance
- Structural damage
- Safety hazard
- System failure

17.8.2.1.11 Improper Grounding

Floor system may fail to provide proper electrical ground.

Causes are:

- Grounding clips are removed or not reinstalled properly

Consequences are:

- Loss of floor system conductivity
- Damage to equipment
- Injury to personnel

17.8.2.1.12 Plenum Leaking

Plenum pressure may be reduced when subfloor is used as an air plenum.

Causes are:

- Missing edge trim
- Lateral instability
- Vertical instability
- Improper sealing the cutouts
- Using stringers without gaskets
- Not using cove base at perimeter and column locations to seal floor

Consequences are:

- Reduction in static pressure
- Improper balance of air delivery around sensitive equipment

17.8.2.1.13 Uneven Wear

Panels may not wear evenly as a result of excessive foot or equipment traffic.

Causes are:

- High traffic in certain areas
- Improper maintenance
- Not rotating panels periodically
- Equipment caster
- Chair caster of facility personnel

Consequences are:

- Loss of static dissipative qualities of panels
- Uneven panel wear
- Life of panels reduced
- Rapid aging of floor system

17.8.2.1.14 Untrimmed Cutouts

Panel cutouts may be without the proper edge molding.

Causes are:

- Proper molding not installed when cutouts were made

Consequences are:

- Damage to cables
- Electrical hazard
- Employee injury
- Panel surface detachment (laminated surface exposed on sides to cleaning chemicals and water)

17.8.2.1.15 Warped Panels

A warped panel is a panel whose structural framework has been altered.

Causes are:

- Repeated heavy rolling loads with wide caster wheels
- Over wetting of wood core panels causing panels to swell

Consequences are:

- Panel failure
- Rapid aging of floor system
- Vertical instability
- Unsightly appearance

17.8.2.1.16 Miscellaneous Problems

Some of other problems are:

- Fascia needing repair
- Loose cutout trim (needing repair)
- Bent stair nosing (creating safety hazard)
- Ramp rubber torn (creating safety hazard)
- Cover base loose/falling off (safety hazard)
- Exposed grommet holes (tripping hazard)

Most of these problems can result in personal injury and structural damage to the floor system.

17.8.2.2 Access Floor Environmental Maintenance

17.8.2.2.1 Underfloor Conditions – Subfloor Debris

Causes are:

- Unsealed cutouts
- Lateral instability
- Debris left over from construction
- Interim construction
- Improper maintenance of subfloor
- Using the cutouts in the floor system as a trashcan

Consequences are:

- Vertical instability
- Structural damage possible to other components
- Particulates harmful to computer equipment
- Unhealthy environment for employees
- Fire hazard
- Debris littering subfloor can block equipment-cooling fans

17.8.2.2.2 Underfloor Conditions – Debris on Grid and Pedestal

Causes are:

- Lateral instability
- Air forcing dirt and debris on grid system
- Unsealed cutouts
- Missing edge trim
- Improper maintenance of subfloor
- Flooding of floor surface causes build-up of residual water and chemicals on stingers and pedestals

Consequences are:

- Vertical instability
- Structural damage to other components

17.8.2.2.3 Panel Surface – Improper Maintenance

Causes are:

- Uneducated maintenance personnel
- Improper cleaning chemicals
- Improper cleaning methods
- Flooding of the floor system
- Neglect

Consequences are:

- Permanent damage to floor system
- Structural damage to other components
- Unsightly appearance
- Loss of static dissipative qualities

17.8.2.2.4 Panel Surface – Residual Wax Buildup

When access floor panels have been cleaned regularly but they appear yellow, dingy, and dirty looking, more than likely, residual wax has built up on the surface. This is a common problem with floor systems. Residual wax rapidly ages a floor system and should be removed; however, commercial wax removers frequently cause access panels to delaminate (panel surface becomes detached) and create a larger problem.

Causes are:

- Cleaning crews using a mop in other areas of a building and using the same mop on the access floor
- Uneducated workers
- Wrong cleaning chemicals
- Improper cleaning methods

Consequences are:

- Affects static dissipating properties of surface
- Introduces unwanted contaminants into closed area
- Causes edge trim to become brittle
- Permanent damage to floor system
- Structural damage to other components
- Creates poor aesthetic quality of panel surface

17.8.2.2.5 Panel Surface – Scuffs

Scuffs are markings on the floor area caused by foot traffic and caster wheels.

Causes are:

- Heel marks
- Black casters
- Dragging equipment across panel surface

Consequences:

- Permanent damage to surface
- Unsightly appearance
- Rapid aging of floor system

17.8.2.2.6 Panel Surface – Ink Stains

Ink can cause staining of panel surfaces.

Causes are:

- Ink spill

Consequences are:

- Permanent staining of panel surface (especially if panel surface is scratched, ink will dye laminate)

17.8.2.2.7 Panel Surface – Scratching

Markings on the panel surface are caused by a variety of objects.

Causes are:

- Objects moved over floor surface
- Not protecting floor when moving equipment
- High traffic areas
- Sand

Consequences are:

- Permanent surface damage
- Poor aesthetic appearance
- Loss of static dissipative properties of surface
- Introduces contaminants into area

17.8.2.2.8 Subfloor Particulate – Cement Dust

Causes are:

- Unsealed concrete subfloor
- Construction debris remaining from initial project
- Interim construction

Consequences are:

- Abrasive to panel surface
- Damage to sensitive equipment
- Continual scratching will remove design on floor panel
- Loss of static dissipative properties of surface

17.8.2.2.9 Subfloor Particulate – Carbon

A specific type of dust usually found by the printers. It is electrically conductive and hazardous to sensitive electronic equipment. It is a flying sticky particulate that can create serious problems. All attempts should be made to eliminate excess carbon in a closed room.

Causes are:

- Toner spills
- Toner used for printers

Consequences are:

- Creates abrasive layer on floor surface
- Failure to computer related circuit boards
- Poor indoor air quality

17.8.2.2.10 Subfloor Particulate – Sand

Causes are:

- Brought into area by foot traffic
- Left from original construction

Consequences:

- Highly abrasive to high-pressure laminates
- Permanent surface damage
- Equipment damage
- Degrades static dissipative properties of surface

17.8.2.2.11 Subfloor Particulate – Rust

Causes are:

- Excessive moisture in area
- Deterioration of pedestals
- High humidity
- Leak underfloor
- Flooding of floor system during cleaning

Consequences:

- Component damage
- Component failure
- Unwanted rust flake particulate

17.8.2.2.12 Subfloor Particulate – Sheetrock Dust

Causes are:

- Subfloor and access floor not properly cleaned after construction or renovation
- Original construction debris not cleared from underfloor
- Interim construction (cutting holes in walls)

Consequences are:

- Damage to sensitive equipment
- Creation of high flying particulate

17.8.2.2.13 Additional Access Floor Maintenance Recommendations

- Develop and implement good daily and weekly housekeeping procedures
- Use care when handling floor panels to avoid damaging panels
- Know the floor loading capacities and do not exceed them
- Depending on activities on the access floor, implement monthly, quarterly, and annual floor inspections
- Depending on conditions (such as construction), implement quarterly or annual subfloor cleaning
- Refer to a guide such as *The Guide to Access Floor Maintenance* by Carol Blake for comprehensive access floor maintenance details.

17.9 Fire Protection and Suppression System Maintenance

17.9.1 Introduction

Fire protection and suppression systems are a necessary system in a data center and are usually required by local fire codes.

17.9.2 Recommendations

Standards such as NFPA 2001 and ISO 14520 outlines inspection, maintenance, testing, and training for fire suppression systems and should be adhered to as a guide for maintenance of fire suppression systems unless the local AHJ specifies otherwise.

All fire suppression systems should only be maintained by properly trained, certified, and authorized persons.

17.10 Security Systems Maintenance

17.10.1 Introduction

Security systems are often required by data center owners to control access into and protect assets within the data center.

Security systems can include but are not limited to:

- Magnetic strip card readers (for entry control)
- Motion detectors
- CCTV with recorders
- Retina scanners
- Fingerprint readers

Security systems can be very basic to extremely elaborate, depending on local site security policy.

17.10.2 Recommendations

Depending on the established security policy and the complexity of the security systems in use, maintenance of these systems should be performed by on-site security personnel or local security systems contractors.

Where fingerprint or other scanners are used to identify personnel, the maintenance regime should provide for regular cleaning of the contact surfaces and anti-bacterial hand cleaner or wipes to avoid cross contamination of personnel from surface borne pathogens.

Very little preventive maintenance is necessary with most modern systems and is often performed in conjunction with remedial maintenance. Maintenance actions should be performed only by persons certified and authorized to service the installed systems.

Maintenance activities can include but are not limited to:

- Camera adjustments
- Motion detector sensitivity and location adjustments
- Automatic door lock/closure adjustments
- Video recording system server updates
- Video tape rotation and storage

All maintenance is dependent upon the type of security systems in place and due to the variety of systems available and criticality of the security systems maintenance should only be performed by the appropriate system specialists.

17.11 Monitoring and Management Systems Maintenance

17.11.1 Overview

Monitoring and management systems are frequently used in data centers for monitoring and management of everything from environmental systems (HVAC) to power generation and distribution, security systems, IT and telecommunications systems.

Many newer systems will utilize SNMP software agents connected to the LAN to report systems status to a central server running a monitoring and management software application that collects all the details and provides a graphic display of monitored systems status to operations personnel in the central operations center.

Less sophisticated systems may have monitors, gauges, and dials that are directly connected to the device they are monitoring (e.g., HVAC systems).

Like security systems, monitoring and management systems could be relatively simple to extremely complex and can consist of numerous individual specialized devices.

17.11.2 Recommendations

For SNMP based systems, it may be necessary to:

- Periodically check for agent software updates from the manufacturer that enhance functionality of the monitoring system.
- Calibrate the device at manufacturer's specified intervals.
- Visually inspect the device at least annually.

For systems with direct connected monitoring devices, such as gauges, dials, and LCD status displays, periodic maintenance should include:

- Visual inspection of the device at least annually
- Calibration of the device at manufacturers specified intervals
- Repair/replacement of failing displays as required

The best practice is to follow the manufacturer/vendor/integrator maintenance recommendations for the system(s) installed.

Only allow maintenance activities to be performed by trained/authorized personnel.

17.12 Maintenance Recordkeeping

17.12.1 Recommendations

Although maintenance recordkeeping is not mandatory, it is a valuable tool to establish maintenance histories, baselines, and data trending.

Recordkeeping can be as simple as maintaining a paper maintenance log for each device/system under maintenance. However, a maintenance database is a much more efficient way of tracking maintenance information.

Some commercial industrial maintenance software products can be tailored for specific applications such as maintenance tracking or facilities management in the data center.

By using software to track maintenance actions, histories, baselines, and data trending can be established to determine the life cycle of components/systems under maintenance. Histories, baselines, and data trending can help to determine if a particular component(s) or systems are prone to premature failure. Histories, baselines, and data trending aid maintenance personnel in being proactive in maintaining failure prone systems and knowing which parts/components should be on hand and when they can anticipate needing them.

17.13 Service Contracts

17.13.1 Recommendations

A service contract should clearly define the terms and conditions between the organization and the contractor. Using written agreements that specify the scope of work (SoW) eliminates misunderstandings and miscommunications.

The service contract should include the:

- Work to be performed and the frequency of said performance (e.g., weekly, monthly, quarterly)
- Price of the contract for the standard service and cost for additional services that are not part of the standard contract (e.g., after-hours or weekend response)
- Terms on which the contract can be terminated by either party

Although different contractors may be servicing different components of the systems at the same facility, the following information should be included as an integral part of all service contracts:

- Facilities to be covered
- Normal working hours and days on which service work can be performed without impacting the organization's business
- Labor rate per hour and associated materials and parts required for normal serving of the systems to be serviced
- Type of response expected (e.g., callback, physical presence on-site) and time frame required once a service call is placed to the contractor's business
- Method of communicating with the contractor, including calls occurring outside the contractor's normal hours of operation
- Categories of system or device failure matched to an emergency condition
- Detailed list of all the systems and related devices to be serviced under the proposed contract

17.13.2 Example ESS Service Contract Provisions

For example, an ESS contract may include:

- Power supplies.
- Detection devices and their specific location within the facility (e.g., motion detectors, glass break detectors, pull stations, smoke detectors).
- Field and data-gathering panels.
- Servers, workstations, printers, network devices, and related peripheral devices.
- Surveillance cameras, listing types (fixed or pan, tilt, and zoom [PTZ]; Internet protocol [IP] or analog), housings, domes, recording devices, camera controllers, and display monitors.
- Uninterruptible power supply (UPS) and related power conditioning and surge protection devices.
- Electronic door locking devices, listing types (e.g., strike, magnetic lock, electrified mortise handset, shear lock).
- Communication devices (e.g., emergency telephones, two-way intercoms, one-way paging systems).
- Audible and other emergency display devices.

This page intentionally left blank

Appendix A Design Process (Informative)

This appendix is not part of the requirements of this standard, but it is included to provide additional information related to this standard.

A.1 Introduction

Communication and documentation are critical in the planning of space, power, and cooling requirements of data centers. Gaps commonly occur due to incomplete communication between disciplines. For example, “watts/m² or watts/ft²” specifications may not be adequate. More specific planning and communication of kW per cabinets of various types, along with the anticipated “end-state” deployment, may lead to higher level of success.

A.1.1 Traditional A/E Design Process

The architectural/engineering (A/E) design process for traditional commercial buildings involves space programming that identifies the various functional areas required. This task is typically performed by the architect or interior designer by interviewing the end users of each of the functional area and surveying the existing spaces occupied by the end user.

Once the “people” space and “people” flow have been identified, the architect or interior designer will work with the various engineering disciplines to determine the appropriate space for the supporting infrastructure (e.g., electrical and mechanical equipment spaces).

When all of the space programming has been completed, the process will then move into the design phases: planning, schematic design, design development, and construction documents.

All of these design efforts are often done without input from IT. However, doing so may result in inadequate telecommunications spaces and pathways to accommodate the desired telecommunications cabling system.

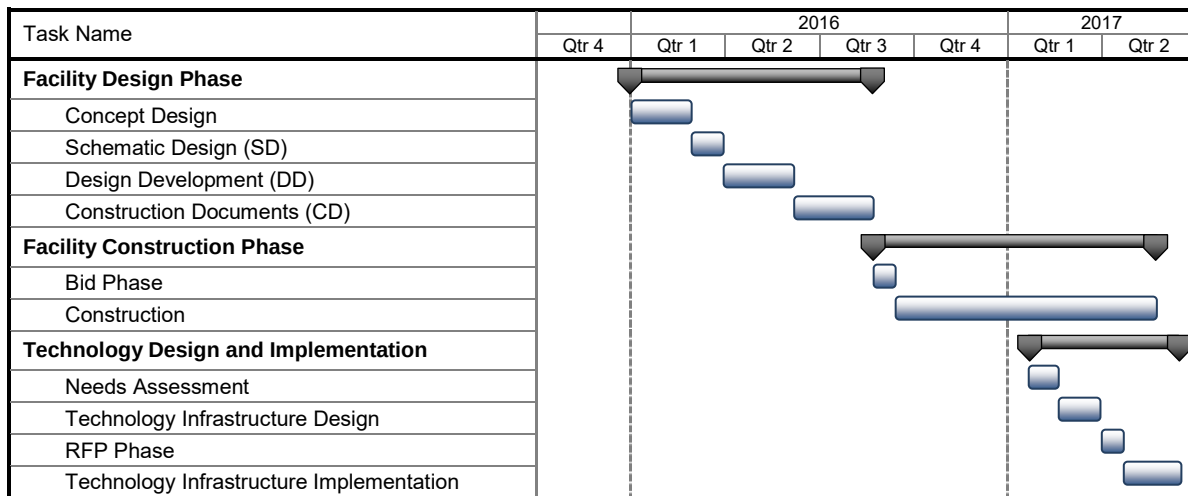


Figure A-1
Traditional A/E Design Process

A.1.2 Traditional Technology Design Process

The technology design process for traditional commercial space often starts after the physical design of the facility has been completed, often weeks afterward.

The technology design process includes a needs assessment that identifies the specific technology requirements of each stakeholder.

When the needs assessment has been completed, the technology design moves into the detailed design and RFP development.

Technology design efforts are sometimes done with little or no coordination with the architectural and engineering design teams. However, doing so may result in inadequate telecommunications spaces and pathways to accommodate the desired telecommunications cabling system.

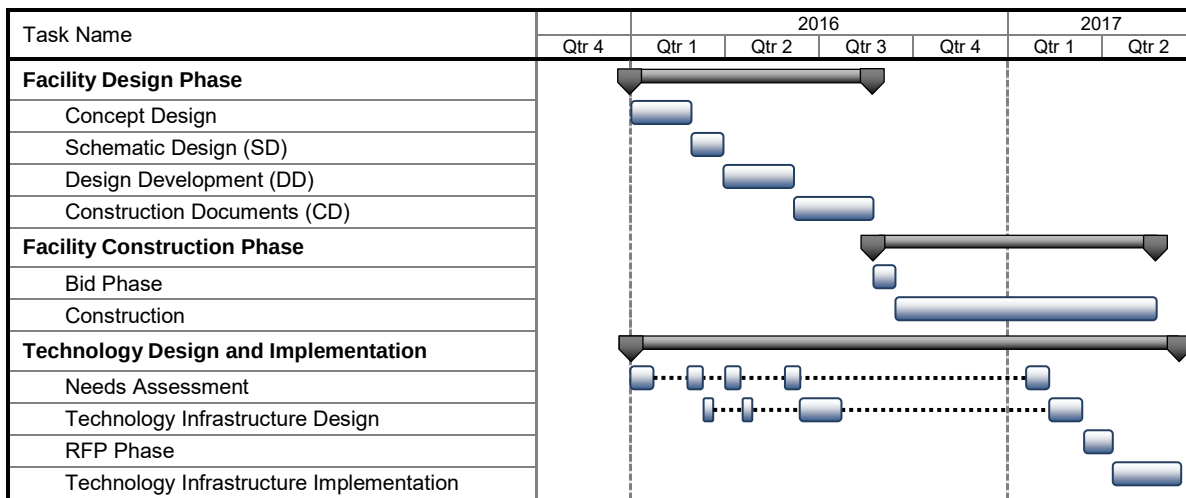


Figure A-2
Data Center A/E Design Process

A.1.3 Data Center Design Process Requirements

A data center is an engineering and technologically complex facility that cannot be approached in a similar manner as traditional commercial space.

The design process must start with a thorough understanding of the technology (network, servers, connectivity) requirements and engineering requirements (power and cooling). The design process for a data center is not focused so much on the “people” space and flow but on the network and computer equipment space and flow. This drives the process to start with the engineering effort before the architectural design effort.

User or application requirements: both user and application requirements tend to drive the reliability of the data center. The design process must gather data regarding the availability and operational requirements of the people and applications supported by the data center and design the space accordingly (see Appendix B for guidance in calculating availability).

A.2 Project Delivery Methods

A.2.1 Design-Bid-Build

The design-bid-build process is a method of project delivery that separates the architectural and engineering design services from construction services.

The end user or owner may hold separate contracts for the design and construction services. The A/E design services and the construction services can both be negotiated or competitively bid in an open or selected market with the responses evaluated with respect to cost, experience, schedule, and any other end user requirement.

The design-bid-build process consists of the entire facility design being completed by the architect/engineering team with the deliverables consisting of a set of construction documents and specifications.

These construction documents (CDs) are then issued to contractors for negotiated or competitive pricing. In a bid environment, the contractors that are allowed to bid are either:

- Invited by the end user
- Selected through a qualification process prior to the issuance of bid documents

The bid documents, prepared based on the user's needs and budget as previously defined, are issued to all contractors interested in bidding.

The architectural/engineering design team will usually be involved in construction administration, which includes periodic site surveys to assess the work progress and compliance with bid documents and specifications.

A.2.2 Design-Build

The design-build process is a method of project delivery in which one entity, the design-builder, provides the architectural, engineering, and construction services all under one contract.

The design-build process starts with a consultant developing the program for the facility to develop the general scope of the project. The general contractor is then selected through either negotiation or competitive bid to complete the design and construction services.

The single entity in the design-build process can be a general contractor, construction management firm, or consulting firm. Each project will result in varying amounts of the scope of work being performed by the single entity. It will be the single entity's responsibility to bring together a team that has the experience to complete the project as required by the end user.

The design-build project delivery method has often been used when the schedule is a primary driver for a successful project. It is also acceptable when schedule is not an issue.

Further information can be obtained from the Design-Build Institute of America website (www.dbia.org).

A.2.3 Construction Management

The construction management (CM) project delivery model can be a fee-based service or an at-risk based service. The construction manager is responsible to, and under contract exclusively with, the owner. The construction manager represents the owners' interests throughout the various phases of the project.

The CM model is similar to the design-bid-build model in that there is a separation of the architectural and engineering design services from the construction services. It is also similar to the design build model in that the CM represents the constructor's perspective throughout the design process, but the CM is solely responsible to the owner and does not have any financial incentive through value engineering during the construction phase.

To obtain the greatest advantage of the CM delivery model, the owner should engage the CM very early in the project at the concept development design phase.

The CM delivery model provides flexibility to the owner in procuring the construction services:

- The owner can procure the construction services, managed by the CM, with a single contract where the general contractor and subtrades are all under contract through one prime contractor.
- The owner can also procure the construction services with multiple contracts where the general contractor and significant subtrades (electrical and mechanical) are under separate contracts directly with the owner; the multiple contracts with the owner would be managed by the CM.

The fee-based CM model is where the CM is under contract to the owner for a fixed fee and all construction contracts are negotiated between the owner and the contractors.

The “at-risk” based CM model is where the CM commits to the owner the delivery of the construction project with a guaranteed maximum price or GMP. This model is similar to the CM acting as a construction consultant to the owner during the design phase and as a prime general contractor during the construction phase.

NOTE: Further information can be obtained from the Construction Management Association of America (<http://cmaanet.org>).

A.3 Facility Design Phases

A.3.1 Planning and Concept Development

The following tasks are commonly included within the planning phase:

- Data center IT and telecommunications infrastructure requirements documents
- Facility programming
- Space relationships/flow diagrams
- Project development scheduling
- Project budgeting
- Life cycle cost studies
- Economic feasibility studies
- Agency consulting/review/approval
- Site selection/analysis utilization
- Environmental studies as well as city or county requirements and permit requirements
- Power requirements and availability
- Energy studies
- Existing facilities surveys
- Client-supplied data coordination
- Services related to project management
- Presentations
- Marketing studies
- Project financing
- Special studies
- Re-zoning assistance
- Project promotion
- Legal survey
- Geotechnical analysis

A.3.2 Schematic Design (SD)

The following tasks are commonly included within the schematic design phase:

- Client-supplied data coordination
- Program and budget evaluation
- Review of alternative design approaches
- Architectural schematic design
- Schematic design drawings and documents
- Statement of probable construction costs
- Client consultation
- Interior design concepts
- Special studies (e.g., future facilities, environmental impact)
- Special submissions or promotional presentations
- Special models, perspectives, or computer presentations
- Project management
- Agency consultation
- IT and telecommunications infrastructure conceptual design documents
- Structural design concepts
- Mechanical design concepts

<List continues on next page>

- Electrical design concepts
- Civil design concepts
- Landscape concepts
- Statements of probable costs

A.3.3 Design Development (DD)

The following tasks are commonly included within the design development phase:

- Client-supplied data coordination
- Design coordination
- Architectural design development
- Design development drawings and documents
- Client consultation
- Interior design development
- Special studies/reports (e.g., planning tenant or rental spaces)
- Promotional presentations
- Models, perspectives, or computer presentations
- Project management
- Agency consultation
- IT and telecommunications infrastructure detailed design documents
- Structural design development
- Mechanical design development
- Electrical design development
- Civil engineering design development
- Landscape development
- Detailed construction cost estimates or quantity surveys
- Cost estimate reconciliation with budget

NOTE: Further information can be obtained from the Design-Build Institute of America (<http://www.dbia.org/>).

A.3.4 Prepurchase

- Define list of long lead items
- Prepare specifications for prepurchase items
- Bid or procure items ahead of issuance of facility construction documents because of possible long lead material cost increases

A.3.5 Construction Documents (CD)

The following tasks are commonly included within the construction documents phase:

- Client-supplied data coordination
- Project coordination
- Architectural construction documents (working drawings, form of construction contract and specifications)
- Document checking and coordination
- Client consultation
- Interior construction documents
- Alternative bid details and special bid documents
- Project management
- Agency consultation
- Low-voltage/telecommunications cabling system bid documents
- Structural construction documents
- Mechanical construction documents
- Electrical construction documents
- Statements of probable costs
- Civil engineering construction documents

<List continues on next page>

- Landscape documents
- Detailed construction cost estimates or quantity surveys
- Cost estimate reconciliation with budget

A.4 Technology Design Phases

A.4.1 Needs Assessment

The following tasks are commonly included within the needs assessment phase:

- Develop a project plan that will outline the tasks, timeframes, and responsibilities for completing the technology project.
- Conduct information gathering sessions identifying and documenting the technology and business needs.
- Review the existing technology systems.
- Interview IT and facilities personnel and determine the group(s) that will be responsible for each portion of the data center infrastructure when the project is complete.
- Review anticipated growth and new technologies.
- Review timeframes, capital, and operational budgets.
- Develop data center IT/Telecommunications infrastructure requirements document.
- Develop a business case for recommendations made during needs assessment analysis.

A.4.2 Design Analysis

The following tasks are included within the design analysis phase:

- Review, evaluate, and prioritize all of the information received and documented during the needs assessments phase
- Validate vendor qualification criteria, technology applications, required infrastructure, industry standards and best practices, budgets and other pertinent information with project stakeholders
- Develop conceptual design for data center IT and telecommunications infrastructure

A.4.3 Acquisition

The following tasks are included within the acquisition phase:

- Develop the detailed IT and telecommunications infrastructure design.
- Draft the RFP for the technology vendor services, including detailed specifications and drawings. The RFP should also include the project organization, expected milestone schedule, current construction schedule, and responsibility matrix.
- Analyze and evaluate all bid responses for accuracy and completeness and financial, technical, and service qualifications.
- Assist in the selection process and final contract review and negotiations.

A.4.4 Implementation

The following tasks are included within the implementation phase:

- Provide project management services to facilitate the implementation of the technology vendor's service contract.
- Facilitate regularly scheduled status meetings to review procedures and processes, maintenance records, and documentation submitted by vendor to ensure that the end user is receiving the service and support as outlined in the service contract.
- Assist end user in measuring and benchmarking services provided by the technology vendor.

A.5 Commissioning

The following tasks are included within the commissioning phase:

- Request design intent document from A/E of record that is reflective of original basis of design identified in concept documents.
- Request sequence of operation for electrical and mechanical components.
- Validate alignment between sequence of operations and controls methodology; review SCADA and building automation system topology and sensor locations.
- Prepare system readiness checklists to be signed off by contractors prior to startup of individual components.
- Prepare verification test procedures for each component in each system and record anomalies encountered.
- Conclude commissioning testing with integrated system test for normal, failure, and maintenance modes; apply simulated loads, such as server simulator load banks, to fully test the entire data center load carrying components.
- Conclude commissioning phase with a lessons learned report that serves to benchmark the operation of electrical and mechanical systems. The corrective action report would also be prepared during this phase.

A.6 Data Center Documentation

A.6.1 Recommendations

Data center documentation should include:

- Construction and implementation:
 - Contract documents:
 - Request for bid/quote
 - Project schedule
 - Specifications
 - Floor plan drawings
 - Outside plant drawings
 - Telecommunications cabling system drawings
 - Equipment layout drawing and details
 - Cabinet and rack elevations
 - Cable pathway details
 - Construction change orders
 - As-built drawings
 - Construction administration reports
 - Test reports
 - Punch-list reports
 - Operations and maintenance (O&M) manuals
 - Close-out, sign-off, and acceptance certificates
 - Certificate of occupancy
- Ongoing change management documentation, including system inventories and configuration databases. These may also be used as a starting point for relocation planning documentation.
- Relocation planning documentation such as equipment, system, and application inventories, including system and application dependencies.

This page intentionally left blank

Appendix B Reliability and Availability (Informative)

This appendix is not part of the requirements of this standard, but it is included to provide additional information related to this standard.

B.1 Introduction

B.1.1 Overview

People have come to expect ready access to information 24 hours a day, every day. The Internet as well as more traditional enterprises—both business and governmental—now operate 7 days a week, 24 hours a day. Typical 24/7 operations include banking systems, credit card companies, 911 emergency centers, telecommunications networks, hospital systems, overnight delivery operations, large multinational concerns, and other international organizations. With the increased reliance on 24/7 availability of information and data processing support, the reliance on mission-critical data processing facilities has also increased.

However, the mission-critical data processing facility requires additional thought and planning, because of its differences with a conventional building (e.g., home, store, office building). Consider some data center and mission-critical facility norms:

- Mission-critical power requirements far exceed any conventional building type. The power supplied to a typical office building is about 110 W/m² (10 W/ft²) while mission-critical facilities often require power between 650 W/m² (60 W/ft²) and 2200 W/m² (200 W/ft²), if not more.
- The ratio of combined mechanical and electrical service space to the overall usable space is typically between 1:3 and 1:4 in a conventional building, but it is close to 1:1 for data centers.
- The cost of mission-critical facilities can run up to four times the cost of more conventional building types as power and cooling requirements drive the cost and design.

These numbers are revealing. Mission-critical power, cooling and network systems evolved from a philosophy dubbed "system + system", meaning that for every critical system, a duplicate system is in place to provide service while the other is repaired, maintained, or tested off-line. Additionally, the risk of natural and provoked disasters causing potential IT downtime dictates a hardened building shell as well as sufficient capacity on site.

Continuous operation implies that critical systems need a measured approach to incorporating reliability with redundant systems being the typical method used. After all, a shutdown can cripple the revenue generating continuity of a business, ruin customer confidence, and possibly threaten its existence if the shutdown is extensive. Disruption to the IT systems underpinning today's industrialized societies may cause loss of life and endanger communities, depending upon the nature and location of the service.

Mission-critical services requiring 7 day at 24 hours/day operations need a comprehensive strategy to sustain their vital activities. Many small businesses have at least a 5 day at 12 hour/day high-availability operating requirement—less rigorous standards, yet still substantial. Mission-critical design variations will stem from each user's requirements. Starting with site selection criteria and working forward through each layer of architectural, engineering, network, IT systems, and operational design, reliability and reducing the risk of downtime must be the prime focus that is weighed and coordinated throughout the design process.

Mission-critical data centers have not traditionally been high-profile projects, yet their design issues are increasingly complex and critical. With an emerging design terminology and vocabulary, their rapid evolution calls for an exceptional degree of building and IT systems coordination and integration. These data centers are not merely warehouses for servers; instead, they rival medical operating rooms or semiconductor plants, with their precise environmental controls and power requirements. Intense, sustained work shifts with employees monitoring computer screens mean that workplace design issues must also be addressed.

Important facility design considerations also extend well beyond the context of the mission-critical building itself. Utility deregulation is causing uncertainty. Increasing power demands challenge reliability of the power supply itself. Some utilities even question their own capacity to power mission-critical facilities. Because IT plants can be highly sensitive to temperature and power fluctuations, these concerns are attracting increased attention. It is not an issue that can be addressed simply through the purchase of UPS systems.

To increase the likelihood of success of a mission-critical facility, required performance levels of availability and reliability should be defined, prior to the start or formalization of the design, procurement, and maintenance requirements and processes. Failure to define performance and availability levels prior to the project start often yields higher construction, implementation, and operational costs as well as inconsistent and unpredictable performance.

B.1.2 Goals and Objectives

This appendix presents an overview for planning mission-critical data centers with the following strategic goals:

- Establish a consistent, cost-effective process
- Develop optimum design and implementation solutions
- Develop a common enterprise-wide design vocabulary
- Establish performance criteria used to generate or evaluate mission-critical data center services.

Additionally, this appendix provides a method for determining data center criticality, which aids in the alignment of project objectives and budgets with appropriate performance levels. It should be noted that the recommendations reached by using this method can then be presented to management for determining if the cost of implementation can be justified.

The information and method presented within this Appendix does not address business continuity requirements. For example, an enterprise may be better served by multiple data centers of lower Availability Class (See Section B.6) than a single data center of a higher Availability Class.

NOTE: Information on multiple data center architectures can be found in Appendix E.

B.2 Creating Mission-Critical Data Centers Overview

There are four stages in the process of designing a new mission-critical data center or upgrading an existing one. These are represented in Figure B-1 and described afterward.

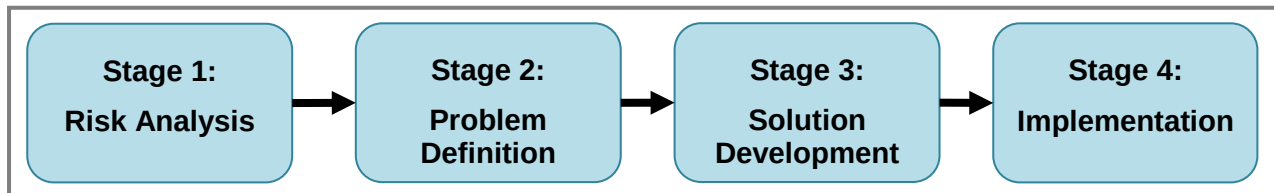


Figure B-1
Planning Process for a Mission-Critical Facility

- **Stage 1: Risk Analysis**
Risk analysis is a linear process. Three key characteristics are defined to arrive at an expression of the criticality of a mission-critical data center:
 - Identify operational requirements for the section of the data center under analysis—the opportunity to suspend operations for scheduled maintenance
 - Identify availability requirements—the targeted uptime of the systems or zones during operations and the ability to endure unplanned interruption of operations
 - Define the impact of downtime—the consequences of unplanned disruptions on the mission
 The process of analyzing and mitigating risk is described in Section B.3. Risk analysis also serves as an important reference source for the remaining three stages of creating a mission-critical data center.
- **Stage 2: Problem Definition**
After completing risk analysis, characterize the data center in terms of computer room space, power, and cooling capacity required to support IT hardware (which may be used to define ITE density) and anticipated redundancy requirements. This information is usually documented in the data center concept design.
- **Stage 3: Solution Development**
Convert the data center conceptual design into one or more design solutions to solve the specific design problem and meet the objectives of the targeted Availability Class.

<List continues on next page>

- Stage 4: Implementation

Construct the chosen solution, incorporating implementation tactics consistent with the targeted Availability Class. This will include appropriate maintenance and operations procedures to ensure a sustainable level of availability.

The remainder of this Appendix pertains to risk analysis and the methodology for selecting data center design Availability Classes.

B.3 Risk Analysis

It is impossible to eliminate the risk of downtime, but risk reduction is an important planning element. In an increasingly competitive world, it is imperative to address downtime in business decisions. The design of systems supporting critical IT functions depends on the interaction between the criticality of the function and its operational profile.

Criticality is defined as the relative importance of a function or process as measured by the consequences of its failure or inability to function. The operational profile expresses the time intervals over which the function or process must operate.

To provide optimal design solutions for a mission-critical data center, consider several key factors. NFPA 75 identifies seven considerations for protection of the environment, equipment, function, programming, records, and supplies in a data center. These include:

- What are the life safety aspects of the function? For example, if the system failed unexpectedly, would lives be put at risk? Examples of such applications include automated safety systems, air traffic control, and emergency call centers.
- What is the threat to occupants or exposed property from natural, man-made, or technology-caused catastrophic events? Will the building be:
 - Equipped with fire suppression?
 - Located within a flood zone?
 - Require seismic reinforcement or dampening because of ground stability and vibration transmission?
 - Located within a tornado or hurricane “corridor”?
- What would be the economic loss to the organization from the loss of function or loss of records?
- What would be the economic loss to the organization from damaged or destroyed equipment?
- What would be the regulatory or contractual impact, if any? For example, if unplanned downtime resulted in loss of telephone service or electrical service to the community, would there be penalties from the government?
- What would be the impact of disrupted service to the organization’s reputation? For example, would subscribers switch to a competitors’ service?
- What is the access to redundant off-site processing systems (e.g., “high performance computing”, massively paralleled systems, cloud service provider, disaster recovery site, backup data center)?

The methodology presented in Section B.5 for determining a data center’s facility Availability Class integrates these considerations and defines the appropriate risk management strategy.

B.4 Availability

B.4.1 Introduction

Availability is the probability that a component or system is in a condition to perform its intended function. While similar to *reliability*, availability is affected by more events than a failure requiring repair or replacement of a component or system.

B.4.2 Calculating Availability

While there are different formulae to calculate availability for calculations involving systems, availability, in its simplest form, is the ratio of uptime observed during a specified interval over the total time of that interval (Equation B-1).

$$\text{Availability} = \frac{\text{Uptime within Observation Interval}}{\text{Total Time of Observation Interval}} \quad (\text{B-1})$$

While equation B-1 can generate the availability of a system, the result does not provide information which can be used to improve the observed value. By splitting total time into its two primary elements (uptime and downtime), the equation changes to the form shown in equation B-2.

$$\text{Availability} = \frac{\text{Uptime}}{\text{Uptime} + \text{Downtime}} \quad (\text{B-2})$$

While equation B-2 proves mathematically what is known through observation or experience (reductions in downtime increases availability), downtime itself can be split into two types: scheduled and unscheduled.

When the two types of downtime are inserted into equation B-2, the resultant equation is shown in equation B-3.

$$\text{Availability} = \frac{\text{Uptime}}{\text{Uptime} + \text{Scheduled Downtime} + \text{Unscheduled Downtime}} \quad (\text{B-3})$$

Thus, equation B-3 shows that availability can be increased by reductions in one or both types of downtime.

B.4.3 Types of Downtime

B.4.3.1 Scheduled Downtime

Scheduled downtime contains activities or events such as:

- Preventive maintenance
- System and equipment setup and upgrades
- System testing/optimization
- Scheduled facilities related events
- Remedial maintenance

B.4.3.2 Unscheduled Downtime

Unscheduled downtime events include:

- Repairs due to failure
- Maintenance delay
- Facility-related failures/outages

B.5 Determining the Data Center Availability Class

B.5.1 Overview

While there are innumerable factors that can be evaluated in a mission-critical data center, there are three factors that can quickly be quantified, providing for an easy determination of an Availability Class and the necessary functions and features required for data center services. These factors are:

- Operational requirements
- Operational availability
- Impact of downtime

Paying careful attention to these factors determines an appropriate Availability Class that matches the mission-critical data center cost with the functions it is intended to support.

Figure B-2 shows how these factors interact in determining the data center services Availability Class with these factors and how to determine an Availability Class described in Sections B.5.2–B.5.5.

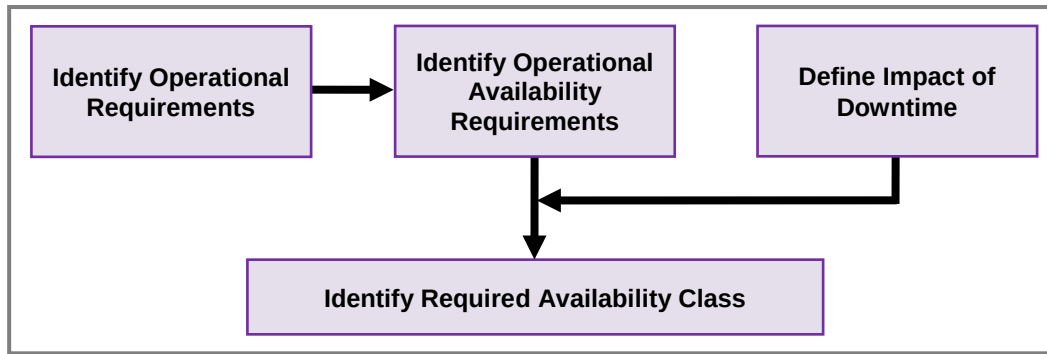


Figure B-2
Relationship of Factors in Data Center Services Availability Class

B.5.2 Identify Operational Requirements

The first step in determining the Availability Class associated with mission-critical data center services is to define the data center's intended operational requirements. Sufficient resources must be available to achieve an acceptable level of quality over a given time period. IT functions that have a high-quality expectation over a longer time period are by definition more critical than those requiring less resources, lower quality, and/or are needed over a shorter time period.

While there are many factors in operations, the key factor to be assessed in this step is the amount of time to be provided for testing and maintenance activities that disrupt normal operation. This is often known as *planned maintenance shutdown*. Once the time for planned maintenance shutdowns is known, this value can be used within Table B-1 to determine an Operational Level. The value of time used should not include projections for unplanned repairs or events.

The indicated Operational Level is used in the next step (see Section B.5.3).

Table B-1 Identifying Operational Requirements: Time Available For Planned Maintenance Shutdown

<i>Operational Level</i>	<i>Annual Hours Available for Planned Maintenance Shutdown</i>	<i>Description</i>
0	> 400	Functions are operational less than 24 hours a day and less than 7 days a week. Scheduled maintenance down time is available during working hours and off hours.
1	100-400	Functions are operational less than 24 hours a day and less than 7 days a week. Scheduled maintenance down time is available during working hours and off-hours.
2	50-99	Functions are operational up to 24 hours a day, up to 7 days a week, and up to 50 weeks per year; scheduled maintenance down time is available during working hours and off hours.
3	0-49	Functions are operational 24 hours a day, 7 days a week for 50 weeks or more. No scheduled maintenance down time is available during working hours.
4	0	Functions are operational 24 hours a day, 7 days a week for 52 weeks each year. No scheduled maintenance down time is available.

NOTE: The term *shutdown* means that operation has ceased; the equipment is not able to perform its mission during that time. Shutdown does *not* refer to the loss of system components if they do not disrupt the ability of the system to continue its mission.

B.5.3 Quantify and Rank Operational Availability Requirements

The second step in determining the Availability Class is to identify the data center's operational availability requirements, specifically the total uptime that the data center services must support without disruption. The term *availability* includes that ITE is operational and able to perform its function; it does not solely refer to operation of the supporting infrastructure. Operational availability refers only to scheduled uptime—that is, the time during which the IT functions are actually expected to run.

These operational availability requirements are reflected by the determination of an Operational Availability rating. By using the Operational level determined in the previous step (See Section B.5.2) and indexing that value with the allowed maximum annual downtime within Table B-2, an Operational Availability Rating is indicated.

NOTE: The Operational Availability Rating is used in conjunction with information from the next step (See Section B.5.4) to determine the Data Center Availability Class (shown in Section B.5.5).

Table B-2 Identifying Operational Availability Rating: Maximum Annual Downtime (Availability %)

Operational Level (from Table B-1)	Allowable Maximum Annual Downtime (minutes) (Availability as %) ¹				
	>5000 (> 99%)	500 – 5000 (99% > 99.9%)	50 – 500 (99.9% > 99.99%)	5 – 50 (99.99% > 99.999%)	0.5 – 5.0 (99.999% > 99.9999%)
Level 0	0	0	1	2	2
Level 1	0	1	2	2	2
Level 2	1	2	2	2	3
Level 3	2	2	2	3	4
Level 4	3	3	3	4	4

NOTE: Availability is sometimes expressed as a percentage, or *nines of availability*. Thus, “five nines of availability” means that the system is fully operable 99.999% of the time throughout a year.

The cost of downtime must be weighed against the cost of mitigating risks in achieving high availability. Note that less than a second of power interruption or a few minutes of cooling interruption can result in hours of recovery time. Thus, the objective is to identify the intersection between the allowed maximum annual downtime and the intended operational level. A function or process that has a high availability requirement with a low operational profile has less risk associated with it than a similar function with a higher operational profile.

B.5.4 Determine Impact of Downtime

The third step in determining the Availability Class is to identify the impact or consequences of downtime. This is an essential component of risk management because not all downtime has the same impact on mission-critical data center services. Identifying the impact of downtime on mission-critical functions helps determine the tactics that will be deployed to mitigate downtime risk. As shown in Table B-3, there are five impact classifications, each associated with a specific impact scope.

B.5.5 Identify the Data Center Availability Class

The final step in determining the data center Availability Class is to combine the three previously identified factors to arrive at a usable expression of availability. This expression of availability is used as a guide to determine the facility (architectural and engineering) and IT (network, cable plant, computer processing and storage system) features needed to appropriately support critical IT functions. Since operational level is subsumed within the availability ranking, as explained in Section B.5.3, the task is to matrix the availability ranking against the impact of downtime to arrive at an appropriate Availability Class. Table B-4 shows the intersection of these two values, and the resultant Data Center Availability Class.

Table B-3 Classifying the Impact of Downtime on the Mission

<i>Classification</i>	<i>Description – Impact of Downtime</i>
Isolated	Local in scope, affecting only a single function or operation, resulting in a minor disruption or delay in achieving non-critical organizational objectives.
Minor	Local in scope, affecting only a single site, or resulting in a minor disruption or delay in achieving key organizational objectives.
Major	Regional in scope, affecting a portion of the enterprise (although not in its entirety) or resulting in a moderate disruption or delay in achieving key organizational objectives.
Severe	Multiregional in scope, affecting a major portion of the enterprise (although not in its entirety) or resulting in a major disruption or delay in achieving key organizational objectives.
Catastrophic	Affecting the quality of service delivery across the entire enterprise or resulting in a significant disruption or delay in achieving key organizational objectives.

Table B-4 Determining Data Center Services Availability Class

<i>Impact of Downtime (from Table B-3)</i>	<i>Operational Availability Rating (from Table B-2)</i>				
	<i>0</i>	<i>1</i>	<i>2</i>	<i>3</i>	<i>4</i>
Isolated	Class 0	Class 0	Class 1	Class 3	Class 3
Minor	Class 0	Class 1	Class 2	Class 3	Class 3
Major	Class 1	Class 2	Class 2	Class 3	Class 3
Severe	Class 1	Class 2	Class 3	Class 3	Class 4
Catastrophic	Class 1	Class 2	Class 3	Class 4	Class 4

B.6 Data Center Availability Classes

To a great degree, design decisions are guided by the identified Availability Class. Therefore, it is essential to fully understand the meaning of each Availability Class. Each Availability Class is defined in terms of four areas of concern:

- 1) **Component redundancy** increases reliability by providing redundancy for critical high-risk, low-reliability components within systems.
- 2) **System redundancy** increases reliability even more by providing redundancy at the system level.
- 3) **Quality** ensures that high quality is designed and implemented in the data center, thereby reducing the risk of downtime due to failure during initial installation and/or premature wear. Since MTBF is a major factor in the determination of system reliability, it stands to reason that higher quality components with lower failure rates will result in systems that are more reliable.
- 4) **Survivability** refers to reducing the risk of downtime by protecting against external events such as physical forces, security breaches, and natural disasters.

The following subsections provide more detail on how each of these four factors is defined for each of the five Availability Classes. Each Class also includes an example application for facility power.

NOTE: Facility power in the examples below uses the prefix “F”, as listed Section B.7.

B.6.1 Availability Class 0

The objective of Class 0 is to support the basic requirements of the IT functions without supplementary equipment. Capital cost avoidance is the major driver. There is a high risk of downtime because of planned and unplanned events. However, in Class 0 data centers maintenance can be performed during non-scheduled hours, and downtime of several hours or even days has minimum impact on the mission.

Table B-5 Tactics for Class 0

Component redundancy:	None
System redundancy:	None
Quality control:	Standard commercial quality
Survivability:	None
Application:	A critical power distribution system separate from the general use power systems would not exist. There would be no back-up generator system. The system might deploy surge protective devices, power conditioning, or even small or non-redundant uninterruptible power supply (UPS) systems to allow the specific equipment to function adequately. Utility grade power does not meet the basic requirements of critical equipment. No redundancy of any kind would be used for power, air conditioning, or networking for a similar reason. Class F0 has multiple single-points of failure.

B.6.2 Availability Class 1

The objective of Class 1 is to support the basic requirements of the IT functions. There is a high risk of downtime because of planned and unplanned events. However, in Class 1 data centers, remedial maintenance can be performed during nonscheduled hours, and the impact of downtime is relatively low.

Table B-6 Tactics for Class 1

Component redundancy:	None
System redundancy:	None
Quality control:	Standard commercial quality
Survivability:	None
Application:	In Class F1, the critical power distribution system would deploy a stored energy device and a generator to allow the critical equipment to function adequately (utility grade power does not meet the basic requirements of critical equipment). No redundancy of any kind would be used for power or air conditioning for a similar reason.

B.6.3 Availability Class 2

The objective of Class 2 is to provide a level of reliability higher than that defined in Class 1 to reduce the risk of downtime because of component failure. In Class 2 data centers, there is a moderate risk of downtime as a result of planned and unplanned events. Maintenance activities can typically be performed during unscheduled hours.

Table B-7 Tactics for Class 2

Component redundancy:	Redundancy is provided for critical components
System redundancy:	None
Quality control:	Premium quality for critical components
Survivability:	Moderate hardening for physical security and structural integrity
Application:	In Class F2, the critical power, cooling, and network systems would need redundancy in those parts of the system that are most likely to fail. These would include any products that have a high parts count or moving parts, such as UPS, controls, air conditioning, generators, ATS or systems that are outside the control of the data center management such as network access carrier services. In addition, it may be appropriate to specify premium quality devices that provide longer life or better reliability.

B.6.4 Availability Class 3

The objective of Class 3 is to provide additional reliability and maintainability to reduce the risk of downtime because of natural disasters, human-driven disasters, planned maintenance, and repair activities. Maintenance and repair activities will typically need to be performed during full production time with no opportunity for curtailed operations.

Table B-8 Tactics for Class 3

Component redundancy:	Redundancy is required for critical and noncritical components, except where the component is part of a redundant system; redundancy is also provided to increase maintainability.
System redundancy:	System redundancy is required where component redundancy does not exist
Quality control:	Premium quality for all components
Survivability:	Significant hardening for physical security and structural integrity
Application:	In Class F3, the critical power, cooling, and network systems must provide for reliable, continuous operations even when major components (or, where necessary, major subsystems) are out of service for repair or maintenance. To protect against unplanned downtime, the power, cooling, and network systems must be able to sustain operations while a dependent component or subsystem is out of service.

B.6.5 Availability Class 4

The objective of Class 4 is to eliminate downtime through the application of all tactics to provide continuous operation regardless of planned or unplanned activities. All recognizable single points of failure are eliminated. Systems are typically automated to reduce the chances for human error and are staffed 24/7. Rigorous training is provided for the staff to handle any contingency. Compartmentalization and fault tolerance are prime requirements for a Class 4 data center.

Table B-9 Tactics for Class 4

Component redundancy:	Redundancy is provided for all critical components and to increase maintainability; also provided for noncritical components.
System redundancy:	System redundancy is provided with component redundancy so that overall reliability is maintained even during maintenance activities.
Quality control:	Premium quality for all components. Where practical, equipment and components in the primary and redundant systems should come from different manufacturers, be a different model, or from different production lots as to avoid being affected by the same type fault or component recall simultaneously.
Survivability:	All systems are self-supporting in any event and are protected against the highest levels of natural forces.
Application:	The critical power, cooling, and network systems in a Class F4 facility must provide for reliable, continuous operations even when major components (or, where necessary, major subsystems) are out of service for repair or maintenance. To protect against unplanned downtime, systems must be able to sustain operations while a dependent component or subsystem is out of service.

B.7 Availability Class Sub Groups

The data center is not just a facility or building, but it is a collection of services that supports the critical business processes. The data center services Availability Class model can be used to guide design and operational decisions for the following critical services:

- Facility: The facility systems (e.g., power, cooling, controls) can be categorized into one of the sub group Class F0 through Class F4 as indicated in Sections 7, 9, and, 10.
- Cable Plant: The network cable plant topology can be categorized into one of the sub group Class C0 through Class C4 as indicated in Section 14.
- Network Infrastructure: The network architecture and topology can be categorized into one of the sub group Class N0 through Class N4 as indicated in Section 15.
- Data Processing and Storage Systems: The computer processing and storage systems can be categorized into one of the sub group Class S0 through Class S4 as indicated in Appendix C.
- Applications: The applications can be categorized into one of the sub group Class A0 through Class A4 as indicated in Appendix C.

B.8 Reliability Aspects of Availability Planning

Achieving an optimum Class of availability for a mission-critical data center requires strategic planning to determine the risks, design features, and potential improvement measures that will lead to fewer critical-systems related failures.

B.8.1 Reliability Engineering Principles and Calculating Reliability

Reliability is the probability that equipment or a system will perform its intended function, within stated conditions, for a specified period of time without failure. It is expressed as a percentage (i.e., a number between 0 and 1), in which a lower percentage indicates a greater likelihood of failure in a given period of time. Reliability is not the same as *availability*. Whereas reliability uses the number (frequency) of failures within a period of time within its calculation, availability utilizes the amount of time equipment or a system is non-operational as a result to planned or unplanned failures, interruptions, or events.

Over the last 30 years, data has been collected and analyzed for a wide variety of mechanical and electrical components and their failure characteristics. This has led to broad-based industry standards for the analysis and design of reliable power and cooling systems (e.g., IEEE Standard 493 (Gold Book)—*IEEE Recommended Practice for the Design of Reliable Industrial and Commercial Power Systems*).

The reliability of a given system can be calculated from the published MTBF (mean time between failures) data for given components of that system. This calculation can then be combined to yield an overall expression of system reliability through the analysis of all series and parallel subsystems. The calculations are as follows:

$$R = e^{(-\lambda T)} \quad (B-4)$$

where:

- R = reliability (percent probability of success)
- e = exponential function
- λ = failure rate (the reciprocal of MTBF)
- T = time period (same units as failure rate)

Example: A UPS module has a published MTBF of 17,520 hours (one failure every two years). Its failure rate would then be 0.0005708 failures per hour. What is its one-year reliability or the probability of not failing in one year (8,760 hours)?

$$R = e^{(-0.0005708 \times 8,760)}$$

$$R = 0.6065 \text{ or } 60.65\%$$

To obtain the reliability of a given system, the individual reliability of each component must be calculated, then the reliability of parallel subsystems, and then the series reliability of all subsystems as follows and as illustrated in Figure B-3.

The reliability of a series system is equal to the product of all component reliabilities. The reliability of a parallel system is equal to the complement of the product of all component complements. Thus, the reliability for the system in Figure B-3 would be calculated as follows:

$$R_{A1A2} = R_{A1} \times R_{A2} = 0.5 \times 0.5 = 0.25$$

$$R_A = 1 - [(1 - R_{A1A2}) \times (1 - R_{A3})] = 1 - [(1 - 0.25) \times (1 - 0.5)] = 0.625$$

$$R_B = 1 - [(1 - R_{B1}) \times (1 - R_{B2})] = 1 - [(1 - 0.61) \times (1 - 0.61)] = 0.848$$

$$R_{TOTAL} = R_A \times R_B = 0.625 \times 0.848 = 0.53 \text{ (53\%)}$$

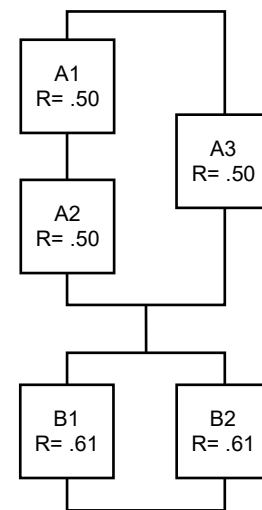


Figure B-3
Sample Reliability Calculation

B.8.2 Trends Affecting Reliability of Critical IT Facilities

As more and more clients require service-level guarantees, service providers and facility managers must determine what data center service performance is required to provide the agreed-to or sufficient end user availability. Table B-10 shows the relationship between availability percentage and allowable downtime.

Availability levels of 99.99% (50 minutes of downtime per year) allow practically no downtime for maintenance or other planned or unplanned events. Therefore, migrating to high-reliability solutions is imperative.

As computers have become more reliable, the overall percentage of downtime events caused by critical system failures has grown. Although the occurrence of such outages remains small, the total availability is dramatically affected because repair times (mean time to repair or MTTR) for certain critical system outages are lengthy (i.e., generator, UPS, chiller).

Where practical, equipment in redundant systems should come from different manufacturers, or different models or different production lots, as to avoid both systems being affected by the same type fault or component recall simultaneously.

Table B-10 Relationship Between Availability Percentage and Allowable Downtime

<i>Targeted Availability (percent)</i>	<i>Allowable Maximum Annual Downtime (minutes)</i>
< 99.0	>5000
99 to 99.9	500 – 5000
99.9 to 99.99	50 – 500
99.99 to 99.999	5 – 50
99.999 to 99.9999	0.5 – 5.0

B.8.3 Planning Process

A proactive, strategic planning approach to mission-critical data center design and management requires a five-step process:

- 1) Analyze the current data center.
- 2) Identify and prioritize risks and vulnerabilities.
- 3) Provide solutions to minimize risks.
- 4) Develop an implementation strategy.
- 5) Measure performance, and verify improvement.

This process should be performed in a continual cycle over the course of a year (see Figure B-4). By use of this cycle, plans can be refined and modified as objectives are met or new technology is deployed.

B.9 Other Factors

The process by which mission-critical Availability Classes are defined is not a perfect science. As projects are built, there will be unexpected outcomes and learned lessons. The following are just a few factors that may alter the selected Availability Class. Other factors will be added over time.



Figure B-4
Continuous Improvement Cycle

B.9.1 Intangible Consequences of Downtime

On occasion, a new product rollout, technical initiative, or other major endeavor will be announced. With heightened press exposure or internal performance pressures, there will be an incalculable and unpredictable cost of unplanned downtime. Avoiding these types of circumstances may dictate a higher Availability Class than is otherwise indicated.

B.9.2 Scheduled Deployment

If a critical IT function must be deployed quickly, it may dictate different risk management strategies outside that normally considered.

B.9.3 Unusual Budget Constraints

If the established budget for a critical data center will not support the required Availability Class, then a less reliable data center will need to be implemented unless additional funding is provided.

B.10 Other Reliability Alternatives

System designs with clustered systems having nodes spread across two or more Class 3 data centers can meet or exceed the uptime of a system in a single Class 4 data center. In such a design, the first failover is to the local node (synchronous), the second failover is to a nearby data center (~16 km [10 miles], and still synchronous), and the third is to a remote data center (but asynchronous).

Such a design does increase the facility's overhead and therefore, the cost. However, it offers a way for designers to avoid many of the costs associated with Class 4 data centers, whether owned, leased or collocated.

B.11 Reliability Planning Worksheet

Use the following planning guide starting on the next page to determine the critical IT requirements.

Project name: _____

Project number: _____

Project description: _____

Project location: _____

STEP 1: Determine Operational Requirements

- 1) How many hours of operation must be supported during a production week? _____
- 2) How many scheduled production weeks are there? (if production occurs every week enter 52.14) _____
- 3) Multiply line 1 by line 2, and enter here. This is annual production hours: _____
- 4) Subtract line 3 from 8,760, and enter the result here: _____
- 5) Are there additional available days or weekends each year for scheduled downtime that have not been accounted for in lines 2 or 3? Enter the total annual available hours: _____
- 6) Add lines 4 and 5 and enter the result (allowable annual maintenance hours) here: _____
- 7) If line 6 is greater than 400, the Operational Level is 0; otherwise, proceed to the next line.
- 8) If line 6 is greater 100, the Operational Level is 1; otherwise, proceed to the next line.
- 9) If line 6 is between 50 and 99, the Operational Level is 2; otherwise, proceed to the next line.
- 10) If line 6 is between 1 and 49, the Operational Level is 3; otherwise, the Operational Level is 4.

STEP 2: Determine Operational Availability Rank.

- 1) Based on the operational level from Step 1 above:
 - Level 0; Proceed to line 2.
 - Level 1; Proceed to line 3.
 - Level 2; Proceed to line 4.
 - Level 3; Proceed to line 5.
 - Level 4; Proceed to line 6.
- 2) Operational Level 0: If the maximum annual downtime is:
 - 500 minutes or greater, then the availability requirement is Operational Availability Rank 0.
 - Between 50 and 500 minutes, then the availability requirement is Operational Availability Rank 1.
 - Less than 50 minutes, then the availability requirement is Operational Availability Rank 2.Proceed to Step 3.
- 3) Operational Level 1: If the maximum annual downtime is:
 - 5000 minutes or greater, then the availability requirement is Operational Availability Rank 0.
 - Between 500 and 5000 minutes, then the availability requirement is Operational Availability Rank 1.
 - Less than 500 minutes, then the availability requirement is Operational Availability Rank 2.Proceed to Step 3.
- 4) Operational Level 2: If the maximum annual downtime is:
 - 5000 minutes or greater, then the availability requirement is Operational Availability Rank 1.
 - Between 5 and 5000 minutes, then the availability requirement is Operational Availability Rank 2.
 - Less than 5 minutes, then the availability requirement is Operational Availability Rank 3.Proceed to Step 3.

<Continues on next page>

- 5) Operational Level 3: If the maximum annual downtime is:
 - 50 minutes or greater, then the availability requirement is Operational Availability Rank 2.
 - Between 5 and 50 minutes, then the availability requirement is Operational Availability Rank 3.
 - Less than 5 minutes, then the availability requirement is Operational Availability Rank 4.
 Proceed to Step 3.
- 6) Operational Level 4: If the maximum annual downtime is:
 - 50 minutes or greater, then the availability requirement is Operational Availability Rank 3.
 - Less than 50 minutes, then the availability requirement is Operational Availability Rank 4.
 Proceed to Step 3.

STEP 3: Define Mission-Critical Risk Level

Downtime will reduce or negatively impact operations (select one):

- Catastrophic (e.g., across the entire enterprise) _____
- Severe (e.g., across a wide portion of the enterprise) _____
- Major (e.g., across a single region or department) _____
- Minor (e.g., at a single location) _____
- Isolated (e.g., a single non-critical function) _____

STEP 4: Determine from the Table below

- 1) Select the column from the Operational Availability Rank in Step 2.
- 2) Select the row from the Risk Level in Step 3.
- 3) Your Availability Class is where the two intersect: _____

Data Center Services Availability Class

<i>Impact of Downtime</i>	<i>Operational Availability Rank</i>				
	<i>0</i>	<i>1</i>	<i>2</i>	<i>3</i>	<i>4</i>
Isolated	Class 0	Class 0	Class 1	Class 3	Class 3
Minor	Class 0	Class 1	Class 2	Class 3	Class 3
Major	Class 1	Class 2	Class 2	Class 3	Class 3
Severe	Class 1	Class 2	Class 3	Class 3	Class 4
Catastrophic	Class 1	Class 2	Class 3	Class 4	Class 4

This page intentionally left blank

Appendix C Alignment of Data Center Services Reliability with Application and System Architecture (Informative)

This appendix is not part of the requirements of this standard, but it is included to provide additional information related to this standard.

C.1 Overview

The BICSI reliability classification framework can be used to guide the data center network, network cable plant, and facility systems. It is important to first understand the constraints or flexibility that is built into the application architecture and the processing and storage systems architecture before defining the reliability requirements of the underlying lower level systems. If the applications support location transparent high availability clusters or cloud services (either private or public cloud based services) that can be implemented across multiple data centers, then the reliability of each data center facility may be able to be reduced as the reliability is built into the technology rather than the facility. This framework is provided to support the analysis of the data center services end-to-end reliability. After all, the “data center” is not just a facility or building, but it is a collection of services that supports critical business processes.

C.2 Application Reliability

The application layer content within this appendix is not meant to drive various methods of application architecture, but rather to identify how application architecture designs can be categorized into the reliability Classes based on how they can meet the defined performance characteristics. With the application architecture design quantified according to the performance requirements of the reliability Classes, it will be possible to correlate the required performance characteristics of the underlying data center service layers, enabling the end-to-end alignment. This framework can assist in:

- Identifying how lower level services can be designed with increased redundancy to overcome the impact of reduced reliability of monolithic application architecture.
- Identify how developing distributed location transparent application architecture with increased redundancy across multiple lower level services can take advantage of reducing the reliability Class of the lower level services.

One of the key elements of any application design is the architecture of the application layers. This architecture defines how the pieces of the application interact with each other and what functionality each piece is responsible for performing. The application layer is divided up to create a series of application layers, each of which is responsible for an individual or atomic element of the application's processing. Applications that meet the higher level performance requirements generally have each layer running on a different system or in a different process space on the same system than the other layers.

The application layers consist of:

- **Presentation:** The presentation layer contains the components that are required to enable user interaction with the application.
- **Business Logic:** The business logic layer is where the application-specific processing and business rules are maintained.
- **Data:** The data layer consists of data access and data store. Data access is responsible for communicating (I/O) and integrating with the data stores that the application needs to be able to function. Data store consist of the data sources accessed by the application. The data sources could be databases, structured, or unstructured file systems.

For the performance characteristics, the application is prefaced with an “A” to identify how it aligns with the reliability Class criteria.

C.2.1 Data Center Application Architecture Availability Classes

The following application architecture examples merely represent one example of many software engineering solutions.

C.2.2 Availability Class A0 and A1

Application layers are implemented without the ability to be distributed or enable diverse user access. Application layers are hardware dependent, non-redundant with no seamless failover or self-healing capabilities from presentation to data layer. All application layers may be implemented on the same process space on the same system.

Table C-1 Tactics for Class A0 and A1

Presentation Layer:	Common user access
Business Logic Layer:	Hardware dependent, monolithic logic
Data Layer:	Non-redundant I/O, hardware dependent non-redundant data sources

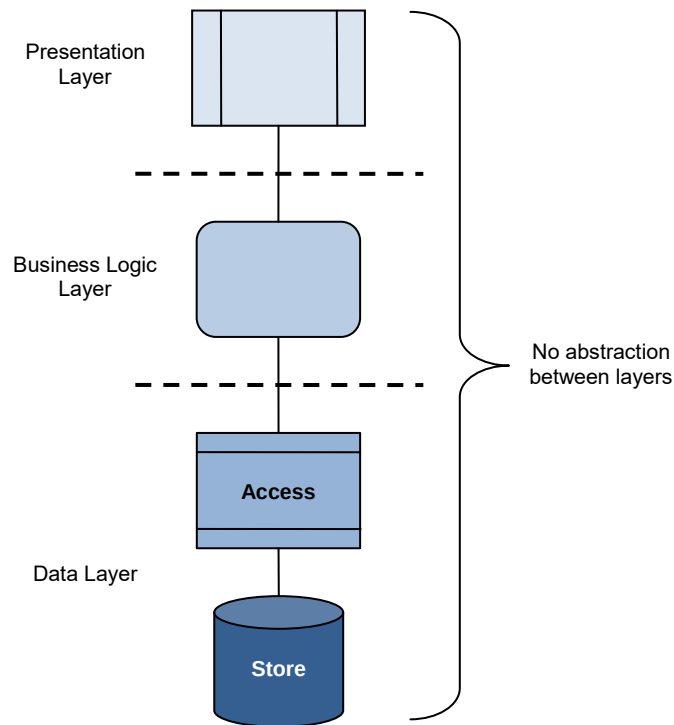


Figure C-1
Class A0 and A1 Application Architecture

C.2.3 Availability Class A2

Business logic layer is designed to support seamless transition between distributed logic. Data layer is designed to support redundant I/O, providing failover or self-healing capabilities. Application layers may be hardware dependent. All application layers may be implemented on the different process spaces on the same system. Active-passive application architecture is an example of application reliability classification A2.

Table C-2 Tactics for Class A2

Presentation Layer:	Common user access
Business Logic Layer:	Hardware dependent, distributed logic
Data Layer:	Support for redundant I/O and redundant hardware dependent data sources

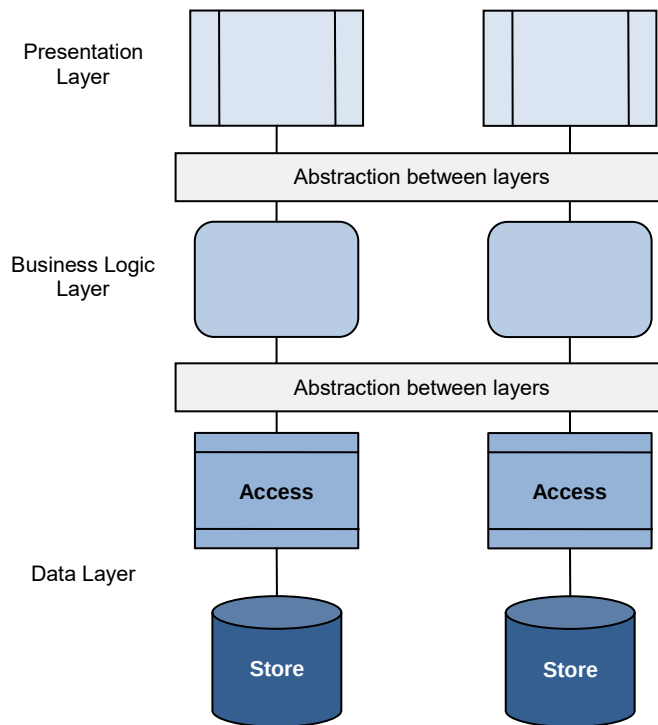


Figure C-2
Class A2 Application Architecture

C.2.4 Availability Class A3 and A4

Business logic layer is designed with seamless transition between redundant distributed logic and hardware platforms. Data layer provides failover or self-healing capabilities on redundant platforms. Application layers will be hardware independent, supporting virtualization and virtual server relocation across the enterprise. The application architecture is capable of expanding horizontally within individual application layers or across all application layers, either within a common data center, across multiple data centers or data center service providers. Each application layer will run on a different system. Active-active architecture supporting virtual server relocation, service orientated architecture (SOA), and location transparent cloud-based application architectures are examples of application reliability classification A3 and A4.

Table C-3 Tactics for Class A3 and A4

Presentation Layer:	Diverse user access
Business Logic Layer:	Hardware abstraction, distributed logic
Data Layer:	Redundant I/O, redundant hardware independent data sources

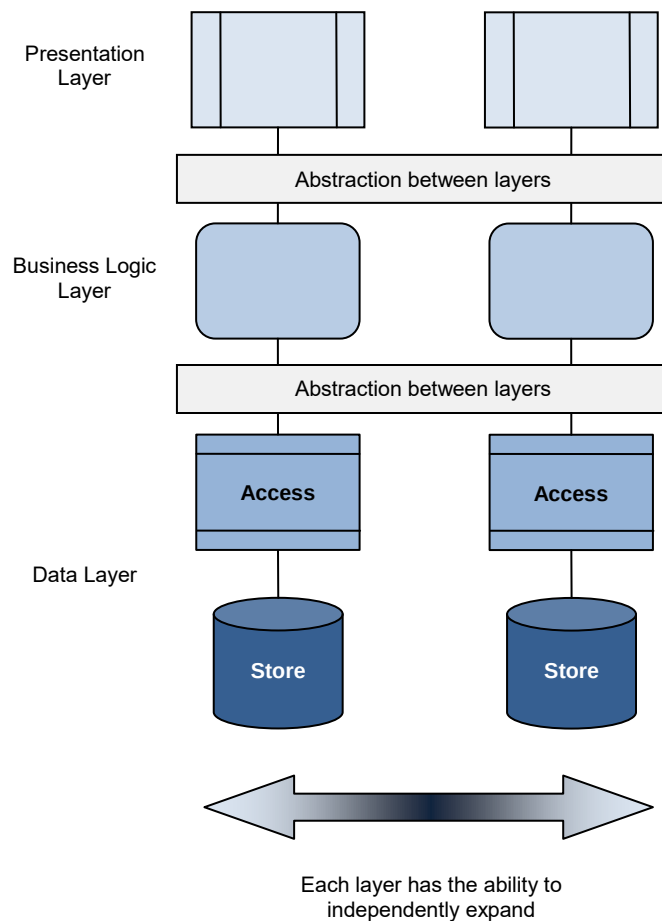


Figure C-3
Class A3 and A4 Application Architecture

C.2.5 Data Center Systems Architecture Summary

It is uncommon for an enterprise data center to have all applications align within the performance requirements of a single reliability class. Each application is developed according to its own requirements and functionality specifications. However, if the business has identified a baseline performance requirement that meets the overall organization's objectives, the associated reliability class should either be the minimum objective or lower level data center service layers should provide higher than identified reliability to compensate, including disaster recovery/business continuity capabilities.

C.3 Data Processing and Storage Systems Reliability

The data processing and storage systems layer has historically been directly dependent on the higher application architecture layer. However, with the development of virtualization and cloud computing, the data processing and storage services layer can be abstracted from the higher application architecture services layer.

Historically, appliance server applications relying on direct attached storage was the predominant low-cost data storage technology solution. The development of network attached and scalable enterprise cross platform storage systems from various manufacturers have also provided a cost effective alternative to the traditional "big iron" enterprise storage systems. Virtualization has also had a significant impact on the data storage system industry, providing intelligent data management, including automated layer management based on defined performance requirements and retention policies.

Current application architecture, data processing, and storage systems not only provide autonomy between the application and the associated data processing hardware, but also provide autonomy between the data processing hardware and the data storage systems.

The data processing and storage systems consist of:

- Processing: The processing systems range from application-specific appliance servers to virtualized, high performance or grid computing hardware solutions.
- Storage: The storage systems range from platform specific direct attached disks to enterprise platform independent networked storage systems.

For the performance characteristics, the data processing and storage systems are prefaced with an "S" to identify how it aligns with the reliability Class criteria.

C.3.1 Data Center Systems Availability Classes

The following system architecture examples merely represent one example of many system engineering solutions.

C.3.2 Availability Class S0 and S1

Systems are implemented on specific platforms and are hardware dependent with no seamless failover or self-healing capabilities.

Table C-4 Tactics for Class S0 and S1

Processing Systems:	Application specific hardware dependent processing
Storage Systems:	Platform dependent direct attached storage

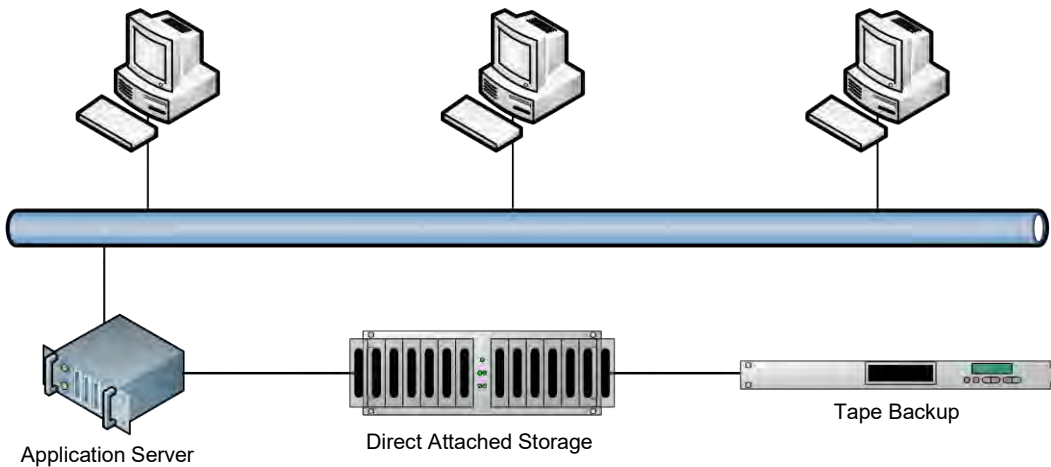


Figure C-4
Class S0 and S1 Systems Architecture

C.3.3 Availability Class S2

Systems are implemented on specific platforms and are hardware dependent with failover capabilities. System failure recovery performed through application and data storage failover to redundant systems.

Table C-5 Tactics for Class S2

Processing Systems:	Application-specific hardware dependent processing with mirrored application on redundant hardware
Storage Systems:	Platform dependent network attached storage with mirrored data on redundant network attached storage system

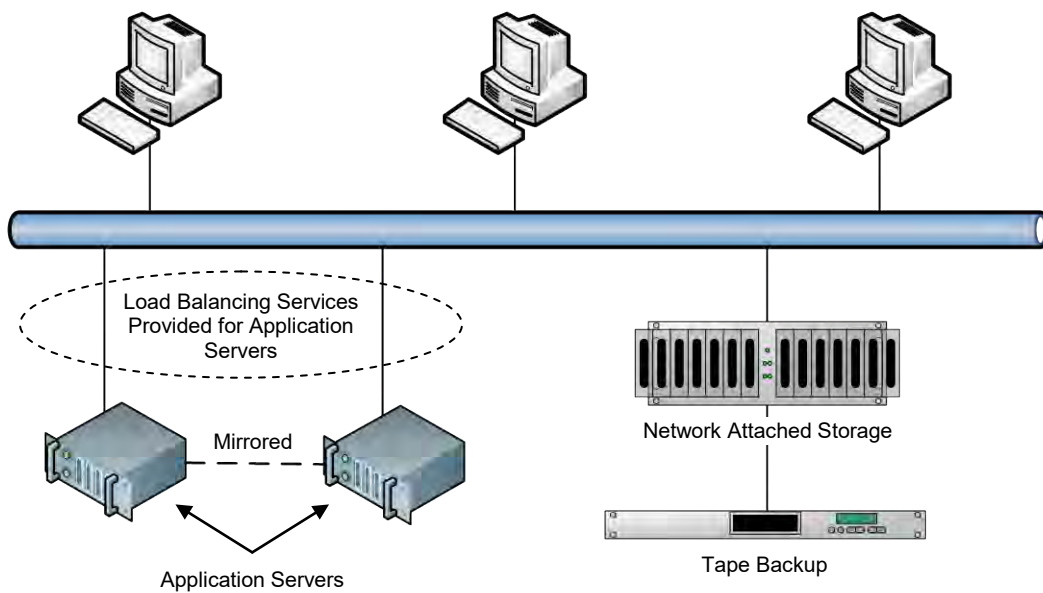


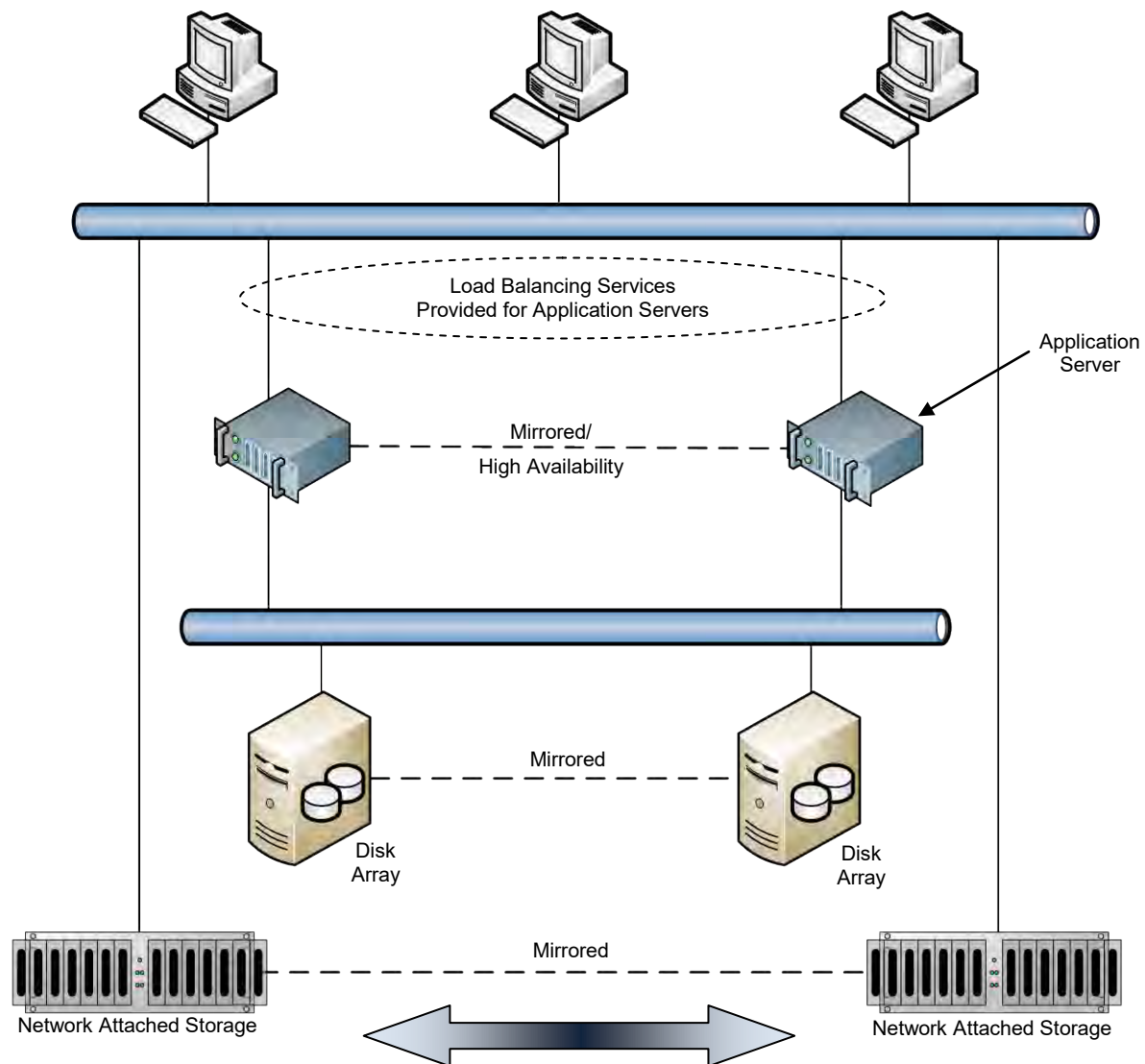
Figure C-5
Class S2 Systems Architecture

C.3.4 Availability Class S3

Processing systems are implemented on specific platforms and are hardware dependent with failover capabilities or on virtualized processing space with location transparency. Storage systems, whether network attached or enterprise cross platform storage systems, are provided with failover capabilities.

Table C-6 Tactics for Class S3

Processing Systems:	Application specific hardware dependent or virtualized processing space with mirrored application on redundant hardware
Storage Systems:	Network attached or enterprise cross-platform storage with mirrored data on redundant storage systems



Mirrored or high-availability systems require that lower level service layers (e.g., network, cabling infrastructure, facilities) supporting redundant processing or storage systems do not have any common mode failures that would impact the systems service layer.

Figure C-6
Class S3 Systems Architecture

C.3.5 Availability Class S4

Systems are provided with system and component redundancy to provide seamless failover in the event of component or chassis failure. No common mode failures exist between processing and storage systems.

Table C-7 Tactics for Class S4

Processing Systems:	Location transparent, virtualized systems or hardware dependent grid computing, processing systems independent from storage systems
Storage Systems:	Network attached or enterprise cross-platform storage with mirrored data on redundant storage systems, automated data management among and between storage layers

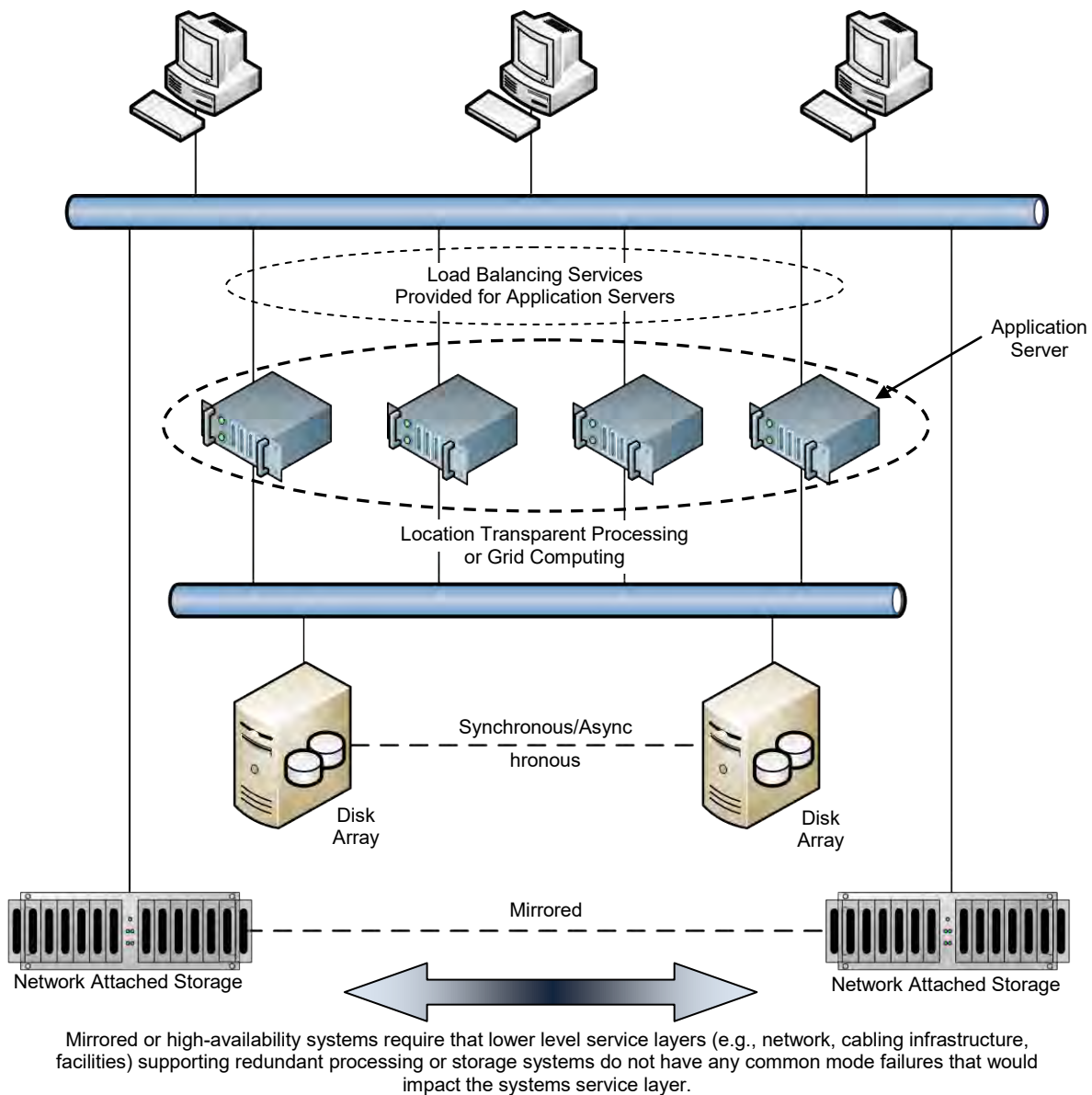


Figure C-7
Class S4 Systems Architecture

This page intentionally left blank

Appendix D Data Center Services Outsourcing Models (Informative)

This appendix is not part of the requirements of this standard, but it is included to provide additional information related to this standard.

D.1 Data Center Services Outsourcing Models

There are various data center outsourcing models that are available to organizations that desire to procure the data center services layer as a service from external vendors. The outsourcing models include:

- Managed services
- Colocation
- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)

Cloud services is not defined as an outsourcing model, but rather, as a method of dynamically delivering outsourced services enabling rapid scaling of capacity up or down as the business requirements change. This dynamic capability can be implemented within a private cloud, public cloud, or private-public hybrid cloud architecture. Public cloud services can be provided by any of the XaaS outsourcing models.

D.1.1 Managed Services Model

The managed services model is used when the business has an existing data center with sufficient redundancy, capacity, and security to meet the business and IT objectives. For various reasons, the business may not want to maintain the staff required to operate the data center. The business contracts with an external vendor to operate the facility and possibly the hardware. The facility and hardware are owned and controlled by the business.

The value of managed services is that businesses can reduce or eliminate staff resources that are required to support the data center infrastructure.

D.1.2 Colocation Services Model

The colocation model consists of the business leasing computer room capacity from an external data center vendor. The external vendor provides physical security, floor space, power, cooling, and the ability to connect to one or more network service providers. The business owns and manages all IT hardware, applications, and OS/middleware.

D.1.3 Infrastructure as a Services (IaaS) Model

The IaaS model consists of the business owning and managing the applications and OS/middleware. The external vendor owns and manages the data center facility and hardware.

D.1.4 Platform as a Services (PaaS) Model

The PaaS model consists of the business owning and managing the applications. The external vendor owns and manages the data center facility, hardware, and OS/middleware.

D.1.5 Software as a Services (SaaS) Model

The SaaS model, also known as “full-service hosting,” consists of the vendor owning the entire infrastructure stack: the facility, hardware, applications, and OS/middleware.

D.2 Data Center Services Outsourcing Model Comparison

The amount of control that the business has over the infrastructure, applications, and data is reduced as the model moves from the internal IT model to the SaaS model. It is very common for IaaS, PaaS, and SaaS outsourcing vendors to use a colocation vendor to own and manage the data center facility. Also, the PaaS and SaaS outsourcing vendors may use an IaaS vendor to own and manage the hardware. This is an important consideration when conducting due diligence on outsourcing vendors as the total infrastructure, application and data stack may consist of one or two vendor relationships behind the outsourcing vendor the end user is negotiating with. Understanding the entire stack is critical to ensuring the outsourcing solution will be able to meet the objectives of the business and the commitments that IT is making to the user community.

System Model	Facilities	Hardware	OS/Middleware	Applications
Internal IT (Not Outsourced)	Business	Business	Business	Business
Managed Services	Business (Own)	Business (Own)	Business	Business
	Vendor (Operate)	Vendor (Operate)		
Colocation	Vendor	Business	Business	Business
Infrastructure as a service (IaaS)	Vendor	Vendor	Business	Business
Platform as a service (PaaS)	Vendor	Vendor	Vendor	Business
Software as a service (SaaS)	Vendor	Vendor	Vendor	Vendor

Public Cloud Services:
Vendors that provide XaaS services to the business in a manner that enable the services to be dynamically provisioned allowing the business to rapidly scale capacity up or down as the requirements change

IaaS/PaaS/SaaS vendor may outsource facilities ownership/management to collocation vendor

PaaS/SaaS vendor may outsource facilities and hardware ownership/management to collocation or IaaS vendor

Figure D-1
Outsourcing Model Matrix

Note that cloud services is not an outsourcing model; rather, it is a method of dynamically delivering outsourced services enabling rapid scaling of capacity up or down as the business requirements change. Public cloud services can be provided by any of the XaaS outsourcing models. One method of taking advantage of public cloud services is to augment internal IT services (private cloud) with public cloud services from a XaaS vendor during periods of peak demands on IT services to meet either processing, storage, or bandwidth capacity. In this case it is required that the internal network infrastructure and application architecture be developed as a private cloud in order to seamlessly integrate with the Public Cloud services offered by the XaaS vendors.

D.3 Public Cloud Services

Public cloud service vendors provide all the data center service layers for the applications they support for the customer. As previously mentioned, a public cloud service vendor may own and manage all data center services layers for their customers, or they may own and manage the application layer and outsource all lower level services layers to other vendors.

Due diligence is required by those considering public cloud services to ensure that the data center services and the public cloud model offered by the vendor provide the level of redundancy and diversity required based on the customer's objectives.

There are generally four levels of redundancy available for the implementation of public cloud services. Each of the levels identified below represent different common modes of failure that may result in outages to the customer.

D.3.1 Virtual Redundancy Level

The virtual redundancy level consists of a public cloud service vendor that provides virtual redundancy within a single physical data center. All shared physical resources represent potential single points or common modes of failure to the customer. It would be critical to validate the level of redundancy provided by all the lower layer data center services if the customer is purchasing cloud services based solely on virtual redundancy to ensure that the overall reliability objectives can be achieved by the sole cloud services vendor.

D.3.2 Redundant Availability Zone Level

The redundant availability zone level consists of a public cloud service vendor that provides redundant availability zones across multiple physical data centers within a common region. All physical resources within each data center do not represent potential single points or common modes of failure to the customer. All external risks, both natural and man-made, that the data centers are exposed to may represent potential common modes of failure to the customer. It would be critical to validate the level of redundancy provided by all the lower layer data center services and the risk of all common modes of failure between the two data centers if the customer is purchasing cloud services based solely on redundant availability zones to ensure that the overall reliability objectives can be achieved by the sole cloud services vendor.

D.3.3 Redundant Cloud Region Level

The redundant cloud region level consists of a public cloud service vendor that has at least two data centers located in separate diverse regions. There are no common modes of failure with any of the data centers internal physical resources or external natural and man-made risks. The customer has the ability to move data center services between the diverse data centers as required. If the reliability of the lower layer data center services cannot be validated, it would be prudent to assume the redundant cloud region level provided by a single cloud services vendor would achieve Class 3 reliability requirements if distributed across two or more physically diverse data centers. As the vendor distributes its redundant cloud region cloud services across more (greater than three) data centers, each located within physically diverse regions, the lower level layers become less significant in ensuring that the cloud services will provide the users access to the applications and data without disruption.

D.3.4 Redundant Cloud Provider Level

The redundant cloud provider level consists of multiple public cloud service vendors, located in separate regions, providing the ability of the customer to move their data center services between providers as required. All physical resources within each vendor's data center do not represent potential single points or common modes of failure to the customer. All external risks, both natural and man-made, that the data centers are exposed to do not represent potential common modes of failure to the customer. The redundant cloud provider model also eliminates the risk of the complete loss of a cloud provider because of external business events or business failure.

D.4 Outsourcing Model Decision Tree

The decision tree shown in Figure D-2 helps guide discussions on the suitability of outsourcing options on an application-by-application basis. It is not intended to identify the specific option that is best suited for the business, but it is primarily intended to identify options for each specific application that are not suited for the business. Once the options that are not suitable have been identified, each of the available options can be evaluated against cost, operational, functional, and security criteria.

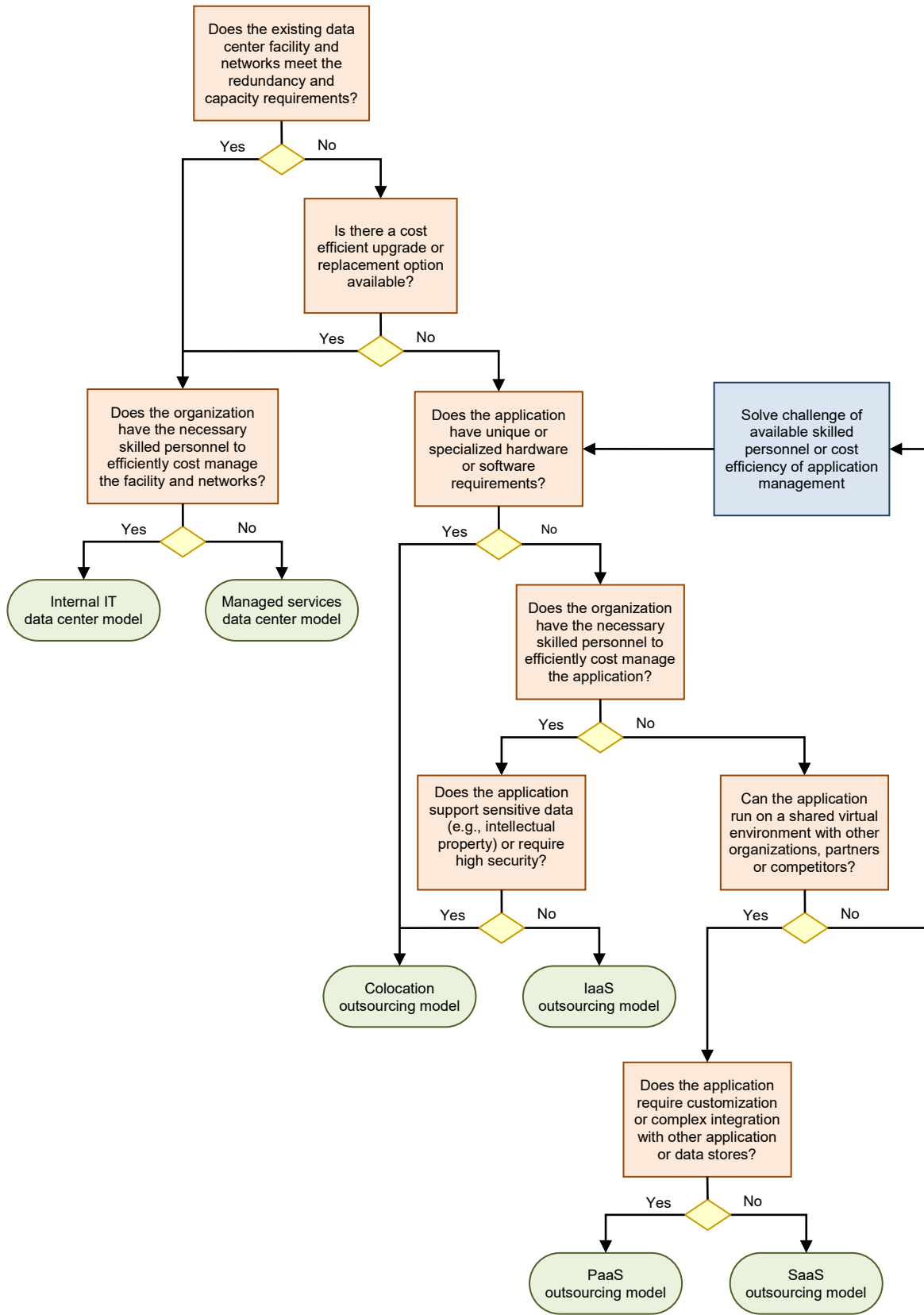


Figure D-2
Outsourcing Decision Tree

Appendix E Multi-Data Center Architecture (Informative)

This appendix is not part of the requirements of this standard, but it is included to provide additional information related to this standard.

E.1 Overview

Prior to virtualization, location transparent applications and cloud services, the optimal data center services configuration consisted of an alignment of the reliability classes across all the data center service layers. This provided the minimum required level of reliability and redundancy without over building any one of the data center service layers. However, it is unlikely that a single data center would have all the applications, data processing, and storage platform systems aligned within a single reliability classification no matter what the targeted base data center reliability classification is.

One of the values of the BICSI data center services reliability framework model is it can be used to:

- Identify the minimum reliability targets.
- Provide a structured methodical approach to guide decisions on how to adjust lower layer services to compensate for higher layer services reliability inadequacies.
- Guide discussions regarding the possible technical and cost benefits of increasing the reliability of the network architecture and higher layers above the targeted reliability class across multiple data centers so that cost savings can be realized by building each of the data centers facilities to a lower Class than the targeted reliability classification.

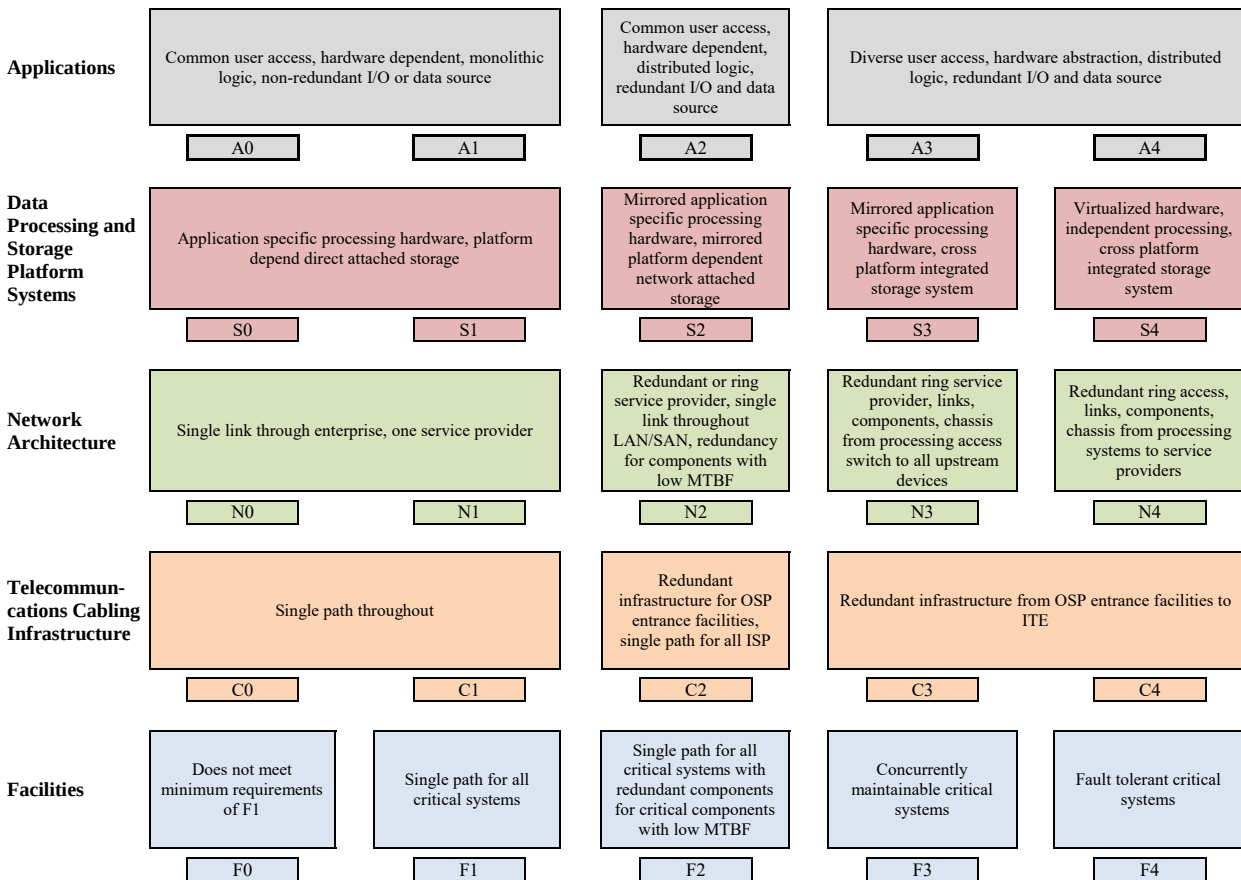


Figure E-1
Reliability Framework Across All Service Layers

E.2 High Availability In-House Multi-Data Center Architecture Example

In this example, a customer has identified Class 3 as the targeted data center services reliability level. The customer has multiple facilities that can support critical data center functions. By provisioning the applications with high-availability configuration across two data center facilities, the customer will be able to achieve the targeted reliability and availability objectives.

It is important that any man-made or natural event common mode risks that may exist within the geographical region that is common between the two data centers be identified and evaluated. The communications between the two data centers can be synchronous or asynchronous, depending on the recovery point objective (RPO) and recovery time objective (RTO) of the disaster recovery/business continuity requirements and the physical distance limitations between the two data centers.

There are times when there are man-made or natural event common mode risks to both data centers that have been deemed an acceptable risk to the organization. An example would be multi-regional events, such as multi-State power outages, that an organization deems acceptable. There would be no loss of data within the data center (running on backup power sources); however, the users would not have access to the applications or data as their networks and systems would be off-line throughout the multi-state region. The organization might determine that the users would not have an expectation of accessing the data in this scenario, and there would be no loss of revenue or business reputation as a result. Therefore, the costs associated with building out multiple data centers across a wider geographical area (possibly outside synchronous communication capabilities) may not be justified.

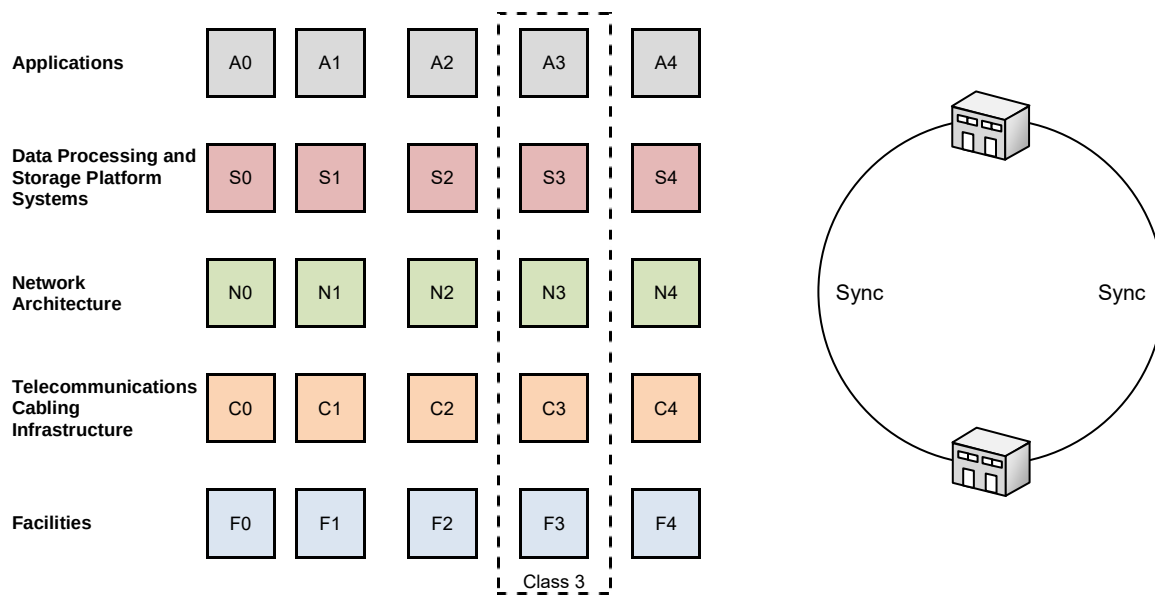


Figure E-2
Multi-Data Center Class 3 Example

E.3 Private Cloud Multi-Data Center Architecture Examples

Private cloud services are implemented in customer-owned data centers. Private cloud applications are developed to improve scalability, speed of deployment, and reliability with the abstraction on the reliance on the lower layer data center services. Private cloud applications may enable the customer to implement highly reliable applications without requiring highly reliable lower layer data center services.

E.3.1 Private Cloud Multi-Data Center Architecture – Class 3 Solution/Three Class 2 Facilities

The first example is a customer that has identified at least two Class 3 data centers as the targeted data center services reliability level. The private cloud applications would be implemented across diverse geographical regions. By provisioning the private cloud applications across three Class 2 data center facilities, the customer may be able to achieve similar reliability and availability objectives. The applications can move around each of the data center facilities with the loss of any one facility having little or no impact on the enterprise.

The two data centers connected via synchronous communications would be located within a common region. The data center that is connected via asynchronous communications would be located outside the region, ensuring no natural or man-made event represents a common mode of failure.

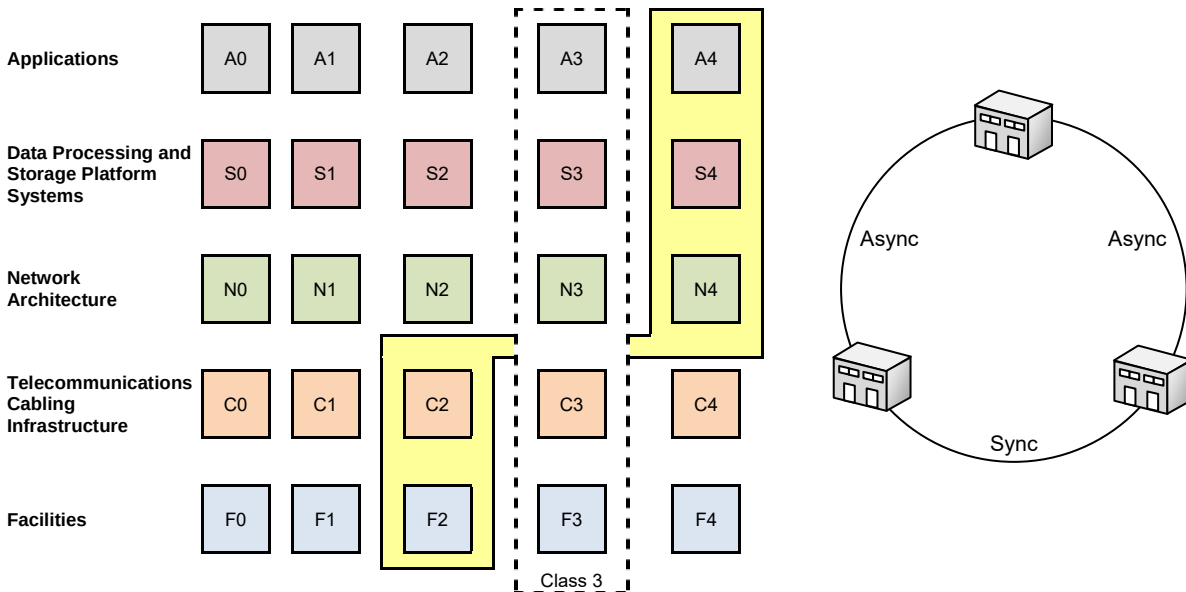


Figure E-3
Multi-Data Center Class 3 Example With Three Class 2 Facilities

This example is not provided as a solution that will always equate to two Class 3 data centers; rather, it is provided to show how the data center services reliability framework can be used to evaluate various options.

E.3.2 Private Cloud Multi-Data Center Architecture – Class 4 Solution/Four Class 2 Facilities

The second example is a customer that has identified two Class 4 data centers as the targeted data center services reliability level. By provisioning the private cloud applications across four Class 2 data center facilities, both within a common region and outside common regions, the customer may be able to achieve similar reliability and availability objectives. The applications can move around each of the data center facilities with the loss of any one facility or facilities within a region having little or no impact on the enterprise.

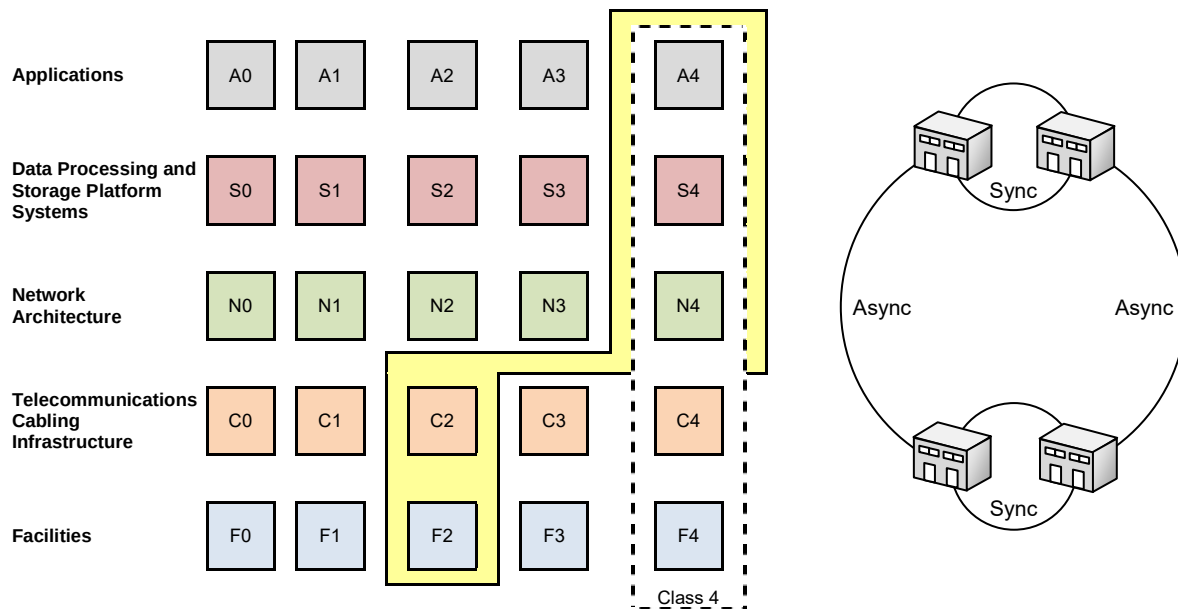


Figure E-4
Multi-Data Center Class 4 Example with Four Class 2 Facilities

Two of the data centers are connected via synchronous communications located within a common region. The pair of data centers located within each common region are connected via asynchronous communications. The pair of data centers would be located outside each other's region, ensuring no natural or man-made event represents a common mode of failure.

This example is not provided as a solution that will always equate to two Class 4 data centers, but it is provided to show how the data center services reliability framework can be used to evaluate various options.

Appendix F Examples of Testing Documentation (Informative)

This appendix is not part of the requirements of this standard, but it is included to provide additional information related to this standard.

F.1 Introduction

This appendix provides examples of two different tests that may be performed during commissioning. Section F.2 provides an example of PDU testing and Section F.3 provides an example of UPS and diesel generator testing.

F.2 Example of PDU Testing

F.2.1 Purpose

To establish steps necessary to finish commissioning the PDUs and perform the Integrated Systems Test in customer room #1 while minimizing potential impact to critical customer equipment.

F.2.2 Introduction

- Connect temporary power jumper from M1BB tiebreaker to 1HUPSDP2
- Shift critical load to UPS 2B at the ASTS PDU level.
- Transfer UPS system 1A to internal bypass from UPS mode
- Energize A side PDUs in customer room #1
- Transfer UPS system 1A from internal bypass to UPS mode
- Power up the B side of customer room #1 PDU/ASTSs using temporary power
- Perform ASTS Commissioning Procedure on STS 3B
- Leave A side PDUs in customer room #1 on the 1A UPS
- Shift critical load in Customer Room #3 and Network to UPS 1A at the ASTS PDU level
- Transfer UPS system 2B to internal bypass from UPS mode
- Energize B side PDUs in customer room #1
- Transfer UPS system 2B from internal bypass to UPS mode
- Restore power to normal power paths

F.2.3 Systems Impacted

The following systems may be impacted by this procedure: UPS system 1A, UPS system 2B and all STS PDUs.

F.2.4 Backout Plan

If a problem occurs with a PDU or STS during testing, it will be isolated from the system until it is repaired.

ID	Time mark	Duration	Task	Resource	Control
			Run temporary power jumpers from M1BB tie breaker to panel 1HUPSDP 2, 4, 6		
		N/A	Site check-in		
			Enable contractor badges for access to proper work areas.		
			Notify monitoring company of impending work. Disable ALC page out function.		
		30 min	Project meeting – introductions, review of project, safety, and tool inventory		
1			At the MSDA, select source 1 (UPS 1A) as the Master Source.		

<i>ID</i>	<i>Time mark</i>	<i>Duration</i>	<i>Task</i>	<i>Resource</i>	<i>Control</i>
2			Record the load on UPS System 1A at the SCC control panel: kVA _____ kW _____ Phase A amps _____ Phase B amps _____ Phase C amps _____		
3			Record the load on UPS System 2B at the SCC control panel: kVA _____ kW _____ Phase A Amps _____ Phase B Amps _____ Phase C Amps _____		
4			Verify that all STS's are programmed with UPS 2B as Preferred source. If the STS is programmed with UPS 1A as the preferred source, transfer to UPS 2B as the preferred source using the following procedure: 3STS1A Time _____ 3STS2A Time _____ 3STS3A Time _____ 3STS4A Time _____ 3STS5A Time _____ 3STS6A Time _____		

<i>ID</i>	<i>Time mark</i>	<i>Duration</i>	<i>Task</i>	<i>Resource</i>	<i>Control</i>
4c			3STS7A Time _____ 3STS8A Time _____ 3STS9A Time _____ STSNETA Time _____ 1) At the STS, select Monitor Mimic screen and verify that no alarms are present. 2) Select Source Transfer screen and verify: a. Source 2 voltage available b. ON Source 1 c. Source 1 Preferred d. OK to transfer e. synchronization within 15°. 3) Simultaneously press Alarm Reset and Down buttons. 4) Verify transfer by checking ON Source Message : a. ON Source 2 b. Source 2 Preferred.		
5			Verify load increase on UPS 2B. It should be approximately the same as recorded in step 1.		
6			Verify that UPS 1A and UPS 2B are operating normally and that transfer to bypass is not inhibited.		
7			1) Transfer UPS 1A from UPS mode to Internal Bypass by: a. Verifying at UPS User Interface Panel: b. OK to transfer c. Static Switch connected d. no alarms present. 2) Review Load Transfer Procedures on the UPS User Interface Panel. 3) Using the Push to Turn Voltage Adjust Pot , set UPS output voltage 2 to 4 V above bypass voltage. 4) Verify UPS leads by 1° to 3° (Synchronization graphic is in upper right corner of display).		
7c			1) If OK to Transfer is highlighted, simultaneously press Control/Enable and Bypass buttons. 2) Press Horn Off to silence alarm. 3) At the UPS SCC Monitor Mimic verify: a. System Bypass Breaker closed b. UPS Output Breaker open.		

ID	Time mark	Duration	Task	Resource	Control
8			Energize A PDUs on normal UPS Source: 1) In CR1 at Panel 1HUPSDP 1, 3, 5 open and lock out breaker being fed by temporary power from M1BB. 2) At UPS 1A SCC distribution in room XXX, close Feeder to 1HUPSDP 1, 3, 5 3) In CR1 at Panel 1HUPSDP 1, 3, 5 close Breaker Main – DP (Fed From UPS1A) 4) Close the Main Input breaker then the Subfeed 1 and Subfeed 2 breakers at: a. 1PDU1A b. 1PDU2A c. 1PDU3A d. 1PDU4A		
9			Transfer UPS 1A from internal bypass to UPS mode by: 1) Verify at UPS SCC Monitor Mimic Panel. a. UPS on Internal Bypass b. UPS Modules are on line 2) Review Load Transfer Procedures on the UPS User Interface Panel. 3) Using the Push to Turn Voltage Adjust Pot, set UPS output voltage 2 to 4 V above bypass voltage. 4) Verify UPS leads by 1° to 3° (Synchronization graphic is in upper right corner of display). 5) If OK to Transfer is highlighted, simultaneously press Control/Enable and UPS buttons.		
9c			1) At the UPS SCC Monitor Mimic verify: a. System Bypass Breaker open b. UPS Output Breaker closed 2) Reset the UPS system output voltage to 488 V.		
10			Verify that UPS 1A and UPS 2B are operating normally and that transfer to bypass is not inhibited.		
11			In customer room #1 open and lock out feed from UPS 2B to panel 1HUPSDP2, 4, 6.		
12			Close tie breaker in M1BB		
13			In customer room #1: 1) Close breaker 1HUPSDP2, 4, 6 2) Close tie breakers among 1HUPSDP2, 1HUPSDP4, and 1HUPSDP6 3) Energize B side PDUs		
15			Perform ASTS Commissioning Procedure on STS 3B: 1) Ensure that the ASTS is in normal operating mode, and that no alarms are present. NOTE: During the performance of the tests, verify proper normal and alarm indications are present. Verify remote alarm indications.		

<i>ID</i>	<i>Time mark</i>	<i>Duration</i>	<i>Task</i>	<i>Resource</i>	<i>Control</i>
15c			1) Apply 100% load to the output of the ASTS. 2) Perform calibration checks for source 1 and record in the appropriate table. 3) Infrared scan the source 1 side and output of the ASTS after 100% load has been applied for at least one hour. Infrared scan the source 1 PDU. 4) Perform a maintenance isolation to source 1 maintenance bypass. 5) Infrared scan the source 1 maintenance bypass of the ASTS after 100% load has been applied for at least one hour. 6) Perform a restoration to normal operation. 7) Perform a manual transfer to source 2. 8) Perform calibration checks for source 2 and record in the appropriate table. 9) Infrared scan the source 2 side and output of the ASTS after 100% load has been applied for at least one hour. Infrared scan the source 2 PDU. 10) Perform a maintenance isolation to source 2 maintenance bypass. 11) Infrared scan the source 2 maintenance bypass of the ASTS after 100% load has been applied for at least one hour. 12) Infrared scan the output breaker distribution section. 13) Perform a restoration to normal operations. 14) Perform a manual transfer to source 1.		

F.3 Example of UPS and Diesel Generator Testing

NOTES:

1. Checkboxes (☒) have been incorporated into the following procedure to ensure full compliance to all steps contained herein.
2. Other types of backup power can be used; this example test plan uses a diesel generator.

F.3.1 Purpose

- To demonstrate that the new UPS module and diesel generator associated with the data center client facility will function in accordance with the manufacturer's specifications
- To ensure that these new critical power components will function accordingly in their parallel configuration

F.3.2 Scope

Testing to be performed as part of this procedure will be done as follows:

- 1) UPS 4 (600 kW required):
 - Input and output THD measurements
 - Voltage regulation measurements
 - Step load transient response
 - Bypass transfer transient tests
 - Transfer to battery transient response
 - Rectifier ramp in measurement.
- 2) Parallel UPS (1800 kW required):
 - Voltage regulation measurements
 - Module output load sharing measurements
 - Step load transient response
 - Bypass transfer transient tests
 - Module fault off and restore transient response.
- 3) DG 3 (2000 kW required):
 - 4 hour burn in
 - Output THD measurements
 - Voltage regulation measurements
 - Step load transient response
 - 100 % block load transient response
- 4) Parallel DG system (2000 kW required):
 - Load sharing measurements
 - Voltage regulation measurements
 - DG fault off and restore transient response.

F.3.3 Vendor's Responsibility

The technicians from each vendor have the responsibility of operating their equipment, and guiding all attending personnel through this procedure.

Vendors are also responsible to provide copies of all startup paperwork, and all equipment specifications for review and inclusion into the final commissioning report.

A copy of all vendor paperwork must be available at the beginning of the commissioning to ensure that applicable equipment startup checks have been performed.

F.3.4 General Contractor's Responsibility

They are responsible for ensuring that the following are available as needed during the performance of this procedure:

- ☐ Technician(s) from the UPS vendor
- ☐ Technician(s) from the diesel engine vendor
- ☐ A minimum of two site familiar electricians to assist as necessary in the performance of this test procedure (e.g., to operate electrical distribution breakers, and or assist with load banks as needed); Additional electricians may be required in the event that the commissioning process will otherwise be delayed.

- ☐ An infrared camera and operator (must be an infrared camera with the ability to take sample thermograms to establish a baseline recording of all major electrical equipment)
- ☐ To provide the necessary air-cooled load banks and cables (please be sure that the cables provided are sufficient in length and ampacity for the amount of load); load bank positioning should be determined before cables are ordered; resistive load equal to the full load rating of each system to be tested shall be available.
 - 1) For UPS module load testing, the load banks should be connected directly to the output switchgear of each UPS module (this will require 480V load banks with external fan power capability):
 - 2) For UPS module testing 1200 kW required. The external fan power for the load banks must be connected to a source, which will not be interrupted during the commissioning process.
 - 3) For diesel generator testing, the load banks should be connected directly to the output of the paralleling cabinet. (This will require 480V load banks with external fan power capability).
 - For diesel generator testing, a minimum of twelve, ideal of twenty-four 200 kW resistive load bank must be available.
 - The necessary diesel fuel oil.
- ☐ To ensure that all parties are aware of their individual responsibilities as they pertain to this procedure
- ☐ To ensure that all testing prerequisites are met before the commencement of the commissioning procedure (this includes the load bank hookup and placement for each day of commissioning)
- ☐ To inform all applicable subcontractors that there will be no other work permitted in the spaces where commissioning is being performed. Failure to adhere to this requirement can result in personnel injury and equipment damage.

F.3.5 Testing Agent's Responsibility

The testing agent shall provide the necessary engineering personnel to complete the proposed testing, and will furnish the following test equipment or its equivalent:

- 2 each power analysis recorder (power meter)
- 1 each chart recorder
- 2 each digital multimeters
- 1 each 600A clamp on current probe for multimeter

F.3.6 Requirements

- The diesel generator system shall be commissioned in accordance with the manufacturers recommendations, and shall be ready to perform to all specifications that pertain to it.
- Each diesel generator (single unit) shall be capable of accepting a 100% block load, and fully recovering (voltage and frequency) within 15 seconds.
- The diesel generator switchgear shall be commissioned in accordance with the manufacturers recommendations, and shall be ready to perform to all specifications that pertain to it.
- The diesel generators shall be capable of paralleling, and load sharing to within 5% of each other from 25% to 100% system load.
- The UPS system shall be commissioned in accordance with the manufacturers recommendations, and shall be ready to perform to all specifications that pertain to this equipment.
- Resistive load equal to the full load rating of each system to be tested shall be available.
- During the performance of this procedure, no other work will be permitted in the spaces in which equipment is being tested (e.g., while UPS module testing is being performed, no other work will be permitted in the UPS room, or in the area through which load bank cables are run). No other work will be permitted on equipment feeding the equipment, directly or indirectly controlling power to devices being commissioned.

Note that this precaution must be adhered to since the proposed work will require testing on exposed and energized electrical equipment – other work in the area jeopardizes the safety of the testing engineers, and the individuals doing the work.

F.3.7 Emergency Generator System Testing

The purpose of this test is to record the operating parameters and compare them to the manufactures specifications. The results of this testing will also be used as a baseline for future testing.

Note that if at any time during the diesel generator testing should a call for emergency occur from any ATS the load bank shall be turned off, the load bank breaker shall be opened and the DG system returned to automatic operation.

F.3.7.1 Diesel Generator

F.3.7.1.1 Diesel Heat Run

This step shall be performed by the diesel vendor and paperwork should be presented to the testing agent's engineer:

- ☐ Place this diesel generator on line and load to 2000 kW
- ☐ Heat run at full load for four (4) hours
- ☐ Take readings of voltage, current, frequency, revolutions per minute and all engine data available from the DG display panel (e.g., exhaust temperature, battery voltage, oil pressure, coolant temperature) every 15 minutes. Take a note of any revolutions per minute instability.

F.3.7.1.2 Infrared Scan

- ☐ Infrared scan the engines once full load has been applied for a minimum of 1 hour.
- ☐ Infrared scan each cylinder head. Values shall be at the same aim point for each head and within 2.5 °C (4.5 °F) of each other.
- ☐ Infrared scan the four turbos and ensure uniform temperatures for all four.
- ☐ Conduct an infrared scan of all power terminal connections, circuit breakers, between the generator and load bank, and record temperature following a minimum of 15 minutes operation at 100% load. Terminal temperature shall not exceed 75 °C (167 °F) Maximum.
- ☐ Conduct an infrared scan of the generator bearing housing and record the generator bearing housing temperature. Bearing housing temperature shall not exceed 50 °C (122 °F) maximum.
- ☐ Repeat the steps in this section after 3 hours of full load operation for each diesel generator being tested. Any abnormalities should be brought to the engineer's attention.

F.3.7.1.3 Steady State Tests

- ☐ Start the engine. Apply 100% rated kW load. Take a snapshot of output voltage, current, frequency and harmonic content with the power meter at 100% load. Record data from the power meter and engine generator panel on the attached data sheet.
- ☐ Apply 50% rated kW load. Take a snapshot of output voltage, current, frequency and harmonic content with the powermeter at 50% load. Record data from the powermeter and engine generator panel on the attached data sheet.
- ☐ Remove all of the load. Take a snapshot of output voltage, current, frequency and harmonic content with the powermeter at no load. Record data from the powermeter and engine generator panel on the attached data sheet.

F.3.7.1.4 Transient Response Tests

- ☐ With generator output at no-load (just load bank fans running), apply 50% rated kW load in one step (0 to 50% in one step). Record output voltage, current and frequency with the power meter in **Monitor** mode. Annotate the event recording as "0 to 50% Transient".
- ☐ With generator output loaded to 50%, apply another 50% rated kW load in one step (50% to 100% in one step). Record output voltage, current and frequency with the power meter in **Monitor** mode. Annotate the event recording as "50% to 100% Transient".
- ☐ With generator output loaded to 100%, remove 50% rated kW load in one step (100% to 50% in one step). Record output voltage, current and frequency with the power meter in **Monitor** mode. Annotate the event recording as "100% to 50% Transient".
- ☐ With generator output loaded to 50%, remove all load in one step. Record output voltage, current and frequency with the power meter in **Monitor** mode. Annotate the event recording as "50% to 0% Transient".

F.3.7.1.5 Block Load Test

The purpose of this test is to establish the load that this engine generator combination can accept and recover to rated voltage and frequency within 15 seconds.

With generator output at no-load, apply 100% rated kW load in one step. Make sure that the load does not exceed 100% capacity. For instance, if the generator is rated for 2000 kW, applying 2050 kW will cause the generator to respond out of specification. In this case, lowering the load by 100 kW is still acceptable as 100% block load. Record output voltage, current, and frequency with the power meter in **Monitor** mode. Annotate the event recording as “0% to 100% Transient.”

Note that if the engine is unable to recover to rated voltage and frequency within 15 seconds, reduce the block load amount to 75% and repeat the test. Annotate the testing record accordingly.

F.3.7.2 Diesel Generator Parallel Testing

Note that for parallel diesel generator testing, full system load for these tests is 2000 kW.

F.3.7.2.1 Steady State Tests

- ☐ Place all engine generators on line. Take a snapshot of output voltage, current, frequency and harmonic content with the power meter at no load. Annotate the power meter recording as “0% Load”. Record data from the power meter and engine generator parallel panel meter on the attached data sheet.
- ☐ With no load applied to the parallel system, record output current readings from each engine, on attached Data Sheet, to verify proper load sharing.
- ☐ Apply 50% rated kW load. Take a snapshot of output voltage, current, frequency and harmonic content with the power meter at 50% load. Annotate the power meter recording as “50% Load”. Record data from the power meter and Engine Generator Parallel Panel meter on the attached Data Sheet.
- ☐ With 50% load applied to the parallel system, record output current readings from each engine, on attached Data Sheet, to verify proper load sharing.
- ☐ Apply 100% load to the system. Take a snapshot of output voltage, current, frequency and harmonic content with the power meter at 100% load. Annotate the power meter recording as “100% Load”. Record data from the power meter and Engine Generator Parallel Panel meter on attached Data Sheet.
- ☐ With 100% load applied to the parallel system, record output current readings from each engine, on attached Data Sheet, to verify proper load sharing.

F.3.7.2.2 Transient Response Tests

- ☐ With system output at no-load, (just load bank fans running), apply 50% rated kW load in one step (0 to 50% in one step). Record output voltage, current and frequency with the power meter in **Monitor** mode. Annotate the recording as “0 to 50% Transient”.
- ☐ With system output loaded to 50%, apply another 50% rated kW load in one step (50% to 100% in one step). Record output voltage, current and frequency with the power meter in **Monitor** mode. Annotate the recording as “50% to 100% Transient”.
- ☐ With system output loaded to 100%, remove 50% rated kW load in one step (100% to 50% in one step). Record output voltage, current and frequency with the power meter in **Monitor** mode. Annotate the recording as “100% to 50% Transient”.
- ☐ With system output loaded to 50%, remove all load in one step. Record output voltage, current and frequency with the power meter in **Monitor** mode. Annotate the recording as “50% to 0% Transient”.
- ☐ With system output at no-load, apply 100% rated kW load in one step. Record output voltage, current and frequency with the power meter in **Monitor** mode. Annotate the recording as “0% to 100% Transient.”

F.3.7.2.3 Generator Fault Testing

- ☐ Connect the power recorder to monitor three phase output voltage and current on the diesel generator parallel bus. Setup the power recorder for 15 minute monitoring period. Create the new power recorder **Site Information** directory and annotate it as “DG Fault Offs”. Create new **Location Information** directories for each DG and annotate them accordingly.
- ☐ Place all diesel generators in parallel.
- ☐ Apply 100% load to the system.
- ☐ Link to the power recorder under **Site Information** directory **DG Fault Offs** and **Location Information** directory as “Fault off and Restore DG 1”, and start recording.
- ☐ Open the output breaker for DG 1 to remove it from the bus. Record the transient with the waveform recorder and annotate the graph accordingly.
- ☐ Restore DG 1 to the parallel bus. Record the transient with the waveform recorder and annotate the graph accordingly.
- ☐ Stop the recording and download the data.
- ☐ Link to the power recorder under **Site Information** directory **DG Fault Offs** and **Location Information** directory **Fault off and Restore DG 2**, and start recording.
- ☐ Open the output breaker for DG 2 to remove it from the bus. Record the transient with the waveform recorder and annotate the graph accordingly.
- ☐ Restore DG 2 to the parallel bus. Record the transient with the waveform recorder and annotate the graph accordingly.
- ☐ Stop the recording and download the data.
- ☐ Link to the power recorder under **Site Information** directory **DG Fault Offs** and **Location Information** directory **Fault off and Restore DG 3**, and start recording.
- ☐ Open the output breaker for DG 3 to remove it from the bus. Record the transient with the waveform recorder and annotate the graph accordingly.
- ☐ Restore DG 3 to the parallel bus. Record the transient with the waveform recorder and annotate the graph accordingly.
- ☐ Stop the recording and download the data.

F.3.8 UPS Testing**F.3.8.1 Critical Load Isolation**

- ☐ Start the diesel generators using the test online position on the parallel switchgear.
- ☐ Ensure that the three circuit breakers (UPS-Input SWGR, UPS-Maint. Bypass A, and UPS-Maint. Bypass B) on the DG parallel switchgear are all closed.
- ☐ Transfer Switchboard UPS-Input to emergency.
- ☐ Transfer the UPS system to bypass.
- ☐ Transfer the Maintenance Bypass Switch A to Generator bypass.
- ☐ Transfer the Maintenance Bypass Switch B to Generator bypass.
- ☐ Open the output breakers on the UPS Parallel Switchgear.
- ☐ Shutdown the UPS system and connect the load banks.

F.3.8.2 UPS Module # 1

UPS Data

Make: _____ Model: _____

Serial #: _____ kVA: _____ kW: _____

Battery Data

Make: _____ Model: _____

of Strings: _____ Jars/string: _____ Cells/Jar: _____ Float/Cell: _____

F.3.8.2.1 Steady-State Load Tests

- ☐ Connect the power meter to the input of the UPS module to be tested.
- ☐ Record three phase voltage, current, power, pF, and total harmonic distortion (voltage and current distortion) at the following load levels:
 - 1) 100% load
 - 2) 50% load
 - 3) No load (0% load).
- ☐ Connect the power meter to the output of the UPS module to be tested.
- ☐ Record three phase voltage, current, power, pF, and total harmonic distortion (voltage and current distortion) at the following load levels:
 - 1) 100% load
 - 2) 50% load
 - 3) No load (0% load).
- ☐ While 100% load is applied to the unit record the following on the attached data pages:
 - 1) 3-phase current into the input filter
 - 2) 3-phase current into the output filter
 - 3) 3-phase current into the rectifier(s).

F.3.8.2.2 Transient Load Tests

- ☐ Connect the waveform recorder to the output of the UPS module to measure three phases of output voltage, and one phase of output current.
- ☐ Record the following load step transients with the waveform recorder:
 - 1) 0%–50%–0%
 - 2) 50%–100%–50%
 - 3) 25%–75%–25%.
- ☐ Connect the Waveform recorder to measure three phases of system output voltage.
- ☐ Place the CT on one phase of the system SS bypass and record the following transfer transients with the waveform recorder:
 - 1) Normal transfer to bypass with 100% load applied
 - 2) Module failure to bypass with 100% load applied.
- ☐ Place the CT on one phase of the UPS module's output and record the following transfer transient with the waveform recorder:
 - Transfer from bypass to UPS with 100% load applied.

F.3.8.2.3 Infrared Scan

- ☐ Infrared scan the entire UPS module after 100% load has been applied for a minimum of 15 minutes.
- ☐ Infrared scan the upstream and downstream breakers of the UPS module after 100% load has been applied for a minimum of 15 minutes.

F.3.8.2.4 Battery Discharge Transient Test

- ☐ Verify that the waveform recorder is set to measure three phases of output voltage and one phase of input current.
- ☐ Verify that 100% load is applied to the UPS module.
- ☐ Send the UPS module to battery. Record the following:
 - The initial transfer to battery with the waveform recorder.
- ☐ Restore the UPS input.
 - Record the utility restoration and rectifier ramp with the waveform recorder.

F.3.8.3 Parallel UPS System Testing

Parallel System Control Cabinet Data:

Model #: _____ Serial #: _____

SCC Rating: _____ SCC Breaker Rating: _____ Amps.

F.3.8.3.1 Steady-State Load Tests

- ☐ Connect the power meter to the output of the parallel system cabinet.
- ☐ Apply 100% load to the UPS system.
 - 1) Record three-phase voltage, current, power, pF, and total harmonic distortion (voltage and current distortion) of the system with the power meter.
 - 2) Record system output voltage, system output current, and bypass voltage on the **System Cabinet Load Test Data** table.
 - 3) Record the output current displayed on each individual UPS modules front panel display on the **System Load Sharing Data** table.
- ☐ Apply 50% load to the UPS system.
 - 1) Record three-phase voltage, current, power, pF, and total harmonic distortion (voltage and current distortion) of the system with the power meter.
 - 2) Record system output voltage, system output current, and bypass voltage on the **System Cabinet Load Test Data** table.
 - 3) Record the output current displayed on each individual UPS modules front panel display on the **System Load Sharing Data** table.
- ☐ Remove the entire load from the UPS system.
 - 1) Record three-phase voltage, current, power, pF, and total harmonic distortion (voltage and current distortion) of the system with the power meter.
 - 2) Record system output voltage, system output current, and bypass voltage on the **System Cabinet Load Test Data** table.
 - 3) Record the output current displayed on each individual UPS modules front panel display on the **System Load Sharing Data** table.

F.3.8.3.2 Transient Load Tests

- ☐ Connect the waveform recorder to the output of the parallel system cabinet to measure three phases of output voltage, and one phase of output current.
- ☐ Record the following load step transients with the waveform recorder:
 - 1) 0%–50%–0%
 - 2) 50%–100%–50%
 - 3) 25%–75%–25%.
- ☐ Connect the waveform recorder to measure three phases of output voltage, and one phase of the bypass current.
- ☐ Place four UPS modules on line, apply 100% system level load, and record the following transfer transients with the waveform recorder:
 - 1) Normal transfer to bypass
 - 2) Transfer from bypass to UPS.

F.3.8.3.3 Infrared Scan

- ☐ Place all UPS modules in parallel.
- ☐ Place full system level load on the UPS system.
- ☐ Infrared scan the UPS side of the parallel system cabinet once full load has been applied for a minimum of 15 minutes.
- ☐ Transfer the UPS system to static bypass and increase the load to full static bypass current.
- ☐ Infrared scan the static switch bypass side of the parallel system cabinet once full load has been applied for a minimum of 15 minutes.
- ☐ Transfer the UPS system to maintenance bypass and infrared scan the maintenance bypass side and distribution of the parallel system cabinet once full load has been applied for a minimum of 15 minutes.

F.3.8.4 Parallel UPS Module Fault Testing

- ☐ Connect the waveform recorder to monitor three phases of output voltage on the UPS parallel bus.
- ☐ Place all UPS modules in parallel.
- ☐ Apply 100% load to the system.
- ☐ Place a waveform recorder CT on the output of UPS Module 1, and connect to the waveform recorder.
- ☐ Open the output breaker for UPS 1 to remove it from the bus. Record the transient with the waveform recorder.
- ☐ Restore UPS 1 to the parallel bus. Record the transient with the waveform recorder.
- ☐ Place a waveform recorder CT on the output of UPS Module 2, and connect to the waveform recorder.
- ☐ Open the output breaker for UPS 2 to remove it from the bus. Record the transient with the waveform recorder.
- ☐ Restore UPS 2 to the parallel bus. Record the transient with the waveform recorder.
- ☐ Place a waveform recorder CT on the output of UPS Module 3, and connect to the waveform recorder.
- ☐ Open the output breaker for UPS 3 to remove it from the bus. Record the transient with the waveform recorder.
- ☐ Restore UPS 3 to the parallel bus. Record the transient with the waveform recorder.
- ☐ Place a waveform recorder CT on the output of UPS Module 4, and connect to the waveform recorder.
- ☐ Open the output breaker for UPS 4 to remove it from the bus. Record the transient with the waveform recorder.
- ☐ Restore UPS 4 to the parallel bus. Record the transient with the waveform recorder.

F.3.8.5 Critical Load Restoration

- ☐ Shut down the UPS system and disconnect the load banks.
- ☐ Close the output breakers on the UPS parallel switchgear.
- ☐ Transfer the UPS system to bypass.
- ☐ Transfer the maintenance bypass switch B to UPS.
- ☐ Transfer the maintenance bypass switch A to UPS.
- ☐ Start the UPS system and transfer from bypass to UPS.
- ☐ Transfer switchboard UPS-Input to normal.
- ☐ Shutdown the diesel generators by returning the DG parallel switchgear to **Automatic**.

F.3.9 Data Tables

DIESEL HEAT RUN TEST DATA SHEET UNIT #: _____ DATA COLLECTED BY: _____ TEST DATE: _____ DIESEL MANUFACTURER: _____ RATING: _____ MODEL NO. _____ SERIAL NO. _____																	
Time	0:00	0:15	0:30	0:45	1:00	1:15	1:30	1:45	2:00	2:15	2:30	2:45	3:00	3:15	3:30	3:45	4:00
Exhaust temp left (°F)																	
Exhaust temp right (°F)																	
Battery voltage (V_{DC})																	
Engine revolutions per minute																	
Oil pressure (psi)																	
Fuel pressure (psi)																	
Coolant temp (°F)																	
Phase A-B V_{AC}																	
Phase B-C V_{AC}																	
Phase C-A V_{AC}																	
Phase A current																	
Phase B current																	
Phase C current																	
Frequency (Hz)																	
kW																	

DIESEL GENERATOR TEST DATA SHEET

UNIT NO: _____ TEST DATE: _____
 MANUFACTURER: _____
 GENERATOR MODEL NO: _____ SERIAL NO. _____
 ENGINE _____ SERIAL NO. _____

Engine Data

	<i>No load</i>	<i>50% load</i>	<i>100% load</i>
<i>Exhaust temp left (°F)</i>			
<i>Exhaust temp right (°F)</i>			
<i>Battery voltage (V_{DC})</i>			
<i>Engine revolutions per minute</i>			
<i>Oil pressure (psi)</i>			
<i>Coolant temp (°F)</i>			

Generator Data

	<i>No load</i>		<i>50% load</i>		<i>100% load</i>	
	<i>Panel mtr</i>	<i>Test inst.</i>	<i>Panel mtr</i>	<i>Test inst.</i>	<i>Panel mtr</i>	<i>Test inst.</i>
<i>Phase A–B voltage</i>						
<i>Phase B–C voltage</i>						
<i>Phase C–A voltage</i>						
<i>Phase A current</i>						
<i>Phase B current</i>						
<i>Phase C current</i>						
<i>Frequency (Hz)</i>						
<i>L–L THD (%)</i>						

Paralleling Switchgear, 3 Generators in Parallel

		System output voltage			System output current			System additional readings		
		A - B	B - C	C - A	A	B	C			
No load	Panel meter									
No load	Test instr									
50% load	Panel meter									
50% load	Test instr									
100% load	Panel meter									
100% load	Test instr									

Parallel Load Sharing, All 3 Generators

	GEN 1			GEN 2			GEN 3		
Mtrs:	θA	θB	θC	θA	θB	θC	θA	θB	θC
0% GEN									
0% Swgr									
50% GEN									
50% Swgr									
100% GEN									
100% Swgr									

UPS MODULE # _____

Load Test and Meter Calibration Data

		Input voltage			Input current			Output voltage			Output current		
		A-B	B-C	C-A	A	B	C	A-B	B-C	C-A	A	B	C
0%	Panel meter												
	Test inst												
	THD												
50%	Panel meter												
	Test inst												
	THD												
100%	Panel meter												
	Test inst												
	THD												

Input Harmonic Filter Current Balance

	AØ	BØ	CØ	AØ - N	BØ - N	CØ - N
AMPS						

Output Harmonic Filter Current Balance

	AØ	BØ	CØ	AØ - N	BØ - N	CØ - N
AMPS						

Rectifier Current Balance

	ΔA	ΔB	ΔC	YA	YB	YC
AMPS						

UPS System Cabinet Readings

		System output voltage			System output current			Bypass voltage		
		A-B	B-C	C-A	A	B	C	A-B	B-C	C-A
0%	Panel meter									
	Test instr									
	THD									
50%	Panel meter									
	Test instr									
	THD									
100%	Panel meter									
	Test instr									
	THD									

Parallel Load Sharing, UPS Modules 1, 2, 3, and 4

	UPS 1			UPS 2			UPS 3			UPS 4		
Mtrs:	θA	θB	θC	θA	θB	θC	θA	θB	θC	θA	θB	θC
0% UPS meter												
0% parallel meter												
50% UPS meter												
50% parallel meter												
100% UPS meter												
100% parallel meter												

Attendees

Telecommunications Contractor:

Owner:

General Contractor:

Electricians:

UPS Vendor:

Infrared:

Diesel Vendor:

Diesel Switchgear:

This page intentionally left blank

Appendix G Design for Energy Efficiency (Informative)

This appendix is not part of the requirements of this standard, but it is included to provide additional information related to this standard.

G.1 Introduction

Opinions about where power is being consumed in a data center will vary from one data center to another and is a topic of debate, but there is general consensus within the IT community that more than half of the power is consumed by the infrastructure that supports the ITE. Most calculations estimate that 50-55% of the power goes into supporting infrastructure. Figure G-1 shows where energy can be lost. The Green Grid suggests that as little as 30% of the power might actually go into useful work, depending upon how many infrastructure elements (e.g., chillers, transformers, CRACs, etc.) are present. The amount of power actually used by the ITE could be even smaller if ITE is deployed and utilized effectively. Numerous studies have found that most data centers have lots of stranded capacity with the typical server running at only 20% of its capacity; frequently, legacy servers remain connected even though they are no longer being used.

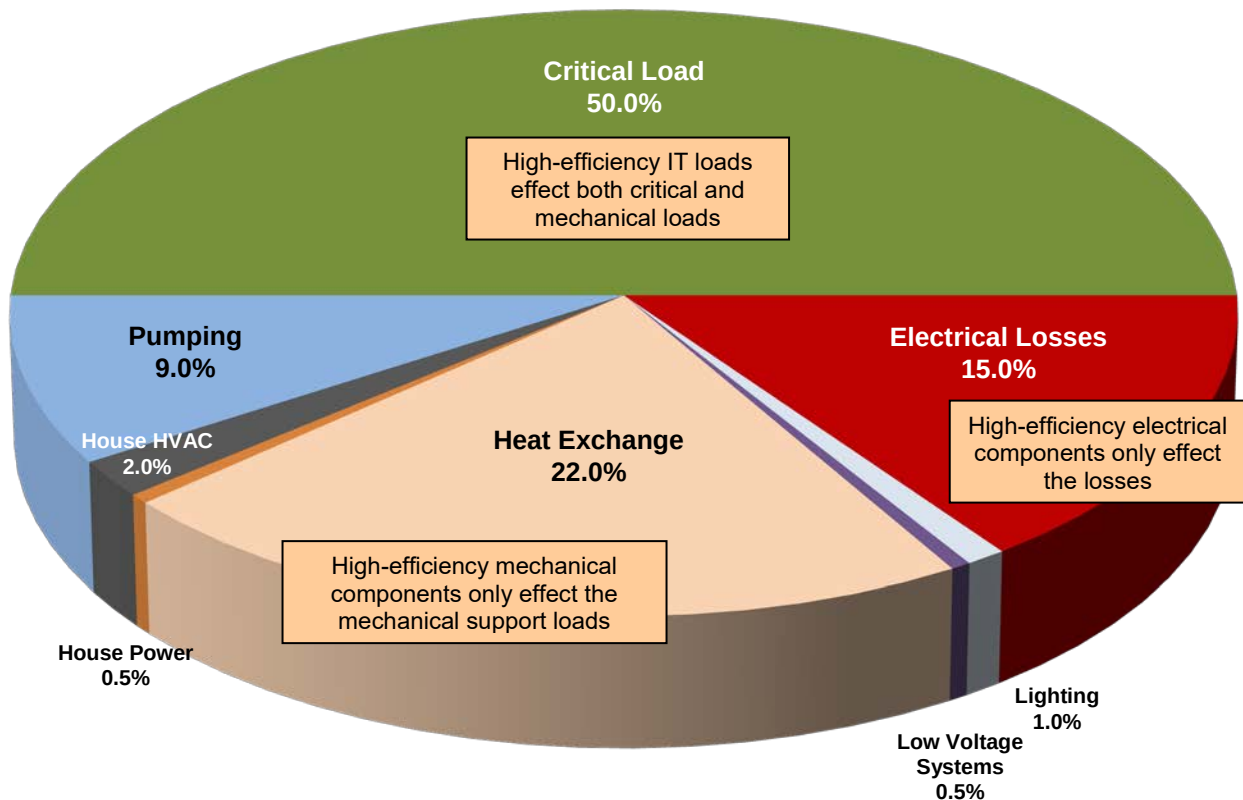


Figure G-1
Data Center Electricity Utilization

Some progress is being made on data center efficiency thanks to higher awareness of the operating costs, better instrumentation, and better metrics such as power utilization effectiveness (PUE). Better software solutions, such as virtualization, are being developed that allow for server consolidation, resulting in higher efficiency and lower total cost of ownership (TCO).

Data center efficiency cannot be managed if it is not accurately measured. Effective measurement relies on the number, location, and accuracy of meters as well as the frequency of measurements. For example, PUE reporting guidelines identify three different sampling levels that factor in where the samples are taken (e.g., UPS, PDU output, or server input), where the facility input power is measured, and how often the measurements are taken (e.g., monthly/weekly, daily, or continuously).

The PUE reporting metric does not factor in the characteristics of the meters themselves. For example, data center switchboard meters are typically “utility grade” with > 99.5% accuracy, whereas meters in rack-mounted power strips frequently have accuracy as low as 96-98%. Because ITE power supplies can create harmonic currents, even when provided with power factor correction filters (e.g., when ITE is operated well below its rated capacity), meters that do not provide true RMS measurements can give misleading data. Higher precision usually means higher capital cost.

G.2 Design for Efficiency

“Design for efficiency” cannot be a separate function. The objective is to create a data center that consumes the least amount of energy possible for any given operation or activity within the data center, but to do so without compromising safety, security, or availability of the IT operation. Efficiency considerations affect almost every aspect of a data center’s design. So-called “holistic” design considerations include:

- Site selection (e.g., climate, proximity to water, air quality, power source[s], etc.)
- Building construction and layout:
 - Construction materials
 - Multi use/multi-tenant vs. purpose-built
 - “Modular” (e.g., containerized) and scalable versus “traditional” network architecture
 - Human-machine interface
 - Layout of operational and support spaces
 - Placement of IT and non-ITE
 - Use of alternative energy (e.g., wind, solar, thermal storage, etc.)
 - High performance building methods, metrics, and certifications (e.g., USGBC LEED, ASHRAE bEQ, ENERGY STAR for buildings/data centers, The Green Grid PUE, STEP Foundation, *EU Code of Conduct for Data Centres*)
- Selection of energy-efficient ITE (e.g., servers, storage devices, etc.)
- Selection of energy-efficient devices within the direct power path (e.g., transformers, UPS systems, power distribution units, power strips, etc.)
- Design of critical path power flow to ensure that the data center, area or zone meets the performance requirements of the desired Availability Class (e.g., levels of redundancy) with minimum power consumption
- Decisions on deployment of open racks versus ITE cabinets
- Selection and placement of energy-efficient essential support equipment (e.g., air conditioning systems) including such things as:
 - Perimeter versus in-row versus ceiling-mount air handling systems
 - Minimizing the distance that air, water, or power must travel between source and use
- Design of mechanical systems to optimize the operating environment of ITE (e.g., operating temperature, humidity), including such things as:
 - Raised floors versus slab
 - Equipment layout (hot-aisle/cold-aisle)
 - Aisle containment systems
 - Air or water side economizer operation
 - Cogeneration/combined heat and power (CHP)
- Integration of building information management systems
 - Metering, reporting, and controls

Certain principles apply to any design such as:

- Design for the entire system rather than for individual components. Two data centers with identical ITE can have very different electric bills and different PUE because of the system design and the activities of the data center
- Optimize equipment cooling infrastructure:
 - At some point, liquid cooling may be a better option than air cooling, but also consider flexibility, capital costs, operating costs, and reliability of pumps.
 - Lay out equipment in a manner to minimize the mixing of ITE input and exhaust air.
 - Use blanking panels.
 - Utilize ITE designed to operate reliably at high ambient temperatures.
 - Consider cabinets versus open rack systems.
 - Consider aisle containment systems.
 - Use water or air-side economizers where feasible.
- Configure and utilize software such as data center infrastructure management (DCIM) software. Minimize the number of task-specific or proprietary software protocols that are used. A common language that can interface with a building information management (BIM) system is best.
- Avoid running power and signal cabling in spaces meant for movement of air (such as under a raised floor) as this practice can create obstructions and alter air patterns.
- Minimize the distances that air, power, and/or water must travel to reach the ITE. Consider using point of use (close-coupled) power systems, air conditioning systems, and/or chilled water distribution systems.
- Use modular equipment (power, cooling, and IT) in order to match the infrastructure components to the needs of the ITE (i.e., “right-size”).
- Use best-in-class power equipment that can deliver high efficiency over a broad range of loads (e.g., percent efficiency in the high 90s when running at 20% to 100% of load). Consider multi-mode equipment that can operate in higher efficiency modes when conditions are favorable (e.g., UPS with eco-mode option or air conditioning with economizer mode).
- Install energy-efficient lighting (e.g., LED) and controls to illuminate only when and where needed.
- Plumb for efficiency. Close couple wherever possible. Insulate plumbing and make it easily accessible without interrupting other datacenter infrastructure.
- Run plumbing (e.g., chilled water) in directions parallel to the equipment and to air flow.

G.3 Efficiency Content of BICSI 002-2014

Within BICSI 002, sections that include information related to improving efficiency are identified in the following list:

• Design for Efficiency and Metrics	Section 6.7
• Site Selection	Section 5
• Building Construction and Configuration	
– Alternative Energy Considerations	Section 5.7.5.4
– Cooling Capacity	Section 6.3
– Critical Path Power Space Planning	Section 6.2
– Environmental Design	Section 6.4.11
– Functional Adjacencies	Section 6.4
– General Considerations	Section 7.2
– Modularity	Section 6.1.2
• Power	
– Capacity versus Utilization	Section 9.1.5
– Critical Path Power Space Planning	Section 6.2
– Direct Current (DC)	Section 9.3.13
– Distribution with Access Floor	Section 6.5.2
– Lighting	Section 9.8
– Mechanical Equipment Support	Section 9.4
– Monitoring	Section 9.3.7

<List continues on next page>

- Mechanical/Cooling Systems
 - Access floors Section 6.5
 - Aisles (e.g., hot/cold aisle, containment) Sections 6.6.3, 14.12.5
 - Ceilings Section 7.5.11
 - Computer Room Cooling Section 10.6
 - Space Planning Section 6.3
 - Thermal Management Sections 10.5, 14.12.5
- Information Technology Equipment
 - Aisles Section 6.6.3
 - Computer Room Configuration Section 15.4
 - Racks, Cabinets and Frames Sections 6.6.2, 14.12
 - With use of access floors Section 6.5
- Data Center Infrastructure Management (DCIM) Section 13.1

Note that this list is not inclusive of all efficiency content within BICSI 002 as other recommendations outside of the sections listed above may provide additional efficiency benefit.

Appendix H Related Documents (Informative)

This appendix is not part of the requirements of this standard, but it is included to provide additional information related to this standard.

The following standards and documents are related to or have been referenced within recommendations of this standard and provide additional information that may be of use to the reader.

American Society for Testing and Materials (ASTM International)

- ASTM B539, *Measuring Contact Resistance of Electrical Connections (Static Contacts)*
- ASTM E136, *Standard Test Method for Behavior of Materials in a Vertical Tube Furnace at 750°C*
- ASTM E814, *Standard Test Method for Fire Tests of Penetration Firestop Systems*
- ASTM F1233, *Standard Test Method for Security Glazing Materials And Systems*

American Society of Civil Engineers (ASCE)

- ASCE/SEI 59, *Blast Protection of Buildings*

American Society of Heating, Refrigerating, and Air-Conditioning Engineer (ASHRAE)

- ANSI/ASHRAE 52.2, *Method of Testing General Ventilation Air-Cleaning Devices for Removal Efficiency by Particle Size*
- ANSI/ASHRAE/IESNA 90.1, *Energy Standard for Buildings Except Low-Rise Residential Buildings*
- *ASHRAE Handbook – Fundamentals*
- *ASHRAE Handbook – HVAC Applications*
- *ASHRAE Handbook – HVAC Systems and Equipment*

BICSI

- ANSI/BICSI 003, *Building Information Modeling (BIM) Practices for Information Technology Systems*

Builders Hardware Manufacturers Association (BHMA)

- ANSI/BHMA A156.13, *Mortise Locks & Latches*

Building Services Research and Information Association (BSRIA)

- BG 5/2003, *Cooling solutions for IT - A guide to planning, design and operation*

European Committee for Electrotechnical Standardization (CENELEC)

- CENELEC EN 50541-1, *Three phase dry-type distribution transformers 50 Hz, from 100 kVA to 3 150 kVA, with highest voltage for equipment not exceeding 36 kV – Part 1: General requirements*

EMerge Alliance

- *Data/Telecom Center Standard*

European Telecommunications Standards Institute (ETSI)

- ETSI EN 300 132-3, *Environmental Engineering (EE); Power supply interface at the input to telecommunications and datacom (ICT) equipment; Part 3: Operated by rectified current source, alternating current source or direct current source up to 400 V*

Factory Mutual

- *FM Global Property Loss Prevention Data Sheets 1-28*

Illuminating Engineering Society (IES)

- *IESNA Lighting Handbook*
- *ANSI/IESNA RP-1-04, American National Standard Practice for Office Lighting*

Institute of Electrical and Electronics Engineers (IEEE)

- *ANSI/IEEE C2, National Electrical Safety Code (NESC)*
- *IEEE C62.72, IEEE Guide for the Application of Surge-Protective Devices for Low-Voltage (1000 Volts or Less) AC Power Circuits*
- *IEEE 446, IEEE Recommended Practice for Emergency and Standby Power Systems for Industrial and Commercial Applications*
- *IEEE 485, IEEE Recommended Practice for Sizing Lead-Acid Batteries for Stationary Applications*
- *IEEE 902 (The IEEE Yellow Book), IEEE Guide for Maintenance, Operation and Safety of Industrial and Commercial Power Systems*
- *IEEE 946, IEEE Recommended Practice for the Design of DC Auxiliary Power Systems for Generating Systems*
- *IEEE 1013, IEEE Recommended Practice for Sizing Lead-Acid Batteries for Stand-Alone Photovoltaic (PV) Systems*
- *IEEE 1375, IEEE Guide for the Protection of Stationary Battery Systems*
- *IEEE 1635, IEEE/ASHRAE Guide for the Ventilation and Thermal Management of Batteries for Stationary Applications*
- *IEEE 1692, Guide for the Protection of Communications Installations from Lightning Effects*

Insulated Cable Engineers Association

- *ICEA S-83-596, Indoor Optical Fiber Cables*
- *ICEA S-87-640, Optical Fiber Outside Plant Communications Cable*
- *ICEA S-104-696, Standard for Indoor-Outdoor Optical Fiber Cable*
- *ICEA S-110-717, Optical Drop Cables*

International Electrotechnical Commission (IEC)

- *IEC 60603-7, Connectors for electronic equipment (multiple document series)*
- *IEC 61300-3-6:, Basic Fibre Optic Test Procedures – Part 3: Examination and measurement (multiple document series)*
- *IEC 61754, Fibre Optic Connector Interface (multiple document series)*
- *IEC 62040, Uninterruptible power systems (UPS) (multiple document series)*

International Organization for Standardization (ISO)

- *ISO/IEC 14908-1, Information technology – Control network protocol*
- *ISO 16484, Building automation and control systems*
- *ISO 27001, Information security management*
- *ISO/IEC TR 29106:2007, Information technology – Generic cabling – Introduction to the MICE environmental classification*

Laser Institute of America (ASC Z136)

- *ANSI Z136.2, American National Standard for Safe Use of Optical Fiber Communications Systems Utilizing Laser Diode and LED Sources*

National Electrical Contractors Association (NECA)

- *ANSI/NECA 339, Standard for Building and Service Entrance Grounding and Bonding*
- *ANSI/NECA/BICSI 568, Standard for Installing Commercial Building Telecommunications Cabling*

National Electrical Manufacturers Association

- ANSI C80.3, *American National Standard For Steel Electrical Metallic Tubing (EMT)*
- NEMA VE 1, *Cable Tray Systems*
- NEMA VE 2, *Metal Cable Tray Installation Guidelines*

National Fire Protection Association (NFPA)

- NFPA 70B, *Recommended Practice for Electrical Equipment Maintenance*
- NFPA 90A, *Standard for the Installation of Air-conditioning and Ventilating Systems*
- NFPA 101, *Life Safety Code*
- NFPA 110, *Standard for Emergency and Standby Power Systems*
- NFPA 111, *Standard on Stored Electrical Energy Emergency and Standby Power Systems*
- NFPA 258, *Recommended Practice for Determining Smoke Generation of Solid Materials*
- NFPA 5000, *Building Construction and Safety Code*
- *NFPA Fire Protection System for Special Hazards*

Telecommunication Industry Association (TIA)

- TIA-232-F, *Interface Between Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange*
- ANSI/TIA-455-57-B, FOTP-57, *Preparation and Examination of Optical Fiber Endface for Testing Purposes*
- ANSI/TIA-455-95-A, FOTP-95, *Absolute Optical Power Test for Optical Fibers and Cables*
- ANSI/TIA-455-133-A, FOTP-133-IEC-60793-1-22, *Optical Fibres-Part 1-22: Measurement Methods and Test Procedures-Length Measurement*
- ANSI/TIA/EIA-4720000-A, *Generic Specification for Optical Waveguide Fibers*
- ANSI/TIA/EIA-472D000-B, *Sectional Specification (Adopted ANSI/ICEA S-87-640-2006) Standard for Optical Fiber Outside Plant Communications Cable*
- ANSI/TIA/EIA-485-A, *Electrical Characteristics Of Generators And Receivers For Use In Balanced Digital Multipoint Systems*
- ANSI/TIA-568-C.0, *Generic Telecommunications Cabling for Customer Premises*
- ANSI/TIA-568-C.1, *Commercial Building Telecommunications Cabling Standard*
- ANSI/TIA-758-B, *Customer Owned Outside Plant Telecommunications Infrastructure Standard*
- TIA-TSB-185, *Environmental Classification (Mice) Tutorial*

Underwriters Laboratories (UL)

- ANSI/UL 797, *Standard for Electrical Metallic Tubing – Steel*
- ANSI/UL 972, *Burglary-Resisting Glazing Material*
- ANSI/UL 1479, *Standard for Fire Tests of Through-Penetration Firestops*

United States Department of Defense

- UFC 3-301-01, *Structural Engineering*
- UFC 3-310-04, *Seismic Design of Buildings*

Other Standards and Documents

- *Americans with Disabilities Act (United States)*
- *Disability Discrimination Act (Australia)*
- Federal Communications Commission (FCC) Part 15 and Part 68 (United States)
- Haas, Pierce & Schutter, "Data Center 2.0 Design Guide Program Overview," The Green Grid, 2009
- *International Fire Code (IFC), 2009*
- Rural Utilities Services (RUS), Bulletin 345-63, *RUS Specifications for Acceptance Tests and Measurements of Telephone Plant (1995)*