STANDARDS

an American National Standard

ANSI/BICSI 005-2016

Electronic Safety and Security (ESS) System Design and Implementation Best Practices

BICSI®

ANSI/BICSI 005-2016

Electronic Safety and Security (ESS) System Design and Implementation Best Practices

Committee Approval: April 2016
First Published: May 2016

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 its 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 By the end of the fifth year after a standard's publication, the standard will be reaffirmed, rescinded, or revised according to the submitted updates and comments from all interested parties.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

Copyright © 2015 BICSI
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 ..... **xi**

1 Introduction **1**

1.1 General **1**

1.2 Purpose **1**

1.3 Categories of Criteria **1**

2 Scope **2**

3 Required Standards and Documents **3**

4 Definitions, Acronyms, Abbreviations, and Units of Measurement **5**

4.1 Definitions **5**

4.2 Acronyms and Abbreviations **9**

4.3 Units of Measurement **10**

5 Telecommunications Infrastructure **11**

5.1 Overview **11**

5.2 Topology **11**

5.2.1 Star Topology 11

5.2.2 Non-Star Topologies 11

5.3 Spaces **12**

5.3.1 Equipment Rooms 12

5.3.2 Telecommunications Rooms and Telecommunications Enclosures 14

5.4 Cabling **15**

5.4.1 Backbone Cabling 15

5.4.2 Horizontal Cabling 15

5.4.3 Horizontal Connection Point (HCP) 19

5.4.4 Power over Ethernet (PoE) 20

5.5 Cabling Pathways **21**

5.5.1 Requirements 21

5.5.2 Enclosures, Pull Boxes and Splice Boxes 21

5.5.3 ESS Pathway Redundancy 21

5.5.4 ESS Pathways between Telecommunications Spaces within a Building 21

5.5.5 ESS Campus Pathways Between Buildings 22

5.5.6 ESS Pathways Serving Equipment Outlets 22

5.5.7 ESS Pathway Separation from Power and EMI Sources 22

5.5.8 ESS Pathway Bonding and Grounding 23

5.5.9 Special Pathways and Spaces Considerations 23

5.5.10 Secure Areas 24

5.6 Telecommunications Outlet and Connectors **24**

5.6.1 Overview 24

5.6.2 Facility Connections by Modified Permanent Link Method 25

5.7 Cabling Installation Requirements **26**

5.7.1 Overview 26

5.7.2 Bonding and Grounding Considerations 26

5.7.3 Transmission Performance Field Testing 26

5.8 Administration and Documentation **28**
5.8.1 Requirements 28
5.8.2 Recommendations 28
5.9 ESS Device Mounting Heights **28**
5.9.1 Requirements 28
5.9.2 Recommendations 29
5.10 Infrastructure for Wireless Transmission **29**
5.10.1 Requirements 29
5.10.2 Additional Information 29
5.11 Coverage Area Planning and Density **29**
5.11.1 Introduction 29
5.11.2 Recommendations 29

6 Intrusion Detection Systems **31**
6.1 Overview **31**
6.2 Developing an IDS **31**
6.2.1 Requirements 31
6.2.2 Recommendations 31
6.3 System Connectivity **31**
6.3.1 Wired Devices 31
6.3.2 Wireless Devices 32
6.4 Sensors **32**
6.4.1 Introduction 32
6.4.2 Recommendations 32
6.5 Notification **32**
6.5.1 Requirements 32
6.5.2 Recommendations 32
6.5.3 Additional Information 33
6.6 Control Panel **33**
6.6.1 Requirements 33
6.6.2 Recommendations 33
6.7 Keypads and Annunciators **34**
6.7.1 Requirements 34
6.7.2 Recommendations 34
6.8 Initiating Devices **34**
6.8.1 Overview 34
6.8.2 Motion Sensors 34
6.8.3 Window Sensors 34
6.8.4 Door Status Sensors 35
6.8.5 Perimeter Sensors 35
6.9 Optional Integrated Equipment **35**
6.9.1 Introduction 35
6.9.2 Requirements 35

7 Video Surveillance **37**
7.1 Overview **37**
7.2 Generation and Conformance with Use Cases **37**
7.2.1 Scene Characteristics 37
7.2.2 Observation as a Primary VSS Function 38
7.2.3 Forensic Review as a Primary VSS Function 38
7.2.4 Recognition as a Primary VSS Function 39
7.2.5 Additional VSS Functions 39

7.3 Device Groups and Interoperability ... 40
7.3.1 Requirements ... 40
7.4 Device Categories ... 40
7.4.1 Requirements ... 40
7.5 Use Cases ... 41
7.5.1 Requirements ... 41
7.6 Open Network Video Interface Forum Conformance ... 41
7.6.1 Requirements ... 41
7.7 Deployment Process ... 41
7.7.1 Requirements ... 41
7.7.2 Recommendations ... 42
7.8 Authentication of Network Video Cameras for Improved ESS Network Security ... 43
7.8.1 Requirements ... 43

8 Access Control Systems ... 45
8.1 Overview ... 45
8.2 System Structure ... 45
8.2.1 Overview ... 45
8.2.2 Central Equipment Processing (Level 1) ... 45
8.2.3 Computer Hardware and Software ... 45
8.2.4 Server ... 45
8.2.5 Software ... 46
8.2.6 Backup ... 46
8.2.7 Event Recording ... 46
8.2.8 Backup Power ... 46
8.2.9 Access Control Workstation ... 46
8.2.10 Badging System ... 47
8.2.11 Visitor Management ... 47
8.3 Controllers for Intelligent Field Processing (Level 2) ... 47
8.3.1 Overview ... 47
8.3.2 Controller Configurations ... 47
8.4 Peripheral Devices (Level 3) ... 48
8.4.1 Overview ... 48
8.4.2 Relays ... 48
8.4.3 Power Distribution ... 48
8.4.4 Readers ... 49
8.4.5 Request to Exit Devices ... 49
8.4.6 Door Contacts ... 49
8.4.7 Electrified Door Hardware ... 49
8.4.8 Fail-Secure/Fail-Safe/Fail Latched ... 49
8.4.9 Power to Locks ... 50
8.5 Credentials (Level 4) ... 51
8.5.1 Overview ... 51
8.5.2 Web-Enabled Access Control ... 51
8.5.3 IP Card Readers ... 51
8.5.4 IP Controllers ... 51
8.5.5 Communications ... 51
8.5.6 Analog Communications ... 52
8.5.7 TCP/IP or Network Communications ... 52

9 Fire Alarm Systems 53

9.1 Introduction 53
9.1.1 Overview 53
9.1.2 Recommendations 54

9.2 Regulatory 54
9.2.1 Overview 54

9.3 Risk Assessment 54
9.3.1 Overview 54
9.3.2 Requirements 54
9.3.3 Recommendations 55

9.4 Fire Alarm Systems 55
9.4.1 Introduction 55
9.4.2 Control Panel 55
9.4.3 Detection/Initiation 56
9.4.4 Notification Appliances 56

9.5 Communications Systems 57
9.5.1 Overview 57
9.5.2 Requirements 57
9.5.3 Recommendations 57

9.6 Pathways 58
9.6.1 Introduction 58
9.6.2 Class N 58
9.6.3 Class N Cabling 60

9.7 Circuits 60
9.7.1 Overview 60
9.7.2 Requirements 61
9.7.3 Recommendations 61

9.8 Monitoring and Supervision 61
9.8.1 Overview 61
9.8.2 Requirements 62
9.8.3 Recommendations 62

9.9 Power over Ethernet (PoE) Implementation 62
9.9.1 Overview 62
9.9.2 Requirements 62
9.9.3 Recommendations 62

9.10 Class N Operations and Maintenance 62
9.10.1 Overview 62
9.10.2 Requirements 62
9.10.3 Recommendations 62

9.11 As-Built Drawings and Related Documentation 62
9.11.1 Overview 62
9.11.2 Requirements 62
9.11.3 Recommendations 62

10 Integrated Systems 63

10.1 Overview 63

10.2 ESS Integrated Services, Design and Integration 63
10.2.1 Public Network Services 63
10.2.2 Design and Selection of Components 64
10.2.3 ESS Integration 64

10.3 ESS Components **64**
10.3.1 Overview 64
10.3.2 Intrusion Detection System 64
10.3.3 Access Control System 65
10.3.4 Video Surveillance System 65
10.3.5 Physical Security Information Management System 65
10.3.6 Sensor-Based System 65
10.3.7 Building Automation System 65
10.3.8 Location System 65
10.3.9 Global Positioning System 67
10.3.10 Automated Infrastructure Management (AIM) with other ESS systems 67
10.3.11 Software 68
10.4 System Configuration and Expandability **69**
10.4.1 Overview 69
10.4.2 Input/Output Matrix 69
10.4.3 Maps and Icons 69
10.4.4 System Response Times 70
10.4.5 System Expansion Capability 70
10.5 ESS Integration Process **70**
10.5.1 Overview 70
10.5.2 Integration Process Team Members 70
10.5.3 Integration Process 71

11 Risk Management and Risk Assessment **75**
11.1 Introduction **75**
11.2 Requirements **75**
11.3 Additional Information **75**

12 Commissioning **77**
12.1 Overview **77**
12.2 Documentation **77**
12.2.1 Overview 77
12.2.2 Requirements 77
12.3 Cleaning **78**
12.3.1 Overview 78
12.3.2 Requirements 78
12.3.3 Recommendations 78
12.4 Labeling Components **78**
12.4.1 Requirements 78
12.4.2 Recommendations 78
12.5 Testing **78**
12.5.1 Acceptance Testing Plan 78
12.5.2 System Testing 78
12.5.3 Acceptance Testing 79
12.5.4 Retesting Equipment and Systems 80
12.5.5 Warranty Periods 80
12.6 Additional Commissioning Tasks **80**
12.7 Training **81**

Appendix A Cabling Pathways (Normative) **83**
A.1 Overview **83**
A.2 Types of Cabling Pathways **83**
A.3 General Installation Practices **91**

Appendix B Electronic Safety and Security (ESS) Design Fundamentals (Informative).. 92
B.1 Introduction 93
B.2 Elements 93
B.3 Types of Projects 94
B.4 Current and Future Trends in Safety and Security 94
B.5 Electronic Safety and Security System Development Basics 95

Appendix C Wireless Transmission (Informative) 97
C.1 Overview 97
C.2 Radio Frequency Transmission 97
C.3 Free Space Optics 97
C.4 Licensed Microwave Radio Transmission 98
C.5 Frequency Selection 98

Appendix D Cloud Computing (Informative) 99
D.1 Overview 99
D.2 Services 99
D.3 Infrastructure Management of Cloud Services 101
D.4 Selecting an Infrastructure Management Model 102
D.5 Cloud Deployment Models 103
D.6 Delivering Secure Services 103
D.7 Trends 104

Appendix E System Training (Informative) 105
E.1 Overview 105
E.2 Sessions 105
E.3 Position or Task Training 105
E.4 Training Schedules 107

Appendix F ESS Operations and Maintenance (Informative) 109
F.1 Operation Best Practices 109
F.2 Maintenance Plan Recommendations 110
F.3 Service Contracts 110

Appendix G Related Documents (Informative) 113

INDEX OF FIGURES

Section 5 Telecommunications Infrastructure

Figure 5-1 Hierarchical Star Topology 11
Figure 5-2 Examples of Non-star Topologies 12
Figure 5-3 Optical Fiber Cabling With Media Converters 18
Figure 5-4 Configuration Examples for Using Hybrid Copper/Optical Fiber Cable to Connect an ESS Device 19
Figure 5-5 Example of a Horizontal Connection Point Within a Star Topology 20
Figure 5-6 Example Locations of User-Administered and Facility Connection Telecommunications Outlets 25
Figure 5-7 Examples of Facility Connections Using a Modified Permanent Link 25
Figure 5-8 Configuration 1: Single Connector Modified Permanent Link Set Up for a Modified Permanent Link Without a Consolidation Point 27
Figure 5-9 Configuration 2: Single Connector Modified Permanent Link Set Up for a Modified Permanent Link With a Consolidation Point 28

Section 8 Access Control Systems

Figure 8-1 Form A, B and C Relays 48

Section 9 Fire Alarm Systems

Figure 9-1 Basic Fire Alarm System 53

Section 10 Integrated Systems

Figure 10-1 Sample Physical Security Information Management System 66

INDEX OF TABLES

Section 5 Telecommunications Infrastructure

Table 5-1 Recommended Cross-Connect Color Codes For Use at Cabling Distributors 13
Table 5-2 Media Selection Criteria 16
Table 5-3 Balanced Twisted-Pair Cabling Frequency Range of Interest and Associated Applications 17
Table 5-4 Typical Coverage Area for Each ESS Link 30

Section 6 Intrusion Detection Systems

Table 6-1 Detection Sensor Technology and Application 32

Appendix A Cabling Pathways (Normative)

Table A-1 Balanced Twisted-Pair Cabling Bend Radius and Pulling Tension Requirements 84
Table A-2 Optical Fiber Cabling Bend Radius and Pulling Tension Requirements 85
Table A-3 Maximum Allowable Cabling Stacking Height in Cabling Pathways 85

Appendix F ESS Operations and Maintenance (Informative)

Table F-1 Emergency Response Category Matrix 112

This page intentionally left blank

PREFACE

Revision History

May 5, 2013 First publication of this standard, titled ANSI/BICSI 005-2013, *Electronic Safety and Security (ESS) System Design and Implementation Best Practices*

May 11, 2016 Revision of ANSI/BICSI 005-2013 published as ANSI/BICSI 005-2016, *Electronic Safety and Security (ESS) System Design and Implementation Best Practices*

Major revisions include:

- Complete revision of Section 9, including section title change to *Fire Alarm System*s
- Addition of Section 12, *Commissioning*
- Addition of Appendix D, *Cloud Computing*
- Addition of Appendix E, *System Training*
- Addition of Appendix F, *ESS Operations and Maintenance*

Minor revisions include:

- Addition of content for automated infrastructure management (AIM)
- Addition of content for physical security of cabling infrastructure
- General content updates and editorial corrections

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.
- Deletions of one or more paragraphs are indicated with a bullet (•) between the content that remains

Translation Notice

This standard may have one or more translations available for the convenience of its readers. As translated text may contain inconsistencies when compared to 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.

This page intentionally left blank

1 Introduction

1.1 General

This standard is written in the context that a comprehensive safety and security strategy for a specific project or property has been developed. The interconnections of these electronic safety and security (ESS) systems are facilitated once the client requirements have been determined by parties responsible for the development of those requirements. The designed or recommended system takes into account the environmental constraints in which the electronic safety and security infrastructure will be installed and operated. This includes consideration of the appropriate safeguards that may be necessary due to:

- Layout of a particular area
- Environment
- Topology
- Climate
- Current and future types of equipment to be supported
- Type of cabling
- Functionality of the network
- Pathways or spaces over which the cabling will be installed

1.2 Purpose

This standard is written for use in the design and implementation of the structured cabling systems used within electronic safety and security systems. This standard provides a reference of common technology and design practices, and is not intended to be used by architects and engineers as their sole reference or as a step-by-step design guide. This standard may also be used to determine design requirements in conjunction with the system owner, occupant, or safety and security consultant.

This standard is intended primarily for, but not limited to:

- ESS system owners and operators
- ESS system consultants and project managers
- Architects
- Authorities having jurisdiction (AHJ)
- Engineers
- ESS system installers

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 ESS system 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. When possible, recommendations and requirements were separated to aid in clarity.

2 Scope

This standard applies to the electronic safety and security systems that are provided by a physical security professional. Electronic devices and systems include, but are not limited to:

- Safety systems
- Physical access control
- Video surveillance
- Intrusion detection systems
- Integrated systems

The performance specifications for the electronic safety and security systems are not offered in this standard unless it relates to the structured cabling systems. For example, desired frame rates and image quality for video surveillance systems impact the bandwidth of the signal and therefore impact the type of cabling selected. This standard will not describe the selection of the frame rates and the video quality but will describe bandwidth and cabling considerations for video content.

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 agreements 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.

BICSI

- ANSI/NECA/BICSI 607, *Telecommunications Bonding and Grounding Planning and Installation Methods for Commercial Buildings*
- ANSI/BICSI 006, *Distributed Antenna System (DAS) Design and Implementation Best Practices*

British Standards Institution (BSI)

- BS 6701, *Telecommunications equipment and telecommunications cabling. Specification for installation, operation and maintenance*
- BS 7671, *Requirements for Electrical Installations. IET Wiring Regulations*

European Committee for Electrotechnical Standardization (CENELEC)

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

Institute of Electrical and Electronics Engineers (IEEE)

- IEEE 802.3, *IEEE Standard for Ethernet*

International Electrotechnical Commission (IEC)

- IEC 60364-4-43, *Low-voltage electrical installations – Part 4-43: Protection for safety – Protection against overcurrent*
- IEC 60364-5-52, *Electrical installations of buildings – Part 5-52: Selection and erection of electrical equipment – Wiring systems*
- IEC 60849, *Sound systems for emergency purposes*

International Organization for Standardization (ISO)

- ISO 12233, *Photography – Electronic still-picture cameras – Resolution measurements*
- ISO 14524, *Photography – Electronic still-picture cameras – Methods for measuring opto-electronic conversion functions (OECFs)*
- ISO/IEC 11801-1, *Generic cabling for customer premises – Part 1: General requirements*
- ISO/IEC 14763-2, *Information technology – Implementation and operation of customer premises cabling – Part 2: Planning and installation*
- ISO/IEC 18598, *Information technology – Automated infrastructure management (AIM) systems – Requirements, data exchange and applications*
- ISO/IEC 30129, *Information Technology – Telecommunications bonding networks for buildings and other structures*

NFPA

- NFPA 70®, *National Electrical Code®*
- NFPA 72, *National Fire Alarm and Signaling Code*

Open Network Video Interface Forum (ONVIF)

- *ONVIF Core Specification, version 2.2*

Telecommunication Industry Association (TIA)

- ANSI/TIA 526-7-A, *Measurement of Optical Power Loss of Installed Single-Mode Fiber Cable Plant, Adoption of IEC 61280-4-2 edition 2: Fibre-Optic Communications Subsystem Test Procedures – Part 4-2: Installed Cable Plant – Single-Mode Attenuation and Optical Return Loss Measurement*
- ANSI/TIA-526-14-C, *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-568.0-D, *Generic Telecommunications Cabling for Customer Premises*
- ANSI/TIA-568.1-D, *Commercial Building Telecommunications Cabling Standard*
- 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-D, *Telecommunications Pathways and Spaces*
- ANSI/TIA-606-B, *Administration Standard for Telecommunications Infrastructure*
- ANSI/TIA-607-C, *Generic Telecommunications Bonding and Grounding (Earthing) for Customer Premises*
- ANSI/TIA-758-B, *Customer-Owned Outside Plant Telecommunications Infrastructure Standard*
- ANSI/TIA-862-B, *Structured Cabling Infrastructure Standard For Intelligent Building Systems*
- ANSI/TIA-1005-A, *Telecommunications Infrastructure Standard for Industrial Premises*
- ANSI/TIA-1152-A, *Requirements for Field Test Instruments and Measurements for Balanced Twisted-Pair Cabling*
- ANSI/TIA-5017, *Telecommunications Physical Network Security Standard*

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

annunciator A device that provides information on the state or condition of components, devices or systems(s). In addition to status, the device may display specific status information (e.g., trouble, alarm).

backbone (1) A facility (e.g., pathway, cable, conductors) between any of the following spaces**:** telecommunications rooms (TRs), common TRs, floor-serving terminals, entrance facilities, equipment rooms, and common equipment rooms (CER). (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, intermediate distribution areas , horizontal distribution areas , and TRs.

backbone cabling See *backbone*.

balun An impedance matching transformer used for coupling two electrical circuit elements, where one is balanced (balanced twisted-pair) and the other is unbalanced (coaxial cabling).

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.

color temperature Characterization of a light source in terms of the temperature of a theoretical blackbody radiator that would have a color (spectral energy density) that most closely resembles that of the illuminating source.

component Any part or subassembly of devices used in the construction of a system (e.g., video surveillance system).

compression The process of encoding or modifying data files from its original form to a file of a smaller size.

credential An item or object that allows the possessor to enter, exit or access an identified space, object or asset.

cross-connect A facility enabling the termination of cabling elements and their interconnection or cross-connection.

device A general term given to the components of a system which perform one or more functions (e.g., detection, measurement, observation), but do not provide system management or complex control functionality. Within an individual ESS discipline (e.g., fire alarm), the term *device* may be further defined to represent a specific functionality or expected behavior.

digital multimedia content Materials or files that include a combination of text, audio, still images, animation, video, or interactive content forms that are stored as a series of discrete values within an electronic device.

direct attach See *modified permanent link.*

display A device that shows images, text, or other content by converting analog or digital signals into visible form.

download The process of receiving data at a specific electronic device from another digital source (e.g., computer, network-enabled system, local or remote server).

egress A point or means of exit from a building, property, or location.

encoder A device that converts data into a form suitable for transmission over a specified medium.

equipment cord A length of cable with connectors on both ends used to join active equipment directly to other active equipment or the cabling infrastructure.

equipment room (telecommunications) An environmentally controlled centralized space for telecommunications and data processing equipment with supporting communications connectivity infrastructure.

fail-latched A property of a locking device that upon the loss of power, the device will latch or remain latched but does not necessarily restrict movement or access from the secured side.

fail-safe A property of a locking device that upon the loss of power, the device will automatically unlock (open) or remain unlocked (open).

fail-secure A property of a device that upon the loss of power, the device will automatically lock (close) or remain locked (closed).

field of view ’The extent of the observable location or area that is seen at any given moment from a defined point. For ESS devices, the field of view is typically described as an angle on a specified plane (e.g., vertical, horizontal) or as a cone within encompasses two or more planes for which a detector or device will perform its observation function(s). For cameras, the field of view may also be known as the *angle of view*.

fire detection The means of detecting the occurrence of heat, smoke or other particles or products of combustion.

fire suppression The products, materials, and methods used to control and extinguish an active fire.

forensic review A property of video surveillance equipment, which denotes that the equipment has been optimized to provide high resolution recordings of scene content or digital multimedia content (DMC) captured by the video camera or encoding device.

horizontal cabling (1) The cabling between and including the telecommunications outlet and 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 connection point A location for connections between horizontal cables that extend from building pathways and horizontal cables that extends to building automation systems (BAS) devices and equipment.

horizontal cross-connect A cross-connect of horizontal cabling to other cabling (e.g., backbone cabling, active equipment).

hybrid cable An assembly of two or more cables, of the same or differing types of media, categories designation, etc., covered by one overall sheath.

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.

interoperability The ability of two or more systems to communicate and exchange data, while allowing any of the participating systems to use the exchanged information.

jumper An assembly of twisted-pair conductors or balanced twisted-pair, optical fiber, or coaxial cable used to join telecommunications circuits and links at a cross-connect or between patch panels. Jumpers may have connectors at neither, one, or both ends of the assembly.

keypad A data input device consisting of a limited number of keys, each with nominated functions.

Listed Equipment, materials, or services included in a list published by an organization that is acceptable to the authority having jurisdiction (AHJ), that maintains periodic inspection of production of listed equipment or materials or periodic evaluation of services, and whose listing states either that the equipment, material or services meets appropriate standards or has been tested and found suitable for use in a specified manner.

luminance A measure of the brightness of a point on a surface that is radiating or reflecting light.

media (telecommunications) Wire, cable, or conductors used for telecommunications.

media converter A device that converts from one type of media to another. Typically referring to a hardware device that connects different transmission media (i.e., from balanced twisted-pair to coax or from balanced twisted-pair to optical fiber).

metadata Data embedded within or associated with a file that describes information about or related to the file or directory. This may include but is not limited to color, size, trajectory and the locations where the content is stored, dates, times, application specific information, and permissions.

modified permanent link The horizontal cabling on the remote device end directly attaching (or connecting) to the device through a connectorized cable or hard-wired termination, eliminating the need for a telecommunications outlet and equipment cord for the device.

modular plug The insert ("male") 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. A modular plug is named for the number of position and contacts it has (e.g., 8P8C for 8 positions, 8 contacts).

NOTE 1 **:** The receptacle that a modular plug is inserted into is named a *modular jack*.

NOTE 2: Some specific configurations of a modular plug may be termed as a *registered jack* or *RJ##*. An example is a RJ45, which is equivalent to an 8P8C configuration.

observation A function in video surveillance systems that may be optimized to provide continuous viewing of scene content captured by the video camera or encoding device and displayed on local or remote monitors, or on remote display devices like smart-phones, tablets, or laptop computers.

panel An electrical device consisting of an enclosure, box or surface that may contain switches, dials, displays or meters for controlling or monitoring other electrical devices.

patch cord A jumper with connectors on both ends used to join telecommunications circuits/links, for example between two patch panels.

patch panel A connecting hardware system that facilitates cable termination and cabling administration using patch cords.

pathway (telecommunications) A facility for the placement of telecommunications cable.

pixel In digital imaging, a single point in a bitmap image, or the smallest addressable screen element in a display device. It is the smallest unit of a picture that can be represented or controlled.

proprietary A characteristic of a technique, technology, or device which is owned and controlled by a company or other party and is thereby only usable or adaptable as allowed by that party and not deemed to achieve interoperability.

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.

recognition In ESS systems, a function used to capture and record imagery that may include, but not be limited to, vehicle license plate recognition, facial recognition, smoke and fire detection, object recognition, pattern recognition, cross-line detection, object temporal characteristics, color recognition and trajectory.

recording media Any device or component to which digital multimedia content (DMC) is written, stored and can be retrieved.

single connector modified permanent link A test procedure for a Category 5e/Class D or higher modified permanent link plug-ended configuration where the fixed length of cabling is punched down at the near end patch panel and an eight position modular plug is attached at the device far end. The test equipment utilizes a test equipment cord on the near end attached to a permanent link adapter and is directly attached to a channel adapter at the far end. A consolidation point may optionally be located between the near and far ends.

soft space In architectural spaces, virtual spaces adjacent to actual spaces that permit expansion of an actual space into the virtual space if required at a later date (e.g., expansion of a telecommunications room). Examples of architectural spaces by this definition include: storage spaces, conference rooms, unassigned coverage areas, or other spaces not located within the life safety egress path to allow for future expansion.

space (telecommunications) An area whose primary function is to house the installation and termination of telecommunications equipment and cable (e.g., equipment room, telecommunications room, entrance facility).

telecommunications Any transmission, emission, and reception of information (e.g., signs, signals, writings, images, sounds) by cable, radio, optical, or other electromagnetic systems.

telecommunications connector The receptacle and insertion elements which provide a means of aligning, attaching and achieving continuity between the conductors and optical fibers used within telecommunication and ICT applications.

telecommunications outlet An assembly of which consists of a faceplate, body, housing, or supporting bracket, and one or more receptacles or jacks of a telecommunication connector.

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.

termination The physical connection of a conductor to connecting hardware.

topology The physical or logical arrangement of a system.

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 when the acceptable quality of either an alternative source of power (e.g., generator) or the normal source of power becomes available.

use case A list of steps, typically defining interactions between a role and a system, to achieve a goal. The actor can be a human or an external system.

varistor An electronic component used to protect circuits against excessive transient voltages by incorporating them into the circuit in such a way that, when triggered, they will shunt the current created by the high voltage away from the sensitive components. Also known as a voltage dependent resistor.

video monitor A type of display for the viewing of live and recorded video. A video monitor may also be known as a *digital panel*.

4.2 Acronyms and Abbreviations

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

AC	alternating current
ACS	access control system
AFF	above finished floor
AHJ	authority having jurisdiction
AIM	automated infrastructure management
AWG	American wire gauge
BAS	building automation system
BIM	building information modeling
BMS	building management system
CCTV	closed circuit television
CRI	color rendition index
DAS	distributed antenna system
DC	direct current
DMC	digital multimedia content
EMI	electromagnetic interference
EMT	electrical metallic tubing
ER	equipment room
ESS	electronic safety and security
FOV	field of view
GPS	global positioning system
GUI	graphical user interface
HCP	horizontal connection point
HDTV	high definition television
HVAC	heating, ventilation, and air conditioning
ICS	integrated control system
ICT	information communication and technology
IDS	intrusion detection system
IP	Internet protocol
LAN	local area network
NAC	notification appliance circuit
NC	normally closed
NO	normally open
NRTL	nationally recognized testing laboratory
PDS	protected distribution system
PIR	passive infrared
PLC	programmable logic circuit
PoE	power over Ethernet
POTS	plain old telephone service
PSE	power sourcing equipment
PSIM	physical security information management
PTP	point-to-point
PTZ	pan, tilt, zoom
QoS	quality of service
RAID	redundant array of independent disks
REX	request to exit
RF	radio frequency
RFID	radio frequency identification
SCADA	supervisory control and data acquisition
TCP/IP	transmission control protocol/internet protocol
TE	telecommunications enclosure
TR	telecommunications room
UPS	uninterruptible power supply
USB	universal serial bus
UTP	unshielded balanced twisted-pair
VSS	video surveillance system
WAN	wide area network

4.3 Units of Measurement

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

Units of measurement used in this standard are defined below:

Ah	ampere-hour
dB	decibel
dBA	ambient decibel adjusted for frequency
fps	frames per second
ft	foot
ft^2	square foot
GHz	gigahertz
Hz	hertz
in	inch
km	kilometer
lbf	pound force
m	meter
m^2	square meter
Mb/s	megabit per second
MHz	megahertz
mi	mile
mm	millimeter
N	newton
nm	nanometer
ppf	pixels per foot
ppm	pixels per meter
V_{AC}	volt alternate current
V_{DC}	volt direct current
W	watt

5 Telecommunications Infrastructure

5.1 Overview

ESS systems may either share the collective set of cabling system components, cabling pathways, and related telecommunications spaces with a traditional voice/data information and communications technology (ICT) network or use a dedicated ESS network operating in parallel with the traditional voice/data information ICT network. Regardless of the way that these systems are deployed, telecommunications cabling infrastructure standards and telecommunications cabling installation best practices should be observed.

This section addresses the best practices for the design and installation of a telecommunications cabling infrastructure for ESS devices to support a wide range of applications.

The basic elements of the telecommunications infrastructure are the following:

- Topology
- Equipment room (ER)
- Telecommunications room (TR)
- Telecommunications enclosure (TE)
- Backbone cabling
- Horizontal cabling
- Cabling pathways
- Telecommunications outlets and connectors
- Coverage areas

The diversity of ESS services currently available, coupled with the continual addition of new services, means that there may be cases where limitations to desired performance may occur. When applying specific applications to these telecommunications cabling systems, the user is cautioned to consult existing codes, regulations, application standards, equipment manufacturer requirements, and system and service suppliers for applicability, limitations, and ancillary requirements.

5.2 Topology

5.2.1 Star Topology

5.2.1.1 Requirements

The topology for horizontal and backbone cabling shall be configured as a star (horizontal) or hierarchical star (backbone). See Figure 5-1 for an example of a hierarchical star topology.

5.2.1.2 Recommendations

Horizontal cabling topology should be planned to allow the deployment of numerous ESS services within the ICT network. Services and their associated devices include, but are not limited to:

- Surveillance and security cameras
- Access control devices
- Intrusion detection sensors and notification devices
- Fire alarm control panels, sensors, and annunciators
- Other specialty applications (e.g., asset management, mass notification)

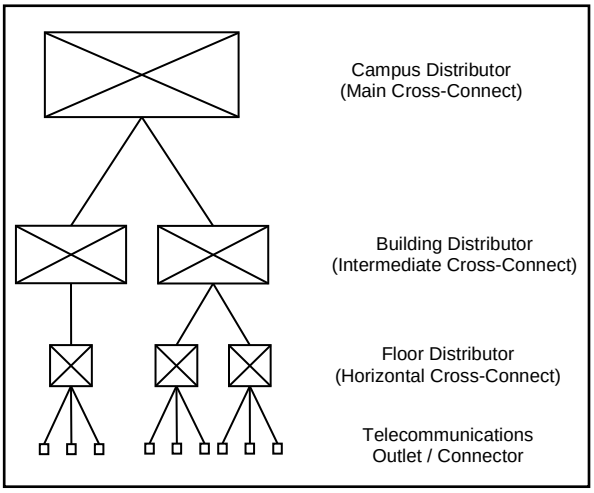

Figure 5-1
Hierarchical Star Topology

5.2.2 Non-Star Topologies

5.2.2.1 Overview

Non-star based topologies may be used in order to accommodate other ICT services and associated cabling infrastructure. For example, ancillary systems cabling from a master control panel to a remote device. Examples of non-star topologies that are commonly used are shown in Figure 5-2.

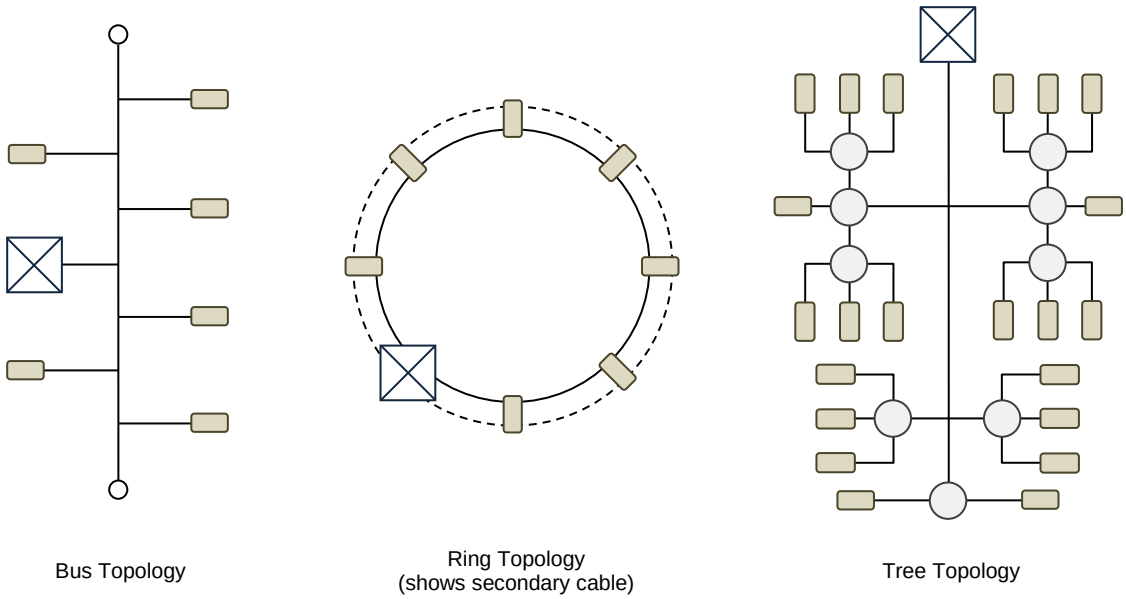

Figure 5-2
Examples of Non-star Topologies

5.3 Spaces

5.3.1 Equipment Rooms

5.3.1.1 Overview

Equipment rooms (ERs) provide connections between ESS equipment and backbone cabling via the campus distributor (main cross-connect) and house electronic equipment to support devices in the building served. Equipment rooms are considered to be distinct from telecommunications rooms because of the nature or complexity of the equipment they contain.

ERs usually house a campus distributor (main cross-connect) or building distributor (intermediate cross-connect). An ER may also house the floor distributor (horizontal cross-connection) intended to connect coverage areas served by the ER. An ER may also serve as the interface point for access or service provider facilities.

5.3.1.2 Equipment Room Size and Provisioning

5.3.1.2.1 Requirements

The design and provisioning of the equipment room shall be in accordance with applicable standards (e.g., TIA-569-D, ISO/IEC 14763-2). The ER shall be able to contain telecommunications equipment, cable terminations, and associated cross-connect cabling.

An ER shall be sized and provisioned (e.g., power, lighting, backboards, pathways) to accommodate enough space for all planned equipment, offering suitable access to the equipment for maintenance and administration, including planned growth based on a five to ten year plan.

ERs shall be climate controlled to help assure proper operation of ESS equipment. This will require the designer to provide the following information to personnel responsible for the engineering or operation of the applicable mechanical systems (e.g. HVAC) supporting the ER, in order to ensure proper operation:

- ESS equipment power and heat loads
- ESS equipment manufacturer/vendor specified operating temperature and humidity ranges and limits

Where dedicated ESS equipment rooms are required, ESS equipment rooms shall be planned to accommodate future expansion on a minimum of one side of the room. Rooms shall be located adjacent to flexible space, also known as soft space (e.g., storage spaces, conference rooms, unassigned coverage areas or other spaces not located within the life safety egress path) to allow for future expansion.

Where ESS equipment is required to share space within an ER or other telecommunications space with components of other building systems, the installation of the ESS equipment and support systems shall:

- Be dedicated to the telecommunications function and related support facilities. Equipment not related to the support of the distributor room (e.g., water pipes, HVAC ductwork, pneumatic tubing) shall not be installed in, pass through, or enter the ER space.
- Comply with the requirements of applicable codes and standards (e.g., NFPA 70) for working space around electrical service equipment.
- Be sized appropriately to accommodate future planned and unplanned adds, moves and changes as the project and client requirements demand.
- Be separated from the other equipment in the ER (e.g., on a separate wall or in a separate equipment rack or cabinet). If ESS equipment shares wall space or equipment rack or cabinet space, ESS equipment shall be clearly labeled as ESS equipment.
- Be designed to incorporate security measures to restrict unauthorized access to the space (e.g., card reader access).

5.3.1.2.2 Recommendations

The ER is the recommended space to install the centralized ESS equipment for the building.

The ER should be located as close as practicable to the center of the area served.

Additional space and pathway sizing should be incorporated into the design to accommodate the ESS cabling systems. Refer to the BICSI *Telecommunications Distribution Methods Manual* for examples of ER designs.

When multiple ERs are located on the same floor, they should be interconnected by a minimum of one metric designator 78 (trade size 3) conduit or equivalent pathway.

The ER should not be shared with electrical installations other than those for telecommunications use. Cross-connect connecting hardware (e.g., patch panels, connecting blocks) intended for use with ESS equipment that is cross-connected to the backbone connecting hardware should be readily and uniquely identifiable (e.g. use of a different color than those used for voice and data interconnections or cross-connections).

Each cross-connect jumper or patch cable should be clearly labeled to identify the ESS equipment it serves. The recommended color codes for cross-connect fields are shown in Table 5-1.

Table 5-1 Recommended Cross-Connect Color Codes For Use at Cabling Distributors

Color	*Pantone Color Number*	*Examples of Services for the Corresponding Colors*
Orange	150C	Public network demarcation point of access provider service
Green	353C	Connections to user side of public network demarcation point
Purple	264C	Common equipment such as private branch exchange and local area networks (LANs), network switches, network servers, network routers and related data equipment
White	N/A	Terminations of building backbone cabling, first level campus or building backbone emanates from the campus distributor (main cross-connect) connecting to a building distributor (intermediate cross-connect) or floor distributor (horizontal cross-connect)
Gray	422C	Terminations of building backbone cabling, second level building backbone emanates from the building distributor (intermediate cross-connect) connecting to a campus distributor (main cross-connect) in one direction and an floor distributor (horizontal cross-connect) in the other direction
Brown	465C	Terminations of campus backbone cabling, second level campus backbone emanates from the building distributor (intermediate cross-connect) connecting to a campus distributor (main cross-connect) in one direction and an floor distributor (horizontal cross-connect) in the other direction
Blue	291C	Terminations of horizontal cabling, from the floor distributor (horizontal cross-connect) connecting to an optional consolidation point and the work area/coverage area serving telecommunications outlets
Yellow	101C	Terminations of cabling serving alarms, security, or energy management systems
Red	N/A	NOTE: Industry practice and the AHJ in some areas reserves red for life safety alarm systems (e.g. fire detection and alarm systems)

Note: Color codes are aligned with standard TIA-606-B, Administration Standard for Telecommunications Infrastructure

5.3.2 Telecommunications Rooms and Telecommunications Enclosures

5.3.2.1 Overview

Telecommunications rooms (TRs) and telecommunications enclosures (TEs) provide connections between backbone cabling and horizontal cabling via the floor distributor (horizontal cross-connect) and houses electronic equipment to support devices in the area served. TRs and TEs are typically environmentally controlled centralized spaces for telecommunications equipment that usually houses a floor distributor (horizontal cross-connect). The TR is typically intended to serve the occupants of a floor in a building. Multiple TRs may be deployed in large buildings or multi-tenant buildings. TEs are typically intended to serve a portion of a floor in a building.

5.3.2.2 Size and Provisioning

5.3.2.2.1 Requirements

A TR is a common access point for cabling subsystems and building pathways. The TR shall be sized to contain telecommunications equipment, cable terminations, and associated cross-connect cabling.

TRs and TEs shall be sized and provisioned (e.g., power, lighting, backboards, pathways) to accommodate enough space for all planned equipment, offering suitable access to the equipment for maintenance and administration, including planned growth based on a five to ten year plan. The TR or TE shall be located as close as practicable to the center of the area served.

The design and provisioning of the telecommunications room or telecommunications enclosure shall be in accordance to applicable standards (e.g., TIA-569-D, ISO/IEC 14763-2). Where ESS equipment is required to share space within a TR, TE or other telecommunications space with components of other building systems, the installation of the ESS equipment and support systems shall:

- Be dedicated to the telecommunications function and related support facilities. Equipment not related to the support of the distributor room (e.g., water pipes, HVAC ductwork, pneumatic tubing) shall not be installed in, pass through, or enter the TR or TE spaces.
- Comply with the requirements of applicable codes and standards (e.g., NFPA 70) for working space around electrical service equipment.
- Be sized appropriately to accommodate adds, moves and changes as the project and client requirements demand.
- Be separated from the other equipment in the TR or TE (i.e., on a separate wall or in a separate equipment rack or cabinet. If ESS equipment shares wall space or equipment rack or cabinet space, ESS equipment shall be clearly labeled as ESS equipment.
- Be designed to incorporate security measures to restrict unauthorized access to the space (e.g., card reader access).

The temperature and humidity of the TRs and TEs shall meet ASHRAE Class B environmental guidelines at a minimum. This may require the provision of climate control if active equipment is located within the TR or TE.

Enclosures installed outdoors shall be selected to meet or exceed the environmental conditions for the particular region. Enclosure design and selection shall accommodate the environmental ranges of the ESS equipment to be installed.

5.3.2.2.2 Recommendations

The size of the TR should accommodate at least 50% more space than a TR intended to serve only voice and data networking applications. Increasing the scale of the TR space allows for a parallel network and future device connections to the network.

Where dedicated ESS telecommunications rooms or telecommunications enclosures are required, ESS equipment rooms should be planned to accommodate future expansion. Rooms should be located to allow for future expansion.

Additional space and pathway sizing should be incorporated into the design to accommodate the ESS cabling systems. Refer to the BICSI *Telecommunications Distribution Methods Manual* for example TR and TE designs.

The TR should be located on the same floor as the area served. When multiple TRs or TEs are located on the same floor, they should be interconnected by a minimum of one metric designator 78 (trade size 3) conduit or equivalent pathway.

The TR or TE should not be shared with electrical installations other than those for telecommunications use.

Cross-connect connecting hardware (e.g., patch panels, connecting blocks) intended for use with ESS equipment that is cross-connected to the backbone connecting hardware should be readily and uniquely identifiable (e.g. use of a different color than those used for voice and data interconnections or cross-connections).

Each cross-connect jumper or patch cable should be clearly labeled to identify the ESS equipment it serves. The recommended color codes for cross-connect fields are shown in Table 5-1.

All TRs should have access to two horizontal cabling pathways on a minimum of two walls.

5.4 Cabling

5.4.1 Backbone Cabling

5.4.1.1 Overview

Backbone cabling facilitates interconnections between the telecommunications rooms or telecommunications enclosures, equipment rooms, and entrance facilities, whether for one building or a campus. The life span of the backbone is dependent on the service requirement level of the facility and ensuing changes of the telecommunications equipment and applications.

5.4.1.2 Recognized Backbone Cabling

5.4.1.2.1 Requirements

Backbone cabling installed within a building shall follow the requirements specified in applicable standards (e.g., TIA-568-D series, ISO/IEC 11801-1). The following media types are recognized for use in the backbone cabling infrastructure:

- 4-pair 100-ohm balanced twisted-pair cabling (e.g., TIA-568-C.2, ISO/IEC 11801-1) Category 5e/Class D or higher. It is recommended to use Category 6/Class E or higher cabling in new installations.
- Multi-pair 100-ohm balanced twisted-pair cabling (e.g., TIA-568-C.2, ISO/IEC 11801-1) Category 3/Class C or higher.
- Multimode optical fiber cabling (e.g., TIA-568-C.3, ISO/IEC 11801-1) 50 micron OM3 minimum. 50 micron OM4 is recommended.
- Singlemode optical fiber cabling (e.g., TIA-568-C.3, ISO/IEC 11801-1) OS1 or OS2 singlemode cabling.

Backbone cabling installed outdoors in a campus environment shall follow the requirements specified in applicable standards (e.g., TIA-758-B, ISO/IEC 11801-1).

5.4.1.2.2 Recommendations

Backbone cabling design should accommodate a variety of systems that may be deployed using these media. For example, the use of singlemode optical fiber backbone cabling may be an optimal solution when deploying both a 10 Gigabit Ethernet system for a data (e.g., voice, video) network as well as Ethernet switches for an ESS system.

For each installed ESS service (e.g., security, access control, fire-life-safety):

- Separate backbone cabling for each ESS service should be provided.
- Backbone cabling for each service should be placed in a separate pathway.
- Redundant backbone cabling (as applicable) should be placed in a physically diverse pathway.

While ESS services may share the same backbone as the data and voice network, the applicable AHJ may have requirements restricting or prohibiting this practice.

Designs for backbone cabling should accommodate projected system and application expansion, as well as increases in utilization and bandwidth capacity for a life cycle of at least ten years past the commissioning date.

It may be necessary to use more than one medium in the backbone cabling, depending on distance and application.

Refer to the BICSI *Outside Plant Design Reference Manual* for additional recommendations and information for campus environments.

5.4.2 Horizontal Cabling

5.4.2.1 Overview

The horizontal cabling is the portion of the telecommunications cabling system that extends from the mechanical termination in the telecommunications outlet to the horizontal cross-connect in the TR or TE.

Horizontal cabling includes:

- Horizontal cable
- Mechanical terminations,
- Equipment cords, patch cords, or optical fiber jumpers
- Consolidation points (optional)

5.4.2.2 Recognized Horizontal Cabling

5.4.2.2.1 Introduction

Horizontal cabling selection is typically based on device location, distance from the serving TR or TE, anticipated lifetime of building occupancy and device required transmission performance characteristics. The distance that an ESS signal may be run is determined by the:

- Signal strength at the source,
- Required signal strength at the receiving end, and
- Signal loss over the distance of the cable run.

5.4.2.2.2 Requirements

Horizontal cabling installed in a premise shall follow all applicable standards requirements and recommendations (e.g., TIA-568-D series, ISO/IEC 11801-1). The following media types are recognized for use in the horizontal cabling infrastructure:

- 4-pair 100-ohm balanced twisted-pair cabling (e.g., TIA-568-C.2, ISO/IEC 11801-1) Category 5e/Class D or higher. It is recommended to use Category 6/Class E or higher cabling in new installations.
- Multimode optical fiber cabling (e.g., TIA-568-C.3, ISO/IEC 11801-1) 50 micron OM3 minimum. 50 micron OM4 is recommended.
- Singlemode optical fiber cabling (e.g., TIA-568-C.3, ISO/IEC 11801-1) OS1 or OS2 singlemode cabling.

Horizontal cabling installed outdoors in a campus environment, shall follow the standards requirements and recommendations as defined in applicable standards (e.g., TIA-758-B, ISO/IEC 11801-1).

5.4.2.2.3 Recommendations

Horizontal cabling should be designed to accommodate future equipment needs, which includes moving from proprietary analog-based systems to IP-based systems.

Table 5-2 provides a guideline for media selection, based on criteria from various cabling standards (e.g., TIA-568.0-D, ISO/IEC 11801-1):

Refer to the BICSI *Outside Plant Design Reference Manual* for additional recommendations and information for horizontal cabling to be installed outdoors.

Table 5-2 Media Selection Criteria

IP-enabled ESS Device	*Maximum Distance*	*Bandwidth*	*Power Source*[1]	*Recommended Minimum Media*
Analog	<= 100 m (328 ft)	1-100 MHz	Local or PoE	Category 5e/Class D
Analog[2]	> 100 m (328 ft)	1-250 MHz	Local or powered baluns[3]	Category 6/Class E
IP	<= 100 m (328 ft)	1-250 MHz	Local or PoE	Category 6/Class E
IP	<= 100 m (328 ft)	1-500 MHz	Local or PoE	Category 6A/Class E_A
IP	<= 100 m (328 ft)	1-600 MHz	Local or PoE	Category 7/Class F
IP	<= 100 m (328 ft)	1-1000 MHz	Local or PoE	Category 7_A/Class F_A
IP	<= 2000 m (6,500 ft)	2000 MHz•km (OM3)	Local or PoE with media converters	Multimode Optical Fiber[4]
IP	<= 2000 m (6,500 ft)	4700 MHz•km (OM4)	Local or PoE with media converters	Multimode Optical Fiber[4]
IP	<= 5000 m (16,400 ft)	Not Applicable	Local or PoE with media converters	Singlemode Optical Fiber (e.g., OS1, OS2)

Notes:
1. This table does not include all power sources, such as PoE+ (e.g., IEEE 802.3at-2009).
2. Analog cameras at distances further than 100 m (328 ft) shall not be used as future IP devices, due to Ethernet distance limitation restrictions (e.g., TIA-568.1-D).
3. Powered baluns are subject to voltage loss.
4. Type of multimode optical fiber cable used may be affected by final design and system requirements (See Section 5.4).

5.4.2.3 Balanced Twisted-pair Cabling Use Guidelines

5.4.2.3.1 Recommendations

Balanced twisted-pair cabling is preferred for distances of 100 meters (328 ft) or less. Table 5-3 offers a list of balanced twisted-pair cabling categories/classes, their frequency range of interest, and associated applications.

When installing balanced twisted-pair cabling, it is recommended to install Category 6/Class E or higher for powering higher current PoE or PoE Plus devices.

Table 5-3 Balanced Twisted-Pair Cabling Frequency Range of Interest and Associated Applications

Category / Class of Cabling	*Frequency Range of Interest*	*Associated Applications*	*Notes/Standards*
Category 3 / Class C	1-16 MHz	IEEE transmission protocols up to 10BASE-T Ethernet	Multipair cabling and 4-pair cabling, shielded and unshielded. Not recommended for new installations.
Category 5e / Class D	1-100 MHz	IEEE transmission protocols up to 1000BASE-T Ethernet	Multipair cabling and 4-pair cabling, shielded and unshielded. Not recommended for new installations.
Category 6 / Class E	1-250 MHz	IEEE transmission protocols up to 1000BASE-T Ethernet	Most commonly installed cabling. 4-pair cabling, shielded and unshielded.[1]
Category 6A / Class E_A	1-500 MHz	IEEE transmission protocols up to 10GBASE-T Ethernet	Augmented Category 6, 4-pair cabling, shielded and unshielded.[1]
Category 7 / Class F	1-600 MHz	IEEE transmission protocols up to 10GBASE-T Ethernet	4-pair shielded cabling, overall braid screen with individually foil shielded twisted-pairs (S/FTP). Also available in 4-pair shielded cabling, overall foil shield with individually foil shielded twisted-pairs (F/FTP).[2]
Category 7_A / Class F_A	1-1000 MHz	IEEE transmission protocols up to 10GBASE-T Ethernet. Features bandwidth to support high definition broadband transmissions	4-pair shielded cabling, overall braid screen with individually foil shielded twisted-pairs (S/FTP). Also available in 4-pair shielded cabling, overall foil shield with individually foil shielded twisted-pairs (F/FTP).[2]

Notes:
1. Referenced by multiple standards (e.g., TIA-568-C.2, ISO/IEC 11801-1)
2. Referenced by multiple standards (e.g., EN 50173-1, ISO/IEC 11801-1)

5.4.2.4 Optical Fiber Cabling Use Guidelines

5.4.2.4.1 Overview

Optical fiber cabling offers the ability to transmit data over greater distances than either coaxial or balanced twisted-pair cabling. Additionally, optical fiber cabling is widely used for outdoor applications due to its inherent immunity to lightning and other transient electromagnetic phenomena.

5.4.2.5 Media Converter Application Notes

5.4.2.5.1 Overview

Media converters will need to be installed between the end device and optical fiber cabling if the device is not equipped with an optical fiber transceiver. Figure 5-3 provides an example of the use of media converters for connecting optical fiber cabling links with balanced twisted-pair equipment cords.

Factors in determining which optical fiber cable to use for a given application are:

- The type of active equipment
- The distance between the two points to be served
- Applicable bandwidth (data rates) requirements

The application may also affect which electronics and passive equipment are available or required to be used.

5.4.2.6 Hybrid Cabling

5.4.2.6.1 Overview

A hybrid cable is a cable that contains two or more different transmission media within a common cable sheath or jacket. Examples of differing transmission media within a common sheath include:

- Different types of balanced twisted-pair cable (e.g., Category 5e and 6_A)
- Different multimode classes of optical fiber (e.g., OM3 and OM4)
- A balanced twisted-pair cable and a coaxial cable
- Differing styles of optical fiber cable (e.g., tight buffered and ribbon)
- Optical fiber cable and balanced twisted-pair cable
- Optical fiber cable and copper conductors (stranded or solid core conductor used for electrical power transmission)

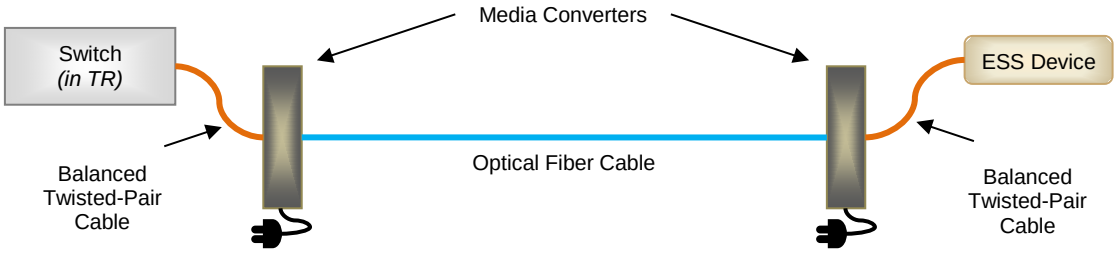

Figure 5-3
Optical Fiber Cabling With Media Converters

5.4.2.6.2 Configuration

5.4.2.6.2.1 Introduction

Three common configurations for using a copper/optical fiber hybrid cable to connect an ESS device are shown in Figure 5-4. These are presented to provide an example of the concept, as requirements from the site, end-user, or AHJ may affect the final acceptability and configuration of components.

Power is supplied to the copper conductors through either a powered media converter or a separate power sourcing equipment (PSE). At the far end of the cable, a passive media converter converts the signals from the optical fiber cable to a balanced twisted-pair cable.

5.4.2.6.2.2 Requirements

Use of hybrid cables and the method of sheath sharing shall conform to the requirements of local codes, regulations and the AHJ.

5.4.2.6.2.3 Recommendations

The supplied voltage to ESS equipment should be within the manufacturers recommended range. Copper conductors for power should be sized to the load of the ESS equipment, accounting for voltage loss due to the overall length of the conductors.

NOTE: Increasing the size of the conductors is a method to overcome voltage loss due to the length of the conductors.

Classes of cables for remote-control, signaling, and power-limited cabling may be defined in codes and standards (e.g., NFPA 70).

5.4.2.7 Coaxial Cabling

5.4.2.7.1 Recommendations

While coaxial cabling has been and may be used for analog video systems, it is not recommended for new installations. When installing IP cameras that utilize a coaxial-based cabling system, media converters, or baluns should be used to convert the signal for transmission over a recognized cabling media.

5.4.2.8 Physical Security

5.4.2.8.1 Recommendations

For additional physical layer security for horizontal cabling, see standards such as TIA 5017.

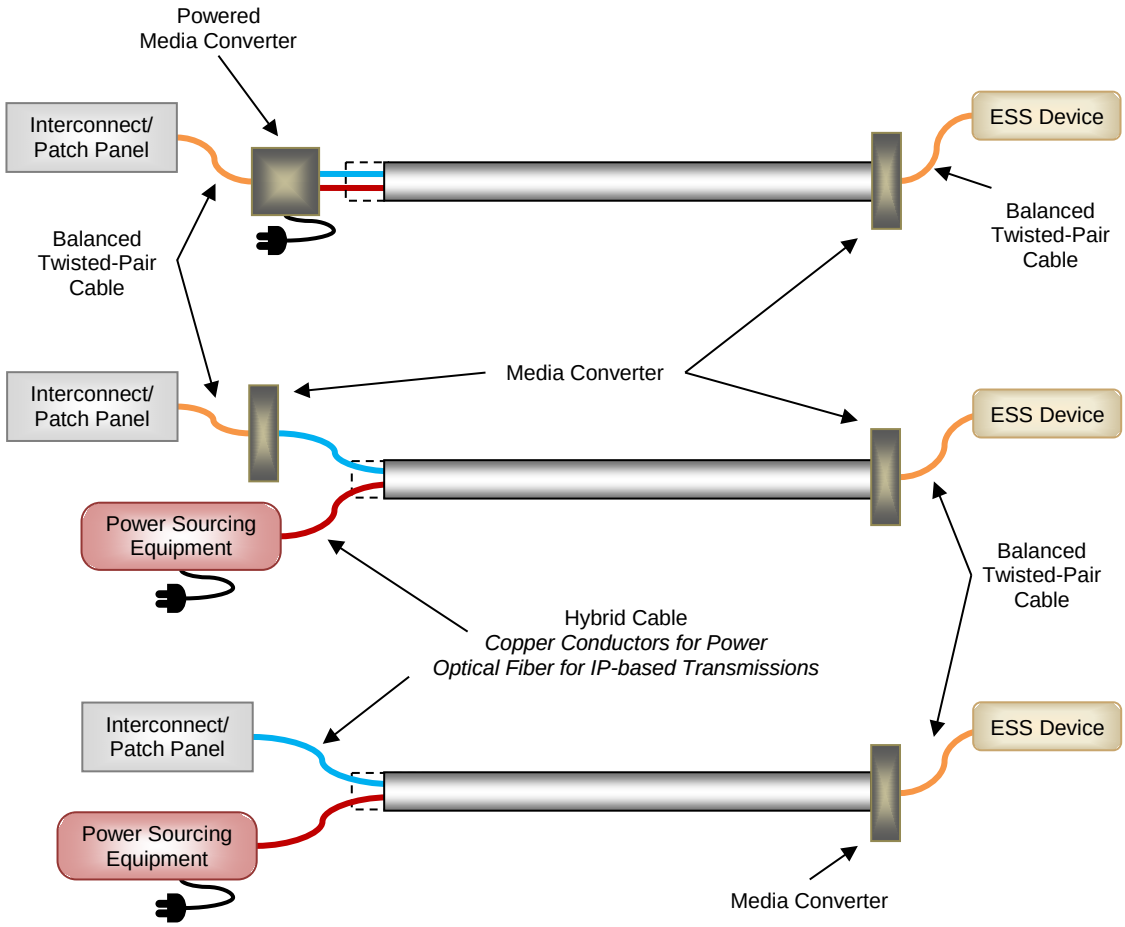

Figure 5-4
Configuration Examples for Using Hybrid Copper/Optical Fiber Cable to Connect an ESS Device

5.4.3 Horizontal Connection Point (HCP)

5.4.3.1 Introduction

An HCP allows coverage area connections to be reconfigured. See Figure 5-5.

5.4.3.2 Requirements

No more than one HCP shall be placed in a single cabling subsystem (e.g., horizontal link). Each cable extending from the HCP shall be terminated directly to an ESS device or to an equipment outlet. Cross-connections are allowed in the HCP. When cross-connections are used at the HCP, an equipment outlet shall not be installed as part of the horizontal cabling subsystem. This requirement ensures that the horizontal cabling channel contains no more than four (4) connections.

HCPs shall be located in fully accessible, permanent locations such as building columns and permanent walls. HCPs shall not be located in any obstructed area, and shall not be installed in furniture systems unless that unit of furniture is permanently secured to the building structure. In all cases the use of HCPs in plenum spaces used for environmental air shall conform to applicable building codes.

HCPs shall be administered in the same manner as telecommunications cabling, connecting hardware, pathways, and spaces as specified in applicable standards (e.g., TIA-606-B, ISO/IEC 14763-2).

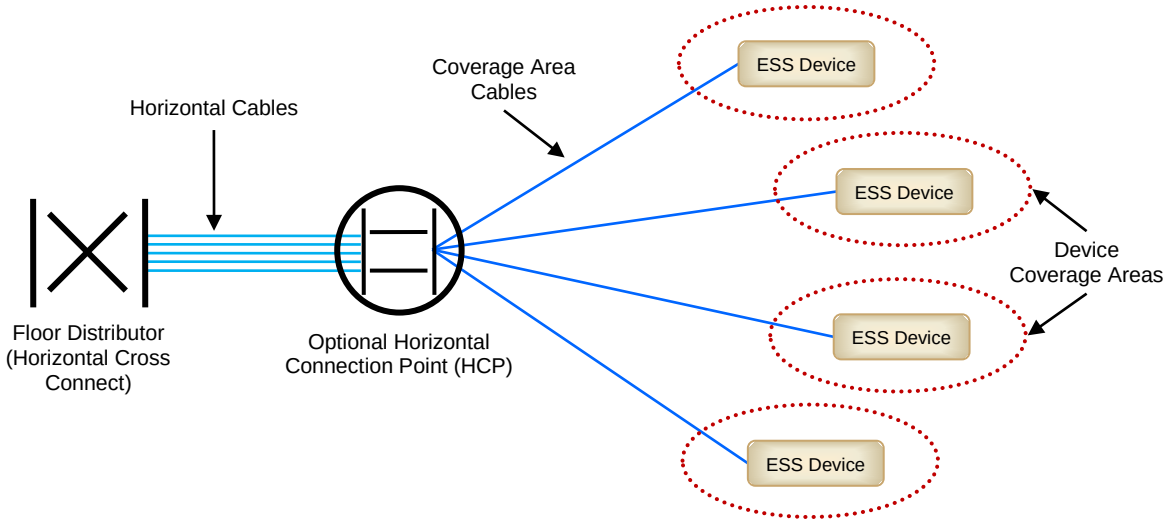

Figure 5-5
Example of a Horizontal Connection Point Within a Star Topology

5.4.3.3 Recommendations

HCP design, including location, should be developed in accordance with the security plan of the building.

The HCP should be readily accessible and its location visibly marked allowing for ease of routine maintenance and reconfiguration. For balanced twisted-pair cabling, in order to reduce the effect of multiple connections in close proximity on near end crosstalk (NEXT) loss and return loss, the HCP should be located at least 15 m (50 ft) from the distributor located in the TR or TE.

The use of suspended ceiling space or access floor space for HCPs may be acceptable, provided that the space is accessible without moving building fixtures, and it is reasonable to assume such space will continue to be in an open space such as a corridor or hallway.

When an equipment outlet is used, the HCP is optional. In this case, from an architectural perspective, the HCP is to ESS or BAS cabling what the consolidation point is to commercial building cabling (e.g., TIA-568.1-D).

The functions of a consolidation point and an HCP can be combined within the same zone box. The number of links served by an HCP should be limited to twelve (12). HCP design will depend on the number of coverage areas served.

NOTE: Spare capacity for future expansion should be considered when determining the size of the HCP.

5.4.4 Power over Ethernet (PoE)

5.4.4.1 Introduction

PoE is a technology that integrates transmitting DC power with data using a structured cabling infrastructure.

NOTE: When optical fiber cabling is used, the power cannot transmit over the fiber itself, rather the signal is transmitted over the optical fiber. At some point, the transmission medium is converted to balanced twisted-pair using media converters where power may then be injected into the available copper medium.

IEEE 802.3 defines both the standard PoE power sources to be used with Ethernet standard-based products, as well as the Power over Ethernet Plus (PoE +) specification which provides capabilities up to 25.5 W. IEEE 802.3bt DTE Power via MDI over 4-Pair will deliver at least 49W is an approved project objective and is expected to be an approved standard in April 2017. HDBaseT, a standard for delivery of uncompressed high definition video, audio, control and power developed by the HDBaseT alliance provides up to 100W of power.

CAUTION: Not all remote powering equipment complies with IEEE 802.3 or HDBase-T standards. Non-compliant equipment providing higher than standardized power levels may increase cable temperatures. Overheating the cable beyond its temperature rating may affect the ability of the cable to transmit data.

5.4.4.2 Requirements

PoE cabling implementations shall conform to the requirements of local codes, regulations and the AHJ, both for the premises and the application being served.

A minimum of one dedicated horizontal cabling link shall be provided for each distinct ESS service.

5.4.4.3 Recommendations

PoE provides power up to 15.4 W on the switch or midspan side, which translates to a maximum power consumption of 12.9 W on the device/camera side – making it suitable for most fixed indoor cameras. PoE+ can power a wide range of powered devices (e.g., PTZ cameras, wireless access points and newer emerging applications) over existing Category 5e/Class D and higher performing cabling.

Cable bundle size for PoE depends on the power level, cable type (e.g., conductor size, construction), and the installation condition (e.g., air, plastic conduit, EMT conduit). See TIA TSB-184-A for further details.

5.5 Cabling Pathways

5.5.1 Requirements

All applicable codes, standards (e.g., TIA 568.1-D, TIA 569-D, ISO/IEC 14763-2) and requirements of the AHJ shall be met. Appendix A of this standard provides a summary of many of the general requirements for specific types of pathways and is considered a normative part of this standard. Additional requirements specific to pathways for ESS applications are presented in the following sections.

NOTE: Appendix A also contains recommendations and additional information for pathways, which may be treated as optional or non-binding.

Each pathway shall be evaluated for risk prior to selecting the means and methods for installing pathway systems.

5.5.2 Enclosures, Pull Boxes and Splice Boxes

5.5.2.1 Requirements

The following requirements apply to the design of ESS enclosures, pull boxes and splice boxes:

- Pull boxes and splice boxes shall be sized in accordance with applicable codes, standards and regulations.
- Covers for pull boxes larger than 0.5 m^2 (5 ft^2) shall be hinged.
- Pull boxes and splice boxes shall not be labeled indicating that they contain ESS cabling or equipment.
- If locking boxes are required during maintenance, a key control plan shall be provided prior to installation.
- Consider providing mechanical tamper switches for enclosures and fittings with covers in high security areas.
- Enclosures exposed to weather shall be corrosion resistant and meet applicable site specifications for resistance to moisture and dust entry.

  NOTE: See standards, such as NEMA 250, *Enclosures for Electrical Equipment (1000 Volts Maximum)* and IEC 60529, *Degrees of protection provided by enclosures (IP Code)*, for more information concerning moisture and dust ingress ratings of enclosures.
- Penetrations of enclosures shall maintain and not reduce the designated enclosure rating (i.e. IP or NEMA classification)
- Outdoor enclosure penetrations shall be sealed with a sealant approved by the cable manufacturer to prevent moisture from entering.

5.5.3 ESS Pathway Redundancy

5.5.3.1 Introduction

Properly implemented ESS systems help to assure the protection of people and property. Redundant ESS pathway designs offer some accommodation in case of catastrophic failures that may occur along the route of one of the ESS pathways.

5.5.3.2 Recommendations

When diverse ESS pathways are developed, they should be separated from each other by sufficient distance to ensure that they are not vulnerable to a single outage event. Wherever possible, they should not pass through the same telecommunications space containing ESS infrastructure.

5.5.4 ESS Pathways between Telecommunications Spaces within a Building

5.5.4.1 Introduction

ESS pathways between telecommunications spaces may be intended for single-tenant occupancy or multi-tenant occupancy floors in buildings. In some multi-tenant occupancy floor environments, an individual tenant's ESS infrastructure requirements may exceed the load and fill capacity of multi-tenant common use pathways or spaces of a floor in a building. A tenant may want to keep their cabling physically separate from the common pathways and spaces used by other tenants in the multi-tenant building. This is sometimes referred to as "bypassing" in multi-tenant buildings. When this type of separation occurs, there is a resulting reduction in the multi-tenant building's common pathways and spaces. As the quantity of bypassing tenants increases, so too does the need for a building's common

pathways and spaces to decrease. Without careful management, tenant bypass can effectively exhaust a multi-tenant building's fixed and limited pathways and spaces.

5.5.4.2 Requirements

The placement, number, and size of sleeves, slots or conduits to be used shall be determined in conjunction with ICT personnel.

5.5.4.3 Recommendations

When multiple telecommunications spaces are located on the same floor, they should be interconnected by a minimum of one metric designator 78 (trade size 3) conduit or equivalent pathway. These recommendations apply to single-tenant occupancy and multi-tenant occupancy floors in buildings.

5.5.5 ESS Campus Pathways Between Buildings

5.5.5.1 Requirements

ESS campus pathways shall meet the requirements of applicable codes and standards. Where a conduit containing ESS cabling is to be placed to a device exposed to the weather, care shall be taken to prevent the ingress of moisture, dirt or other objectionable materials. Care shall also be taken to ensure that moisture will not collect in low points, which may freeze in some climates and damage the ESS cabling. Nonmetallic conduit shall be UV resistant and marked accordingly.

NOTE: Refer to the BICSI *Outside Plant Design Reference Manual* for recommendations and information.

5.5.6 ESS Pathways Serving Equipment Outlets

5.5.6.1 Introduction

Cabling system performance is sensitive to the arrangement of slack cable behind the equipment outlet. The following requirements and recommendations offer cautionary guidance for the design and installation of cabling infrastructure associated with ESS pathways.

5.5.6.2 Requirements

Sufficient space shall be provided so that cable bend radius requirements are not violated in equipment outlet termination spaces. See Tables A1 and A2, located in Appendix A, for cabling bend radius requirements.

5.5.6.3 Recommendations

The location, mounting, and strain relief of the equipment outlet should allow pathway covers and trim to be removed without disturbing the cable termination. Equipment outlets should be mounted in such a way that they do not reduce the required pathway cabling capacity.

5.5.7 ESS Pathway Separation from Power and EMI Sources

5.5.7.1 Introduction

Co-installation of telecommunications cabling and power cabling is governed by applicable electrical codes for safety. Consult with the AHJ for local compliance.

5.5.7.2 Requirements

The separation guidelines offered by applicable codes, standards and regulations and enforced by the AHJ shall be followed. Several examples of applicable codes and standards that offer separation guidelines include:

- BS 6701, *Telecommunications equipment and telecommunications cabling. Specification for installation, operation and maintenance*
- BS 7671, *Requirements for Electrical Installations. IET Wiring Regulations*
- EN 50174-2, *Information technology – Cabling installation – Part 2: Installation planning and practices inside buildings*
- IEC 60364-5-52, *Electrical installations of buildings – Part 5-52: Selection and erection of electrical equipment – Wiring systems*
- ISO/IEC 11801-1, *Generic cabling for customer premises – Part 1: General requirements*
- NFPA 70®, *National Electrical Code®*
- ANSI/TIA-569-D, *Telecommunications Pathways and Spaces*
- ANSI/TIA-1005-A, *Telecommunications Infrastructure Standard for Industrial Premises*

5.5.8 ESS Pathway Bonding and Grounding

5.5.8.1 Requirements

Pathways utilized for ESS cabling shall meet all bonding and grounding requirements of applicable codes, the AHJ, and applicable standards (e.g., TIA-607-C, NECA/BICSI-607, IEC 60364-4-43, ISO/IEC 30129).

5.5.9 Special Pathways and Spaces Considerations

5.5.9.1 Requirements

The AHJ shall be consulted before designing systems within areas which have additional requirements due to codes, environmental factors, intended use, or other factors not listed here. Typical areas with additional requirements include:

- *Seismic requirements* – Codes, regulations and the AHJ may have specific operational parameters that designs must address and may require or prohibit the use of specific installation methods.
- *Hazardous (Classified) environments* – Depending on the classification of the environment, additional measures, such as conduit seal or explosion proof apparatus may be required. Review of codes, regulations and AHJ requirements shall be accomplished to satisfy local requirements.
- *Existing conditions* – Surface mounted raceway, other types of compliant cabling pathways or other accommodations required when installing ESS cabling in existing structures with limited or no existing cabling pathways.
- *Healthcare facilities* – Compliance with codes, standards and regulations (e.g., NFPA 99, Americans with Disabilities Act*)* pertaining to healthcare facilities, patient and information privacy, and public access is required.
- *Corrosion/corrosive environments* – All metallic cabling pathways (e.g., conduits, hangers and supports) shall contain corrosion protection or be resistant to corrosion when used in pathways installed in corrosive atmospheres.
- *Wet and damp locations* – When metallic cabling pathways are installed in outdoor and indoor locations that may be considered to be wet or damp, appropriate cabling and metallic cabling pathway types shall be selected for use in these environments.

5.5.9.2 Recommendations

Additional special pathways and spaces considerations include:

- Environmental
  - *EMI* – Electromagnetic interference can disrupt signaling. Shielded cabling or metallic pathways may reduce the effects of EMI.
- Architectural
  - *Space* – New construction pathways should be coordinated with other trades in new construction. Building information modeling (BIM) models should be used for this purpose.
  - *Existing conditions* – Surface mounted raceway, other compliant cabling pathways or other accommodations that are used when installing ESS cabling in existing structures with limited or no existing cabling pathways.
- Building Function
  - *Security / Sensitive information* – Physical protection of ESS pathways and spaces should be considered to deter or prevent the ESS systems from being accessed or compromised by unauthorized personnel.
  - *Places of assembly* – In theaters, carnivals and fairs, due to the presence of large groups of people, AHJ may have design or installation method restrictions so that systems do not jeopardize the safety of occupants.
  - *Agricultural buildings* – Special considerations for bonding and grounding may be necessary to protect animals from stray voltages.

5.5.10 Secure Areas

5.5.10.1 Overview

Governments, military organizations, and other entities with critical facilities (e.g., data centers, healthcare, emergency services) handle sensitive and classified material over secure networks, which are located in areas most commonly referred to as secure areas.

Occasionally, telecommunications cabling for secured areas needs to be routed outside of the secured area. (e.g., backbone connection between two physically separated secured areas).

While there are different types of pathways that may be used, allowed pathways for secure area applications are collectively known as protected distribution systems (PDSs). PDSs protect sensitive cabling from unauthorized access outside of secure areas by enclosing the cabling in a sealed raceway or conduit system.

5.5.10.2 Requirements

Where not otherwise specified, cabling containing sensitive or classified information outside of a secure area shall be placed in metallic conduit per applicable standards (e.g., TIA-5017).

5.5.10.3 Recommendations

Facilities with defined secure areas will typically have their own set of guidelines for PDS construction. The designer should check with the organization requiring the system for their particular guidelines.

PDSs should be located in common areas where they can be inspected on a regular basis, for unauthorized access. Routing a PDS through a locked or seldom used area is not recommended. See TIA-5017 for other measures that can be taken to improve the physical network security of telecommunications cabling infrastructure.

Within secure areas, the following recommendations are applicable for the design and selection of ESS enclosures, pull boxes and splice boxes:

- Enclosures made from metal or similar materials that provide high strength, durability and tamper resistance should be used.
- Where permitted by the AHJ and where damage or degradation to the interior wiring/cabling and components will not occur as a result, “tack” or temporarily weld enclosures and fitting covers that are not needed for maintenance access.
- Use mechanical tamper switches for enclosures and fittings with covers.
- It may be necessary to consider the use of mechanical (key or combination) or electrical (keypad or card) locksets on enclosures containing equipment in “high security” areas.
- High security access points should be alarmed, monitored by remote cameras, or both.

5.6 Telecommunications Outlet and Connectors

5.6.1 Overview

Telecommunications outlet and connectors provide the ability to easily connect equipment (e.g., computer, phone, security camera, wireless access point) to the telecommunications cabling system. The most prevalent example is the wall mounted connector (receptacle) in which a cable is inserted. Within ESS applications, telecommunications outlets may be located in a wider variety of areas and spaces, to support cameras, sensors, readers, and other related ESS devices.

The use of telecommunications outlets can be defined into the following two categories:

- User administered
- Non-user administered, also known as a facility connection

A user-administered connection is designed primarily in an office environment where the end device is administered by the user (e.g., computer, telephone). In comparison, once an ESS device is installed, it becomes part of the facility and is relatively permanent. Figure 5-6 illustrates typical locations of user-administered and facility connections.

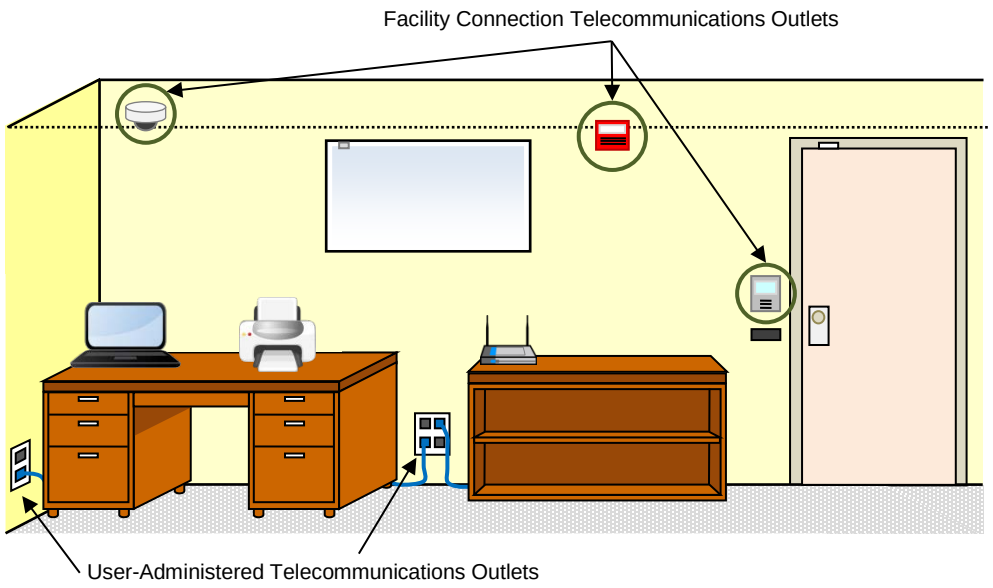

Figure 5-6
Example Locations of User-Administered and Facility Connection Telecommunications Outlets

5.6.2 Facility Connections by Modified Permanent Link Method

5.6.2.1 Overview

In these IP applications that extend outside the voice and data scope, there are circumstances that do not allow a jack-to-outlet scenario on the device end. Standards for these applications recognize these circumstances and allow the elimination of a workstation outlet and equipment cord at the device end. See Figure 5-7 for examples of facility connections using a modified permanent link.

5.6.2.2 Requirements

Facility connections shall be tested and meet the requirements of applicable standards (e.g., TIA-568-D Series, TIA-862-B, ISO/IEC 11801-1, ISO/IEC 14763-2) as well as Section 5.7 of this standard.

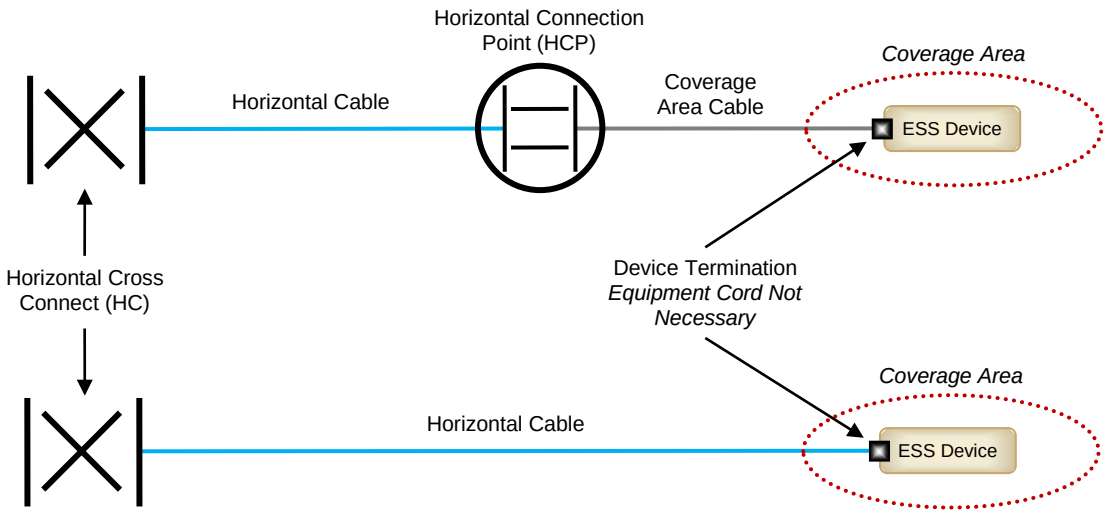

Figure 5-7
Examples of Facility Connections Using a Modified Permanent Link

5.6.2.3 Recommendations

The modified permanent link method is acceptable in the following scenarios:

- In plenum spaces where the outlet or equipment cord are not plenum rated
- Where there is no room for a workstation outlet or equipment cord assembly
- Where it is not safe or secure for an exposed outlet or equipment cord assembly to be installed
- When the customer deems it is not aesthetically pleasing with the design of the facility
- When the ESS cable is enclosed in conduit and the conduit system is directly attached to the ESS equipment (e.g., IP outdoor camera)
- Where acceptable to the AHJ
- Where its use will not result in mechanical failure of the cable (e.g., repeated motion of a PTZ camera)

5.7 Cabling Installation Requirements

5.7.1 Overview

This section applies to the installation of all forms of recognized cable and connecting hardware including:

- Optical fiber cabling
- Balanced twisted-pair cabling
- Coaxial cabling

5.7.1.1 Requirements

Cabling installation shall conform to applicable standards (e.g., TIA-568-D Series, ISO/IEC 11801-1).

5.7.1.2 Recommendations

Cabling installation should conform to global best practices (e.g., BICSI *Information Technology Systems Installation Methods Manual*).

5.7.2 Bonding and Grounding Considerations

5.7.2.1 Requirements

Bonding and grounding shall meet the requirements and practices of the AHJ. In addition, the building telecommunications bonding and grounding system shall conform to applicable standards (e.g., TIA-607-C, NECA/BICSI 607, ISO/IEC 30129) requirements. Adherence to cable manufacturers' bonding and grounding requirements shall be followed when installing shielded cabling systems.

5.7.3 Transmission Performance Field Testing

5.7.3.1 Introduction

Field testing of installed cabling is typically conducted after balanced twisted-pair and optical fiber cabling links are installed. These cabling links may be pre-terminated or field terminated.

5.7.3.1.1 Requirements

All installed cabling (e.g., balanced twisted-pair, optical fiber, coaxial cabling), shall be measured with the appropriate field-test instrument, in accordance with applicable standards. All installed cabling shall meet the field-test measurement requirements of applicable standards (e.g., TIA 526-7-A, TIA-526-14-C, TIA-568-C.2, ISO/IEC 14763-2).

Field test instruments used to test installed balanced twisted-pair cabling shall meet the requirements of TIA-1152-A or equivalent standards.

5.7.3.1.2 Recommendations

In a modified permanent link connection utilizing Category 5e/Class D or higher cabling, a single connector modified permanent link configuration should be measured.

5.7.3.2 Field Test Configurations

5.7.3.2.1 Recommendations

The following field test configurations are recommended for Category 5e/Class D and higher cabling for a single connector modified permanent link (Reference UL File E349672, Project 11CA44391). Following are the two field test configuration models.

Configuration 1 – Single connector modified permanent link set up for a modified permanent link without consolidation point

A fixed length of horizontal cabling terminated to a randomly selected port of the near end patch panel and an eight position modular plug on the work area/device far end. The field-test instrument shall be fitted with the permanent link adapter on the near end and a channel adapter on the work area plug far end. (See Figure 5-8)

Configuration 2 – Single connector modified permanent link set up for a modified permanent link with consolidation point

A fixed length of horizontal cabling terminated to a randomly selected port of the near end patch panel with an optional consolidation point connector in close proximity to an eight position modular plug on the work area/device far end. The field-test instrument shall be fitted with the permanent link adapter on the near end and a channel adapter on the work area plug far end. (See Figure 5-9)

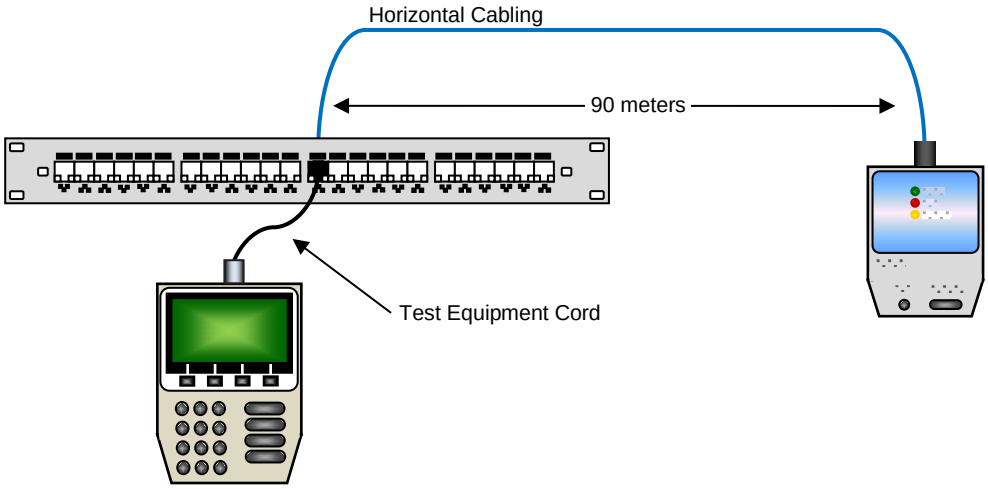

Figure 5-8
Configuration 1: Single Connector Modified Permanent Link Set Up for a Modified Permanent Link Without a Consolidation Point

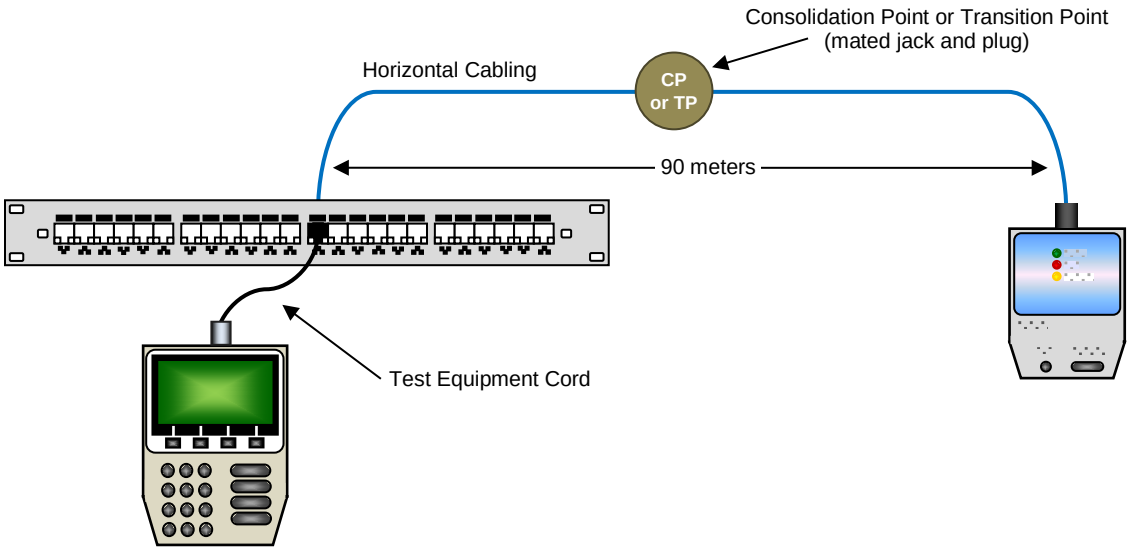

Figure 5-9
Configuration 2: Single Connector Modified Permanent Link Set Up for a Modified Permanent Link With a Consolidation Point

5.8 Administration and Documentation

5.8.1 Requirements

ESS administration shall comply with applicable administration standards (e.g., TIA-606-B, ISO/IEC 14763-2, ISO/IEC 18598).

All applicable documentation, including accurate drawings, applicable to the work performed shall be provided by the installer upon work completion.

5.8.2 Recommendations

The use of automated infrastructure management systems should be considered for those portions of the network including:

- Patch panel ports
- Patch cords
- Horizontal cabling
- Coverage area connectivity (outlet and equipment cords, if installed)
- Backbone cabling

5.9 ESS Device Mounting Heights

5.9.1 Requirements

Mounting heights shall conform to applicable codes and standards as applied by the AHJ. The following criteria shall apply:

- Special accommodations provided for the occupants of the facility shall be incorporated into the specifications and installations of device mounting heights.
- Codes and regulations (e.g. ADA) may determine minimum and maximum mounting heights.

Installation of ESS device boxes shall be coordinated with other devices trades (e.g., electrical, mechanical) including drywall.

5.9.2 Recommendations

Codes may only provide minimum and maximum mounting height. When mounting heights are not specified, convenience of users should be considered when determining mounting height including users with disabilities.

Typical mounting heights:

- Fire alarm pull station – Not less than 1.1 m (3.5 ft) and not more than 1.2 m (4 ft) above finished floor (AFF)
- Fire alarm horn/strobe – Not less than 2 m (6.5 ft) and not greater than 2.4 m (8 ft) AFF.
  Exception: where low ceiling heights do not permit mounting at a minimum of 2 m (6.5 ft), visible appliances should be mounted.
- Intercom – 1.2 m (4 ft) AFF
- Nurse call stations – 1.2 m (4 ft) AFF
- Buzzers or bells – 2 m (6.5 ft) AFF or 150 mm (6 in) below ceiling
- Clocks – 2.4 m (8 ft) AFF or 150 mm (6 in) below ceiling
- Access control card/badge reader – 1 m (3.3 ft) AFF

Clients may provide specifications for mounting heights that differ from the typical examples offered above.

5.10 Infrastructure for Wireless Transmission

5.10.1 Requirements

Cabling infrastructure used for wireless transmission within ESS devices shall conform to all requirements of Section 5.

Any distributed antenna system (DAS) used within ESS application shall conform to BICSI 006. DASs shall also conform to the requirements of the AHJ, codes, and standards for the particular application (e.g., emergency mass notification, public responder) being served.

5.10.2 Additional Information

Appendix C provides additional information on wireless transmission methods.

5.11 Coverage Area Planning and Density

5.11.1 Introduction

The coverage area refers to the space served by one ESS device.

5.11.2 Recommendations

Each ESS application required for the building project (e.g., security camera, card reader) should be considered in determining the density of coverage areas and devices. ESS devices may have overlapping coverage areas. For example, multiple ESS devices may serve the same building space.

For planning purposes, a sufficient number of cabling links should be provided for ESS over the average floor space. For example, in an office space, a minimum of one cabling link should be provided per 25 m^2 (270 ft^2) of floor space. Each cabling link may serve multiple coverage areas.

If the quantity of ESS coverage areas is unknown, use Table 5-4 to estimate the quantity of cabling links recommended for serving that space. Coverage areas may be served by:

- Centralized equipment located in spaces containing one or multiple distributors
- Distributed equipment located in spaces containing one or multiple distributors
- Local equipment located in the coverage area

Table 5-4 Typical Coverage Area for Each ESS Link

Usage of Floor Space	*Coverage Area m^2 (ft^2)*	*Additional Considerations*
Office	25 (270)	In an open office environment, coverage area sizes will typically be greater than in a dedicated office space.
Indoor Parking	50 (538)	Identify fire, security, carbon monoxide and HVAC requirements[1] .
Retail	25 (270)	Security requirements may increase the coverage area density (e.g., CCTV, alarm, access).
Factory	50 (538)	Coverage area size may vary according to manufacturing processes, environment and building design.
Hotel	25 (270)	Coverage area requirements may vary if ESS applications have centralized control (e.g., HVAC, fire alarm safety system, access).
Classroom	25 (270)	Coverage area requirements may be centralized for security and access controls.
Hospital	25 (270)	Coverage area density is averaged to compensate for a variety of environments (e.g., patient rooms, labs, emergency room and operating room) – Plan for the unique ESS requirements for each area type.
Mechanical Room	5 (53)	Determine location of air handlers, chillers, boilers, pumps, fans, compressors, etc. Air handlers will typically have a higher concentration of ESS devices.

Note 1: May also require voice connections for security.

6 Intrusion Detection Systems

6.1 Overview

An intrusion detection system (IDS) detects unauthorized entry into a protected area. Its methodology of operation is to detect an intrusion and provide some form of notification that a breach has occurred in the area under protection.

An IDS is an integration of the following components and devices:

- Field devices consisting of a system keypad(s), detection sensors, and annunciators
- Processor controllers
- Notification panels and console(s)
- Power source

Typically, an IDS panel will monitor door and window contacts to annunciate an alarm upon an unauthorized opening. These systems can be expanded to include motion detection, glass break sensors, and even video motion detection and recording. In addition, the system can be connected to smoke detectors, water leak sensors, and a variety of other monitoring devices to allow integration with a building management system (BMS).

An IDS may include software applications that monitor network or system activities for malicious activities or policy violations. Additionally, an IDS may produce reports to a management station.

6.2 Developing an IDS

6.2.1 Requirements

The primary requirements when developing an IDS are as follows:

- An IDS shall be used to identify a security breach of unauthorized entry for the exterior building perimeter, interior building security boundaries, and exterior site perimeter.
- Use of detection sensors, devices that monitor and detect forced and unauthorized entry into a protected area.
- Use of processor controllers, systems that receive and process outputs from connected sensors and use predefined parameters to generate alerts based on the information received from each sensor.
- Use of a notification console, a device that monitors events and system alerts that operators can use to make informed decisions as to the operational status of the entire IDS.
- Use of power source, low-voltage transformers and backup batteries.

6.2.2 Recommendations

The primary recommendations when developing an IDS are as follows:

- IDS panels should be monitored from a central monitoring station to provide enhanced security.
- IDS should be tied into a local alerting system and into a police station or a private security station.
- IDS should be capable of alerting homeowners and business owners via pager, telephone, or Internet.

6.3 System Connectivity

6.3.1 Wired Devices

6.3.1.1 Overview

The following is the typical required cabling for an addressable device system:

- Panel to keypad: 4-conductor stranded 0.823 mm^2 (18 AWG)
- Panel to addressable devices: 1-pair twisted 0.823 mm^2 (18 AWG)
- Panel to powered device: 1-pair 0.823 mm^2 (18 AWG)
- Conventional device to addressable module: 1-pair 0.326 mm^2 (22 AWG)

The following is the typical required cabling for a conventional device system:

- Panel to keypad: 4-conductor non-twisted 0.823 mm^2 (18 AWG)
- Panel to device: 2-conductor 0.326 mm^2 (22 AWG)
- Communication bus: 4-conductor 0.823 mm^2 (18 AWG)
- Panel to powered device: 2-conductor 0.823 mm^2 (18 AWG)

6.3.1.2 Requirements

Any telecommunications or ICT cabling required for an IDS shall be of a type listed in Section 5.4.

6.3.2 Wireless Devices

6.3.2.1 Overview

Wireless systems are utilized where it is difficult to install wire. These systems tend to be favored more in the residential market because of increased difficulty in installing wire in finished homes. The devices commonly utilized in a wireless system use replaceable batteries that may last between six months and two years.

6.3.2.2 Requirements

The use of wireless devices in an IDS shall meet AHJ requirements.

6.4 Sensors

6.4.1 Introduction

IDS detection sensors operate on the principle of sensing or detecting changes that occur to the operational conditions specified at the area under protection.

6.4.2 Recommendations

If detection sensors are used, they should be used to monitor:

- Perimeters – doors, windows, fences, and walls
- Area of space – office spaces, hallways, cabinets, and lobbies
- Points of interest – safes, paintings, and expensive artifacts

Detection sensors should be deployed considering the technology utilized and the basis of activation (see Table 6-1).

Table 6-1 Detection Sensor Technology and Application

Technology	*Basis of Activation*	*Application*
Audio	Sound	Interior areas, vaults, and other low sound level areas
Capacitance	Proximity	Exterior areas
Electromechanical	Breaking of electrical circuit	Interior and exterior areas
Glass break	Vibration/audio	Windows
Infrared	Movement	Interior and any areas where the temperature remains fairly constant
Interfaces	Dry contact	Fire detection and alarm, HVAC, refrigeration, surveillance
Microwave	Movement	Interior and exterior areas
Photoelectric	Interrupting light beams	Interior and exterior areas with line of sight from transmitter to receiver
Pressure	Weight	Interior and exterior areas
Sonic/ultrasonic	Movement	Interior areas

6.5 Notification

6.5.1 Requirements

Notification devices, such as keypads, audible devices (e.g., speakers, sirens, bells), strobe lights, video monitors, relays, recording devices and power line carriers, shall be used as part of an IDS. A combination of more than one type of notification device in a given IDS is possible and permitted by this standard.

When active devices are used, power shall be provided to these devices. When connected to the building's structured cabling system, cable length limits shall be observed (See Section 5.4).

6.5.2 Recommendations

An IDS should be monitored by an off-site facility or monitoring station to indicate alarms, or off-normal conditions so that necessary actions or responses will not be delayed. Communications to a remote site can be accomplished in many different ways.

6.5.3 Additional Information

An IDS can use the following means of communicating with a central reporting station:

- Telephony (e.g., landline or POTS)
- Internet protocol (IP) technology
- Cellular telephony
- Wireless communication

When utilizing wireless, an IDS can transmit:

- Status signals from edge devices
- System trouble, supervisory responses, or alarms back to a monitoring station
- User data from a system keypad

An IDS, when utilizing wireless technology, can be used in place of most wired devices, including:

- Glass break detectors
- Recessed window contacts
- Short-range passive infrared (PIR) motion sensors
- Surface mount door contacts
- System key fobs and system keypads

6.6 Control Panel

6.6.1 Requirements

The control panel or controller shall be designed to analyze the various outputs from the detection sensors as well as monitor their own internal circuitry for abnormal operation of its internal devices.

Power limitations of the control panel shall be observed in order to not overload a power output or the entire power panel. The total current draw for an output shall never exceed its rated value. If either the maximum value of an output or the total panel will be exceeded, an external power supply shall be added to the system to power the additional load.

The battery backup shall be correctly sized for the necessary runtime of the panel without external power. The control panel battery shall not be oversized. Battery sizing shall be determined by applying the following formula.

$$B = T_s \times I_s + T_a \times I_a \qquad (6\text{-}1)$$

Where:

B = Battery size (ampere-hour, Ah)

T_s = Required battery run time (hour, h) during Standby

I_s = Current draw (ampere, A) during Standby

T_a = Required battery run time (hour, h) during Alarm

I_a = Current draw (ampere, A) during Alarm

6.6.2 Recommendations

When a standard battery backup size for a given total value determined (by applying formula 1) is not available, battery size should be sized up (this information is usually available in the manufacturer's literature). When a required battery runtime is necessary while the panel is in alarm condition, additional calculations should be performed. Standby runtime is generally a requirement of fire alarm systems (See Section 9).

Control panels should be installed in a secure area with limited or restricted access. Access to the control panels is usually only needed by installation or service personnel.

6.7 Keypads and Annunciators

6.7.1 Requirements

An IDS shall have keypads and annunciators in order to provide a means for the users and installers to input commands to the control panel as well as provide information to users, installers and managers.

6.7.2 Recommendations

Keypads and annunciators can be found in three different styles such as hard button, numeric keypad, and touch screen. The specification of such devices is out of the scope of this standard.

6.8 Initiating Devices

6.8.1 Overview

Initiating devices are used in an IDS to send input signals to the panel such as a breach or a change in state of the device. These devices are either passive and do not require external power (2-wire) or active and require external power (4-wire).

6.8.2 Motion Sensors

6.8.2.1 Recommendations

An IDS should have motion sensors used to detect motion in a room or area.

Motion sensors should be correctly placed in order to allow proper coverage of a given area. Power as recommended by the manufacturer, should be provided to motion sensors.

NOTE: For information about sensors, types and coverage capacity, refer to the manufacturer's literature)

Motion sensors should not be pointed toward heat registers or items hanging from the ceiling to reduce false alarm events.

6.8.2.2 Additional Information

Motion sensors usually rely on three types of technology: PIR, ultrasonic, and microwave. The specification of such devices is out of the scope of this standard.

6.8.3 Window Sensors

6.8.3.1 Introduction

Window sensors are available in a variety of styles and use different methods to detect breaches. Some styles are acoustical (also referred as to glass break detectors), sensitive to vibration and mount directly to the window or the window frame, magnetic switches, and customized window security screens.

6.8.3.2 Recommendations

When appropriate, an IDS should have window sensors in order to detect breaches. The specification of window sensors is outside the scope of this standard. A wide variety of styles of window sensors should be considered as part of an IDS. Combinations of multiple sensor styles are allowed. The following styles may be considered:

- Glass break sensors
- Shock sensors
- Magnetic switches
- Security screens

6.8.3.3 Additional Information

A 7.5 m to 9 m (25 ft to 30 ft) radius is common for glass break sensors. Some units only detect a radius no larger than 3 m (10 ft). For accurate information about sensor operation, refer to its manufacturer's literature.

Many shock sensors are standalone active devices that have an internal processor, require power, and have contacts for signaling alarms to the control panel. Other types of shock sensors send signals to a remote processor that powers the units, interprets the signals, and passes alarms on the control panel. Refer to the manufacturer's installation instructions for further information.

6.8.4 Door Status Sensors

6.8.4.1 Introduction

Door status sensors (wired) are generally passive and composed of dry contacts that can be activated by an external magnet, plunger or roller ball that is integrated into the sensor.

6.8.4.2 Recommendations

An IDS should have door status sensors used to report status on each door or latch that can offer access to a controlled area, space or property.

6.8.5 Perimeter Sensors

6.8.5.1 Introduction

Perimeter sensors are used to provide intrusion detection notification for the outer edge of an area or property. These sensors are intended to provide notification when unauthorized entry is gained onto the property. Types of perimeter sensors include:

- Outer motion sensors
- Photoelectric beam sensors
- Fence sensors
- Seismic sensors
- Radar sensors

The following technologies are deployed in the manufacturing of perimeter sensors:

- Passive magnetic field sensor
- Electric field sensor
- Microphonic sensor
- Optical fiber cable sensor
- Radar sensors

Pan, tilt, and zoom (PTZ) cameras can be deployed as perimeter sensors, due to their ability to locate a target.

6.8.5.2 Recommendations

An IDS should have perimeter sensors to provide intrusion detection notification.

Outdoor motion sensors generally are mounted on the exterior of a building and have a detection range of 9 m to 15 m (30 ft to 50 ft). When connected to the building's structured cabling, cable limits should be observed (See Section 5.4).

Photoelectric beam sensors (transmitter and receiver) may need external power and should be wired for power when used. When connected to the building's structured cabling, cable length limits should be observed (See Section 5.4).

6.9 Optional Integrated Equipment

6.9.1 Introduction

An IDS usually operates as a stand-alone system, but most systems allow other systems to be incorporated into the control panel with expansion modules that are already built into the system.

The following systems can be incorporated into an IDS:

- Access control (See Section 8)
- Fire detection and alarm (See Section 9)

6.9.2 Requirements

Addition of any fire alarm device to an IDS can change the classification of the system from IDS to fire alarm. Ensure compliance with all applicable fire alarm codes and standards.

This page intentionally left blank

7 Video Surveillance

7.1 Overview

Video surveillance is the extension of human vision to areas requiring surveillance. Discussions regarding surveillance system deployment, integration, monitoring, and convergence often lead to the determination of functional needs.

Some primary applications of this technology include:

- Observation
- Investigation and forensic review
- Recognition of objects (e.g., human faces, license plates)
- Prosecution
- Loss prevention and deterrence
- Intrusion detection and perimeter monitoring
- Access control
- Operations management and resource allocation
- Safety
- Security

This section applies to video surveillance systems deployed for use cases listed in the following text, but may also be applicable to other uses not cited.

When planning video surveillance systems, like all ESS systems, device performance in unanticipated conditions and potential interdependencies with other external devices, systems, and infrastructure should be included, as elements to be addressed for achieving the highest level of fault tolerance possible.

7.2 Generation and Conformance with Use Cases

7.2.1 Scene Characteristics

7.2.1.1 Introduction

The video surveillance system (VSS) use case is defined by the scene characteristics and the specification of the VSS function(s).

7.2.1.2 Requirements

7.2.1.2.1 Scene

The scene shall be identified to include one or more areas of interest or scene content.

The VSS shall present a scene of interest to a user in sufficient detail to make a decision or perform a task based on recognition of what is happening in the scene. For example, an end user may wish to be able to read the characters in a license plate, or determine the identities of individuals at a local convenience store while performing surveillance.

The VSS shall be designed to accomplish one or more specific tasks regarding a scene. The primary functions of the VSS shall be identified as one of the following:

- Observation
- Forensic review
- Recognition

The VSS scene content criteria shall incorporate resolution, object size, speed, trajectory, scene lighting level, and required refresh rate.

7.2.1.2.2 Resolution

Resolution, as required by the VSS primary function, and shall be measured in pixels per meter (ppm) or pixels per foot (ppf). The pixels per meter or foot calculation shall be derived for both horizontal and vertical pixels and is equal to the imager's pixel dimensions divided by the corresponding field of view linear dimension (meter or feet).

The use of video cameras and encoding technology with built-in pixel counting shall be considered as an enhancement to the design process, measurement and verification of pixels on target.

7.2.1.2.3 Object Size

The size of the object(s) in the scene content, in conjunction with the VSS's primary function, shall be used in the design of the VSS.

For all objects occupying 25% or less of the field of view, high definition television (HDTV) video cameras shall be required.

7.2.1.2.4 Object Speed and Direction

HDTV video cameras shall be required in video surveillance systems where the moving object(s) of interest occupy 10% or less of the field of view.

The imager orientation shall match the direction of movement (e.g., 16:9 horizontal, 9:16 vertical).

7.2.1.2.5 Lighting Levels

The scene environment and the scene's light sources shall be used in evaluating the lighting of the VSS scene.

Lighting levels shall be measured using resolution targets and reflected light.

7.2.1.2.6 Display Refresh Rate

Refresh or display rate in frames (images) per second (fps) for the VSS function shall be matched for the display size.

The refresh rate for the VSS function shall be matched to the percentage that the object(s) of interest occupy within the field of view, together with the object's speed and trajectory.

NOTE: Mobile devices with smaller display resolution utilize a lower minimum refresh rate for the VSS function; larger displays utilize a higher refresh rate.

7.2.1.2.7 Testing

Qualified personnel shall verify the performance of the video camera or encoding device in production of suitable images for observation, forensic review or recognition functions.

Testing shall include site testing with actual test objects or test charts developed upon applicable standards and documents (e.g., ISO 12233, ISO 14524, HDTV test charts).

7.2.1.3 Recommendations

The ability for the video camera or encoding device to render images that match the VSS primary function should be used.

The use of video cameras and encoding technology with built-in pixel counting can enhance the design process, measurement, and verification of pixels on target.

Smaller objects require higher resolution image capture. Video cameras with image capture characteristics complying with image quality standards are recommended, such as HDTV.

For subjects traveling at speeds of 40mph and occupying greater than 10% of the viewing area, use of both MJPEG and h.264 compression encoding is recommended. For recording subjects exceeding the same relative speed on board a moving craft or vehicle, also use dual encoding.

7.2.2 Observation as a Primary VSS Function

7.2.2.1 Requirements

Video surveillance systems designed for the observation function shall be optimized to provide continuous viewing of scene content captured by the video camera or encoding device, and displayed on local or remote monitors, or on remote display devices (e.g., smart-phones, tablets, laptop computers).

The minimum resolution as measured in ppm (ppf) shall be 65 ppm (20 ppf) to achieve a VSS observation function using imaging standards like HDTV. Non standardized cameras shall pass the lighting level and resolution target test process.

7.2.3 Forensic Review as a Primary VSS Function

7.2.3.1 Requirements

Video surveillance systems designed for the forensic review function shall be optimized to provide high resolution recording of scene content or digital multimedia content (DMC) captured by the video camera or encoding device. The DMC shall have resolution high enough to permit general identification of scene content or object(s) of interest, identification of object colors, specific identification of an object's characteristics, the time, and location of the objects in the DMC.

The minimum resolution shall be 131 ppm (40 ppf) using imaging standards like HDTV to achieve a VSS forensic review function. Non standardized cameras shall pass the lighting level and resolution target test process.

7.2.4 Recognition as a Primary VSS Function

7.2.4.1 Requirements

Video surveillance systems designed for the recognition function shall be dependent on the specific recognition function required for the use case. Recognition functions shall include but not be limited to:

- Vehicle license plate recognition
- Facial recognition
- Face location
- Smoke and fire detection
- Object recognition
- Pattern recognition
- Cross-line detection
- Object temporal characteristics
- Color recognition
- Trajectory

Qualified personnel shall verify the performance of the video camera or encoding device, together with the recognition application to produce suitable data through site testing with actual test objects.

The minimum resolution as measured in pixels per linear distance shall be 262 ppm (80 ppf) using imaging standards like HDTV to achieve a VSS recognition function. Non standardized cameras shall pass the lighting level and resolution target test process.

Designs shall consider visual verification of image quality using normative resolution and visual acuity tools available where possible. In the case of public safety, homeland security, port security, critical infrastructure, video surveillance used for remote healthcare and all video surveillance applications used by first responders, designs shall incorporate any applicable codes, standards and regulations that offer global best practices.

NOTE: Additional guidance on achieving video quality is offered from a variety of resources (e.g., *Handbook of Video Quality in Public Safety and Security*, as administered by the US Dept. of Homeland Security and Public Safety Communications Research).

Designs and component selection shall accommodate the following minimum image quality requirements to optimize recognition and identification:

- Video format
- Audio format
- Metadata format
- Multiplex and transport protocol
- Data security and integrity

7.2.5 Additional VSS Functions

7.2.5.1 Requirements

In addition to the primary VSS functions, additional functions shall be identified as required:

- Prosecution
  The VSS shall incorporate recording of the object's time, location, and specific characteristics, considering the resolution minimum as forensic review function.
- Loss prevention and deterrence
  The designer shall employ the use of public view monitors where possible, displaying entry activity and in prominent public view. Inactive camera shells or "dummy" cameras shall not be used.
- Intrusion detection and perimeter monitoring
- Access control identity
- Operations management and resource allocation
- Safety
- Security (object left behind)

7.3 Device Groups and Interoperability

7.3.1 Requirements

The designer shall identify the devices necessary to achieve the VSS use case and accommodate the user's total cost of ownership requirements. The devices required for a given use case shall vary and be dependent on the geographic dispersion, number of video cameras, or encoders and specialized DMC or video content management.

7.4 Device Categories

7.4.1 Requirements

Device categories shall include, but not be limited to:

- DMC source
  - Video cameras
  - Encoders
- VSS physical infrastructure
  - Ethernet cable
  - Power over Ethernet
  - Power sourcing equipment
  - Wireless infrastructure
  - Media converters
- VSS logical infrastructure
  - Ethernet switches
  - Routers
  - Firewalls
- VSS control and analysis devices and applications
  - Video analytics algorithms and processing
  - Intelligent video search applications
  - Video synopsis applications
  - Positionable video camera control
  - Camera selection control
  - Video source to display control
- VSS video management devices and applications
  - Digital video recorder
  - Network video recorder
  - Video recording server
  - Video management system application
  - Physical security information management application
  - Digital data management,
  - Cloud-based video software-as-a-service
- DMC storage
  - Local storage within digital video recorders and network video recorders,
  - Network attached storage,
  - Cloud-based video infrastructure-as-a-service
- DMC display
  - Flat panel video monitors and walls
  - Mobile devices
  - Tablets and laptop computers

All VSS devices shall support network time protocol. Foreign systems interfacing to the VSS require network time protocol support and periodic audit of total system time synchronization.

7.5 Use Cases

7.5.1 Requirements

For all use cases, designs shall include a:

- DMC source
- VSS physical infrastructure
- VSS logical infrastructure
- VSS video management
- DMC storage

For a use case requiring greater than five (5) sites and low or non-existent VSS control and analysis, the VSS video management shall be a network video recorder, video management system application or combined cloud-based video management and storage application/service.

For the use case where the jurisdiction requirements require DMC to not be stored on-site due to theft concerns, the design shall specify a combined cloud-based video management and storage application/service.

For a use case requiring less than five (5) sites and medium to high VSS control and analysis, the VSS video management shall be a video management system application, physical security information management system or digital data management system.

Designs shall specify DMC storage to accommodate user compliance requirements. Facilities processing personally identifiable information (e.g., business transactions, government issued ID number, credit/banking account numbers) or conforming to the Payment Card Industry-Data Security Standard (PCI-DSS) and Statement on Auditing Standards 70 (SAS70) for physical and logical security shall require a minimum of ninety (90) days DMC retention, unless otherwise directed by those standards or AHJ.

If the system requires remote viewing or if the solution is using managed or hosted video, qualified personnel shall verify that the end user's connectivity (upstream bandwidth) can support these requirements. Mobile devices require lower resolution and network attached storage can accept a HDTV stream while a lower resolution stream is sent to the remote user or the managed video service.

7.6 Open Network Video Interface Forum Conformance

7.6.1 Requirements

All VSS devices shall conform to an interoperability test as specified by the design. Where possible, devices conforming to the Open Network Video Interface Forum (ONVIF) shall be used, as long as the VSS device manufacturer can provide proof of the specification conformance test document. Devices used that are not ONVIF conformant shall demonstrate interoperability via a manufacturer's application program interface (API), whose support for that API have been in place via an established partner program greater than five years and documented interoperability testing performed.

7.7 Deployment Process

7.7.1 Requirements

Designs shall incorporate information from a video site survey, identify camera functions, and accommodate multiple VSS functions as applicable.

Qualified personnel shall assess the lighting conditions, measure the reflected light at the facility during various times of day and recommend DMC sources capable of rendering usable images with the available illumination and satisfying the primary VSS function. The ESS designer shall also assess the DMC source device compatibility with the color temperature of the reflected light and color rendition index (CRI) of the illumination for compatibility. Use of illumination with as high a CRI is recommended.

Infrared illumination shall be used in the 850 nm wavelength where possible. Network cameras capable of rendering images illuminated by either 850 nm or 950 nm covert infrared illuminations to maintain maximum VSS flexibility shall be used.

VSS devices that utilize PoE shall be provisioned, powered and connected to cabling that conforms to IEEE 802.3. All PSE shall deliver the power on request from a compatible VSS powered device and maintain operation supervised by an external management system. Critical failures, such as PSE device failure, shall be monitored by the owner or end user's information management, information technology or systems solutions staff. PoE and high power PoE designations for powered devices and PSEs shall be considered manufacturer specific and not used where devices compliant with IEEE 802.3 are available. Deployments at higher power levels than these standards shall be accompanied with an analysis of cabling, cabling installation, supporting cabling accessories, local compliance, and dedicated data cabling, negating any temperature concerns and guaranteeing safe and consistent operation.

Qualified personnel (e.g., ESS designer) shall:

- Assess the existing or proposed infrastructure / system architecture / network topology / protocol support and determine the impact on the VSS.
- Recommend specific physical infrastructure improvements as part of the current design or separate project, capital project, or periodic expansion to accommodate the requirements of the VSS.
- Provide guidance for infrastructure lifecycle management, or the continuous assessment of the facility's transmission system to maintain compatibility with the VSS bandwidth, user access, infrastructure-delivered power, and scalability requirements.
- Consider systems external to the VSS to manage power and connectivity where possible.
  These systems shall be known as infrastructure management systems and shall provide intelligent patching and provision services, using the network to aggregate power usage reporting. The infrastructure management system shall be necessary for systems expected to exceed 20% expansion.
- Specify the resolution and image refresh rate for network cameras, according to the use case requirement.
- Provide the necessary data to make use of a user's existing network:
  - Estimate bandwidth using approved manufacturer tools and verify with average site conditions with scene motion.
  - Get individual values.
  - Prepare bandwidth use and overlay on network device map.

  NOTE: Verify expected protocol compliance and performance with user's network or IT professional (make sure bandwidth needs and protocol requirements match infrastructure).
- Verify users are satisfied with the workstations' intended use and expected performance.
- Verify server performance and modify VSS as required.
- Finalize the equipment list with merging components into assemblies by function / purpose.
- Create a matrix of VSS uses and stakeholder responsibilities containing:
  - The person and group responsible
  - How the responsible group is informed
  - Identification of input and support to group responsible
- Make use of virtual local area networks (VLANs) and quality of service (QoS) as much as possible to ensure minimal impact on shared infrastructure (See Section 5).
- Dedicated infrastructure shall only be used when the ESS designer has shown the shared infrastructure is over capacity or over-utilized for the use case and the safety management program, security management program or risk assessment requires same.
- Use these documents and define who is responsible for developing a commissioning statement.

7.7.2 Recommendations

Where illumination is unavailable or poor quality images are rendered by the DMC source, designs should consider using infrared illumination, HDTV devices capable of supporting low light conditions. Network-based thermal imaging cameras of the uncooled sensor type, capable of multiple palette rendering, verifying compatibility with the VSS primary function, should be considered.

7.8 Authentication of Network Video Cameras for Improved ESS Network Security

7.8.1 Requirements

The non-person entity shall be a network camera capable of streaming DMC. The DMC shall also be known as digital video content, network video content or digital multimedia evidence. Each of these formats are capable of incorporating digital data representing audio content, video content, metadata information, location-based information, relevant IP addresses, recording time, and system time attached to a digital file.

Where applicable by user requirements, the DMC source shall be a network camera incorporating embedded memory, SD or MicroSD card media. The network camera shall be capable of running a cryptographic algorithm authenticating the network camera, DMC source originating from the network camera and the DMC user that consumes, stores or displays the DMC in accordance with an identity, credential, and access management (ICAM) policy. This ICAM policy shall incorporate a trustworthy process for assigning attributes to a digital identity (DMC source) and to connect that identity to an individual (DMC user) via a trusted framework.

This page intentionally left blank

8 Access Control Systems

8.1 Overview

Access control refers to the practice of controlling access to a property, building, or select space within a facility for authorized persons only. Currently, a wide variety of mechanical and electronic hardware devices are used to protect or prevent unauthorized access to important items or to restrict access to protected areas and valuable information. These devices vary from traditional physical keys and locks to elaborate electronic access systems capable of recognizing the biographical and biometric data of system users prior to granting access to secure spaces.

8.2 System Structure

8.2.1 Overview

The minimum of required components for an ACS include a computer, a control panel, and a peripheral device connected to the control panel. An ACS may be more complex, having multiple control panels and peripheral devices, and may use additional components, such as credentials.

The components of ACS may be classified into the following levels:

- Level 1 – Central equipment processing, recording, software, and database
- Level 2 – Controllers for intelligent field processing (e.g., data gathering panel)
- Level 3 – Peripheral devices (e.g., card reader, lock, door position switch)
- Level 4 – Credentials (e.g., cards, fobs, biometrics, personal identification numbers [PINs], passwords)

8.2.2 Central Equipment Processing (Level 1)

8.2.2.1 Overview

The host computer or server runs the access control software, manages the system parameters, maintains the system database, and controls all communication with the control panels. The host computer receives all event and alarm transactions from the control panels. It then saves them into separate history files that may be used to run reports by specific criteria. The host computer may provide a GUI to simplify various tasks an operator would need to accomplish within the ACS.

For instance, multiple screens in most access control software are object oriented, allowing operators to use the point-and-click method to highlight a text box and type the data, disable an input point, or control an output device. A graphical map of the campus or a detailed CAD drawing of a building may display on a monitor to indicate an alarm location, or a window may display a live video (when integrated with a VSS) of the person pushing the intercom button to request entry into the lobby.

8.2.3 Computer Hardware and Software

8.2.3.1 Recommendations

Computer hardware used within an ACS should exceed the manufacturer's minimum requirements for processor speed, memory, and drive size. If the computer will be used for the badging station, the size and type may depend on the space required by the video capture cards.

The size and type of monitor used with the ACS may depend on the location and purpose. In certain high-sensitivity/security environments, redundant computer hardware may be required to ensure system availability and reliability.

8.2.4 Server

8.2.4.1 Overview

Typically, an ACS database resides on a server. The ACS server(s) may be in a number of locations, depending on the application. It may be collocated with IT servers in a computer room or be a stand-alone computer in an office. The server commonly runs a number of applications (e.g., badging software, card entry software) that are part of the card access system.

A large server typically runs the database only. Certain applications may require the use of dedicated or multiple servers.

The server communicates with ACS components through various media. Some examples are:

- Hardwired or wireless connections to the card reader panels and other devices
- IP communications through a network to either the card reader panels or remote workstations
- Telephone modem connection to off-campus reader panels

8.2.5 Software

8.2.5.1 Overview

An ACS may use proprietary software, which can limit its interoperability with other systems. Additionally, there may be licensing requirements based on the number of devices or credential holders expected to use the ACS.

8.2.6 Backup

8.2.6.1 Overview

Backup specifications for the ACS are determined by the length of time the information is intended to be made available and the amount of data that is intended to be stored. The manufacturer may determine the drive size once the amount of data required has been established. The ACS server provides long-term secure storage as needed.

8.2.7 Event Recording

8.2.7.1 Recommendations

A means to record and store events in the system should be provided. If the event is on the ACS, the initial events should be written to the local hard drive. If the event or alarm has a surveillance camera associated with it, the image should be recorded.

The types of events to be recorded or monitored are part of the initial planning stages of the ACS and may include:

- Door forced open alarm
- Invalid badge read
- Card/badge passback attempts
- Duress alarm
- Fire alarm
- Infant alarm

Once the event is recorded, a means to provide long-term storage and retrieval should be provided. The length of time that recordings are to be archived may be governed by AHJ guidelines.

8.2.8 Backup Power

8.2.8.1 Recommendations

The ACS power supply should have a backup. All computers should be provided with an UPS that can provide the required length of operation. The minimum time recommended for an orderly shutdown and saving of all data with a software/hardware connection to the ACS computers should be fifteen minutes.

The card reader panels should have some type of battery backup for the electronics, and where possible, the doors controlled by the reader panel. A four-hour backup should be provided for door operation. Depending on the application and applicable codes, the AHJ may provide requirements for the reader panel back-up.

NOTE: AHJs may require that a door fail-safe when the batteries fail.

If emergency power is available, it may be advantageous to connect the ACS to this source as well as to the UPS.

In addition to backup power recommendations, the ESS designer may request dedicated access control branch circuits for the primary power source for ACS equipment.

8.2.9 Access Control Workstation

8.2.9.1 Recommendations

The ACS workstation is primarily used for entering system data through some type of GUI into the ACS access software. The workstation also may be shared for badging functions and visitor management uses. The workstation's location should accommodate the intended uses (e.g., visitor management software installation requires locating the workstation near the facility's entry point).

The workstation communicates with the access control server over a network, hard wire, or modem connection.

8.2.10 Badging System

8.2.10.1 Recommendations

The badging station may be located in the security or the human resources office. If photographic images are included as part of the badging system, they may be captured by:

- Video capture card located in the workstation. (The card is connected to the camera)
- USB connection made directly to the digital camera
- Removable media drive that reads images taken from the camera. (This item may be helpful if the camera must be taken to the individual for the picture)

8.2.11 Visitor Management

8.2.11.1 Recommendations

Visitor management systems may offer benefits beyond security, such as:

- Electronic visitor registration may be quicker and more reliable
- Preprinted badges enhance a professional image for the company
- Improved visitor services (e.g., wayfinding)
- Enhanced confidentiality
- Enhanced emergency response because a visitor's presence is traceable

By combining employee and visitor ACS, a facility can comprehensively provide access to and monitor the movement of both groups. The ACS may be integrated with video surveillance to capture images of people entering, exiting, and moving around a facility. This also may help prevent the loss of physical assets. Another benefit is that a number of facilities can be managed from a central location.

8.3 Controllers for Intelligent Field Processing (Level 2)

8.3.1 Overview

A system controller provides multiple purposes and benefits as a critical element in an ACS. System terminology varies and the following terms are often used interchangeably:

- Control panel
- Field access control panel
- Access control controller
- Access control field controller
- Data gathering panel
- Intelligent field panel

The access controller’s primary purpose includes providing:

- A consolidation point where independent peripheral devices are connected.
- Power for level 3 connected peripheral devices.
- A redundant means of decision-making in the event that communication is lost between the access control server and the system controller.

8.3.2 Controller Configurations

8.3.2.1 Overview

Controller configurations vary by manufacturer and have no standard appearance, or dimensions. However, the following two controller configurations are typically used:

Configuration 1

All of the electronics and terminations are enclosed in a single cabinet. This design traditionally consists of a large backplane or motherboard where daughter boards or function cards are connected as required.

Configuration 2

Multiple enclosures are used and are electrically connected in a ring or star topology. Each enclosure contains electronics that are dedicated to perform a single or selected multiple functions. One of the controllers functions as the master node in this configuration and is equipped with the communication ports.

8.4 Peripheral Devices (Level 3)

8.4.1 Overview

Peripheral devices may be sensor equipment that monitors certain conditions (e.g., temperature) and reports the status back to the control panel. Peripheral devices also may be output devices that control passage through entryways or bells indicating shift change.

Peripherals in ACS are generally classified as being in one of the following categories:

- Readers
- Request-to-exit devices
- Door contacts
- Electrified door hardware

8.4.2 Relays

8.4.2.1 Overview

Relays have sets of contacts that are described as closed (allowing electrical current flow) or open (not allowing current flow). Switch contact variations are normally described by the number of poles and throws it contains. The number of poles defines the number of separate contacts for a switch position. The number of throws is the number of switch positions available.

Within ESS applications, specific relay configurations and functions may be known as:

- Form A relay (normally open relay) – a single pole, single throw relay that remains open until it is energized
- Form B relay (normally closed relay) – a single pole, single throw relay that remains closed until it is energized
- Form C relay – a single pole, double throw relay

NOTE: A "Form A/B/C relay" may also be known as a "Form A/B/C contact".

Figure 8-1 provides an illustration of these three types of relays.

Control devices consist of lock output and relays for auxiliary inputs and outputs. Relays are typically used for auxiliary inputs and outputs to the ACS. The reason for relays is that the current required by the load is too much for the control device.

A relay may be used to open a gate upon instructions from the controller after the card reader or keypad inputs have been verified. An example of output would be the return of elevators to the ground floor of a high-rise building after the fire department personnel activates this function using the key in the ground floor lobby.

Inputs to the control device may be either normally open (NO) or normally closed (NC). The door is locked when the default door relay output is de-energized. The door relay output is energized to unlock the door. A default shunt time is assigned to the door position (approximately 25 seconds), a time is assigned to the egress device (normally 0 seconds), and a default pulse time is assigned to the lock (approximately 10 seconds).

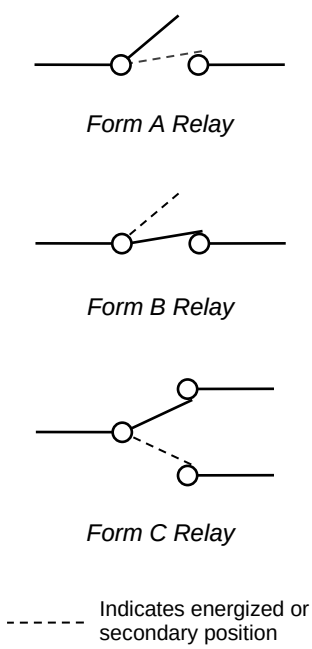

Figure 8-1
Form A, B and C Relays

8.4.3 Power Distribution

8.4.3.1 Recommendations

Peripheral devices are typically powered by either 12 V_{DC} or 24 V_{AC} power supplies. Voltage drop should be considered when determining the distance from the device to the power source. Once the voltage drop is considered, the appropriate gauged wire size should be specified to ensure adequate voltage reaches the device.

Connecting the device to multi-fused 12–24 V_{DC}/V_{AC} power supply centralizes the power sources for multiple devices and accessories. This is in lieu of having AC outlets installed near each device. Voltage drop and wire size calculations should be considered for each individual device back to the multifused power supply.

The AC power input, the power transformer, and all fused power outputs should be enclosed in one lockable enclosure with tamper switches monitored by the alarm monitoring system. It is recommended that all outputs be individually fused. If a device or accessory is individually AC powered, more UPS circuits may be needed than when using a multi-fused power supply. A multi-fused power supply also simplifies placing a UPS circuit by having only one source for the multiple devices or accessories.

8.4.4 Readers

8.4.4.1 Requirements

Readers shall be placed and installed in accordance to codes and the AHJ, in addition to any requirements pertaining to the accessibility or interaction by a person (e.g., *Americans with Disabilities Act*).

8.4.5 Request to Exit Devices

8.4.5.1 Overview

A request to exit (REX, or also known as RX, RTE, or RQE) device is a device installed on the secure side of the door that allows egress without triggering an alarm. In most ACS, if the door opens from either side without a valid credential presented to the reader or REX, an alarm is activated. When activated, the REX device sends an REX signal to the ACS, communicating an authorized exit through the door.

8.4.5.2 Requirements

A REX may be used to unlock a door from the egress side to exit an area, which is commonly performed using magnetic locks. When an REX device is used for this purpose, its installation and use shall conform to applicable codes and the AHJ.

8.4.6 Door Contacts

8.4.6.1 Overview

Magnetic door contacts are often used for monitoring an open or closed door. The door contact consists of two parts - a reed switch and an actuator magnet. The actuator magnet's pull on the reed switch causes the contacts to close. The reed switch part of the door contact is generally installed in or on the doorframe near the latch side of the door. The magnet is generally installed in or on the door near the latch side of the door.

8.4.7 Electrified Door Hardware

8.4.7.1 Overview

Electrified door release hardware is a generic term for electromechanical locking hardware that is released upon an approval signal. This signal may originate from various sources, such as a simple remote button or the ACS software.

8.4.7.2 Requirements

Electrified door hardware shall meet all applicable codes and requirements of the AHJ.

8.4.8 Fail-Secure/Fail-Safe/Fail Latched

8.4.8.1 Fail Secure

8.4.8.1.1 Overview

Fail-secure hardware goes to a locked state when power is removed from the hardware. It is sometimes referred to as power unlocked. Power is applied to unlock this type of device. This type of hardware is normally specified for security purposes as a device failure leaves the door secured.

8.4.8.1.2 Requirements

If a fail-secure device is kept unlocked for long periods of time, the device shall be rated for continuous duty.

8.4.8.1.3 Recommendations

Employing an inline power conditioner to minimize DC voltage surges also is recommended to extend the life of the device.

8.4.8.2 Fail Safe

8.4.8.2.1 Overview

Fail-safe hardware fails in the unlocked position when power is removed. It is sometimes referred to as power locked. Power is removed to unlock this type of device. This type of device is normally used in emergency situations when the door must fail unlocked for life safety egress.

8.4.8.2.2 Recommendations

Certain door release devices require power to lock (e.g., magnetic locks). When door release devices requiring power to lock are used solely for security purposes and there are no life safety issues, backup power is recommended.

8.4.8.3 Fail-Latched

8.4.8.3.1 Requirements

A related term to “fail-secure” is “fail-latched”. Fire-rated door release devices shall be rated fail-secure to avoid unlatched egress doors. Doors that are fire rated and part of a fire separation (e.g., stairwell doors) shall remain latched even though they are unlocked.

8.4.8.4 Fail-Secure and Fail-Safe REXs

8.4.8.4.1 Overview

The installation and setup of REX devices that require power have to be carefully planned and performed. If the REX is set to the fail-secure configuration and power is lost, the REX will not change state, bypass the alarm, or open the door. If the REX is set to the fail-safe configuration and power is lost, the REX changes state, bypasses the alarm, and releases the door.

8.4.8.4.2 Requirements

The following items shall be verified when using fail-secure or fail-safe REXs:

- Does the PIR, door release button, or panic button unlock the door when activated?
- Does the door lock automatically on closure?
- Does the ACS detect that the door is open and display this condition?
- Does a local audible alarm sound when the door is opened?
- If required, is video coverage of the door adequate?
- Is an alarm generated if the door is open longer than the preset time?
- Is the fail-safe configuration for proper operation feasible?
- Does the door release when power is lost?

8.4.9 Power to Locks

8.4.9.1 Requirements

Power supplies shall be sized to provide adequate power for the connected devices and have a source of primary power at their location.

8.4.9.2 Recommendations

Having battery backup to allow uninterrupted operation for a selected period of time in the event of loss of primary power is desirable.

Certain types of release hardware require specific power supplies because of the initial power inrush necessary to activate the device. This power may be significantly different from the power necessary to keep the device seated in a normal operation.

NOTE: This type of power inrush is most commonly seen with electrified exit or panic hardware.

Considerations for selecting voltage should include the following:

- Manufacturer recommendations
- Distance between the power supply and the devices should be calculated to ensure that there is an allowable level of voltage drop at the device. This level varies with the gauge of the wire run between the device and the power supply.
- If distance from the power supply causes the voltage drop to be too high, a separate circuit should be installed. It is not recommended to share the electrical circuits in the room.
- Available power should exceed the sum of the power consumed by the devices by at least 10 percent.
- Power for the door release hardware should be separate from the power for any other electronics.

A metal-oxide varistor (MOV) meeting the ratings for the voltage application should be used across electronic lock inputs at the door to mitigate the possibility of a reverse current presented by the lock causing damage to the controller or the lock’s power supply.

8.5 Credentials (Level 4)

8.5.1 Overview

A credential is an item or object that possession or knowledge of can be used to provide authorized persons access to a secure space.

Types of credentials include:

- Passwords
- PINs
- Radio frequency identification (RFID) tags
- Access Cards (e.g., smart card, Wiegand effect, magnetic stripe
- Biometic information (e.g., fingerprint, iris scan, facial recognition)

8.5.2 Web-Enabled Access Control

8.5.2.1 Overview

Web-enabled access control is a type of access control platform that utilizes an Internet browser exclusively to perform administrative tasks. These tasks can range from basic credential creation or updates to system-wide programming.

8.5.3 IP Card Readers

8.5.3.1 Overview

IP ready card readers are devices that have all the connections for the lock, REX device, and door position sensor for an access door. All that is required for connectivity is a balanced twisted-pair cabling connection from the campus distributor (main cross-connect), or floor distributor (horizontal cross-connect) and one local power connection to the card reader. Each reader has a built-in web server that allows the device to contain an IP address, web interface program, and a small database of card holders.

IP ready card readers also accept PoE, which eliminates the need for a separate power cable. While PoE is an option, most major metropolitan areas require that lock power drop when the fire alarm detects an alarm condition.

8.5.4 IP Controllers

8.5.4.1 Overview

IP controllers are mounted on the secure side of the door, allowing for both “fail-secure” and “fail-safe” locks to be utilized. Like IP card readers, they have a small web server installed. However, IP controllers contain all the connections necessary for one or two doors.

8.5.5 Communications

8.5.5.1 Serial Communications

8.5.5.1.1 Overview

In a hardwired copper system configuration, the host computer communicates to the control panels through one of its serial or communications ports using the TIA-232-F communication protocol. A TIA-232-F to EIA/TIA-485-A converter may be used to convert the TIA-232-F signal to a EIA/TIA-485-A signal. The converter must be located within 15 m (50 ft) of the host computer. This conversion to EIA/TIA-485-A may be preferred because of a distance limitation on the communication between the devices using TIA-232-F.

The TIA-232-F standard supports 20 kb/s to approximately 15 m (50 ft) as compared to the EIA/TIA-485-A standard that supports 1 Mb/s to 35 Mb/s over a range of 90 m (295 ft) to 300 m (1000 ft) and beyond.

This first control panel also can communicate to other control panels through the TIA-485-A protocol by looping a connection from one controller to another in a daisy-chain fashion or in a star configuration, whereby the first controller is the common communication point between all other controllers and the host computer.

8.5.5.2 Optical Fiber for Extended Distances

8.5.5.2.1 Overview

In an optical fiber configuration, the host computer communicates to the control panels through fiber converters. They also are known as optical-to-electronic (O-to-E or O/E) and electronic-to-optical (E-to-O or E/O) converters.

Fiber converters are used when a great distance separates the host computer and the control panel and telephone lines are not available or convenient. One fiber converter (E-to-O) is connected to the host computer, and another fiber converter (O-to-E) is connected to the control panel.

8.5.6 Analog Communications

8.5.6.1 Overview

In an analog configuration, the host computer communicates to the control panels through modems connected to analog telephone lines. Modems are used when a great distance separates the host computer and the control panel, and a conventional wiring installation would be cost prohibitive. A modem is connected to the host computer, and another modem is connected to the control panel. These modems must have access to an analog telephone line.

Depending on the access control manufacturer, several control panels may be connected downstream from the control panel with the modem. When configured in this way, any time a downstream control panel communicates to the host, the information is relayed up the chain from a control panel to a control panel until it reaches the head of the line. The last control panel will dial the host computer to communicate on behalf of the initiating control panel.

To limit the number of telephone calls made by the control panels, they may be programmed only to communicate with the host computer a few times per day or when there is an alarm condition to report. In this instance, the control panel will hold information (e.g., valid access transactions, other noncritical events) until its scheduled communication time.

A control panel also can be programmed to dial the host computer and download its information before its memory gets too full. The user can program a memory threshold in the control panel. When the memory fills to a predetermined capacity, the application sends a request to dial the host computer to download its information.

8.5.7 TCP/IP or Network Communications

8.5.7.1 Overview

Many control panels have, or connect to, interface cards to communicate with an IP network, usually utilizing Ethernet protocols. Each control panel is given a unique IP address. Control panels and other network devices on the network use this IP address to identify one another for communication.

Depending on the access control manufacturer, several control panels may be connected downstream from the network control panel through a direct hardwired connection. In this configuration, when a downstream control panel needs to communicate to the host, the information is relayed up the chain from a control panel to a control panel until it reaches the head of the line. The last control panel communicates over the network to the host computer on behalf of the initiating control panel.

9 Fire Alarm Systems

9.1 Introduction

9.1.1 Overview

This section covers classes of fire alarm systems. Included in this section is information on detection and initiation devices, notification devices, pathways, circuits, monitoring, supervision and other systems connected to the fire alarm systems. In order to better understand a basic fire alarm system, a drawing is provided below.

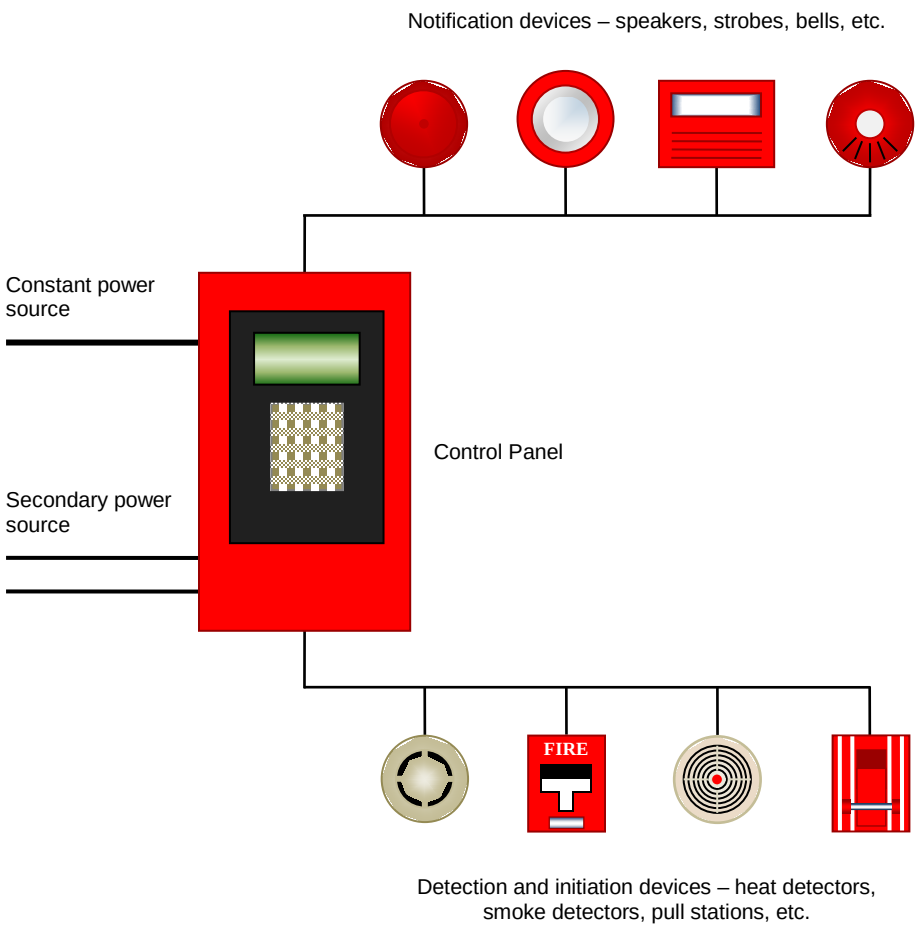

Figure 9-1
Basic Fire Alarm System

Basics of every fire alarm system include the following:

- Incoming power source
- Secondary Power
- Control panel
- Detection and initiation devices
- Notification devices

Each of these components will be explained in more detail throughout this section.

Fire alarm systems are typically designed by professional fire engineers and designers with experience in national, state, and local code requirements related to designing and integrating such systems.

Equipment manufacturers conduct installation seminars on fire alarm systems products to ensure that all equipment is installed properly and within code requirements. Continuing education related to changes in products, codes, and regulations helps to assure fire alarm systems professionals to maintain proficiency in design and installation skills.

Classes of fire alarm systems; whether wired, wireless, or IP-based, generally fall into one of three types. These types include:

- Protected Premises - This system is a closed protected system, meaning the entire system is contained to the entire campus or single building. This is protected by a single fire and detection alarm system and is under common ownership and use.
- Supervising Station - This system embellishes on a protected premises system and is continuously monitored by a central monitoring company for any abnormal events. The central monitoring company is responsible for dispatching, reporting, or similar functions due to events initiated by the protected premises system.
- Household Fire – This system is typically a residence with sleeping occupancies.

Fire alarm systems contain components that initiate a fire alarm condition by either manual operation, or automatic operation through the detection of smoke, heat or both. The systems activate notification appliances to alert the occupants of a building to safely evacuate the area when a fire condition is detected.

Fire suppression systems and their related initiation devices help to ensure active suppression of a fire condition. These supervisory devices monitor such items as the open and closed position of valves and the pressures and flow within a fire suppression system, as well as, indicate trouble conditions that would contribute to the system's inability to perform as designed. Their functions include notification of personnel for the maintenance of a component or a break in a circuit.

9.1.2 Recommendations

While every effort is made to ensure the accuracy of the content in this document, it is recommended that designers /installers of fire alarm systems should check with appropriate fire services professionals and AHJs while considering national, state and local codes to ensure compliance with all applicable codes and standards.

Installers should be trained in the latest codes and standards and certified under professional development programs (e.g., National Institute for Certification in Engineering Technologies [NICET]). This type of certification is vital to the proper installation of the fire alarm system.

9.2 Regulatory

9.2.1 Overview

The fire alarm industry is governed by many codes and standards. The primary standard of this type that applies within the United States (U.S.) is the NFPA 72: *National Fire Alarm and Signaling Code* which is published by the National Fire Protection Association (NFPA). NFPA 70: *National Electrical Code* is the U.S. electrical code which is followed by electrical and communications contractors. Additional codes that are coming into play within the fire alarm market are the International Building Code (IBC) and the International Fire Code (IFC). Each of these codes is updated on a cyclical basis and it is important to keep up to date on these codes and standards. State and local codes vary by jurisdiction and it is important to understand and fully comply with these codes as well.

9.3 Risk Assessment

9.3.1 Overview

When preparing a fire alarm system, a risk assessment is typically conducted prior to the design to fully encapsulate the site specific needs. Some primary considerations include:

- Observation of ignition sources
- Recognition of fuel loads
- Fire containment
- Operational management and resource allocation

9.3.2 Requirements

As with all fire safety issues, a formal risk assessment is required to define the design criteria for fire safety applications. This risk assessment shall be based on the Emergency Response Plan for each specific site.

9.3.3 Recommendations

Determining the primary function of the fire alarm system is the first and most critical step in the system design process. A proper system design should be established to match the needs of the user, comply with national, state, and local codes and standards, and the approval of the AHJ.

9.4 Fire Alarm Systems

9.4.1 Introduction

The main elements of a basic fire alarm system include the control panel, detection/initiation devices, notification devices, and battery backup. Each of these main elements are covered in further detail below in this section.

9.4.1.1 Requirements

Fire alarm systems are required in many premises environments (e.g., commercial building, healthcare facilities, educational facilities, etc.) and can be either wired, wireless or IP based and range from very basic to extremely complex.

9.4.2 Control Panel

9.4.2.1 Overview

Typically, all fire alarm devices are connected to a control panel. The control panel may contain the power supplies (normal and backup) required to operate the system and the control logic to cause the appropriate system actions. The panel can also contain auxiliary relays for interfacing with other building systems, as well as, communication devices for notifying off-premises personnel of system conditions.

Fire alarm control panels can be interfaced with various auxiliary building components (e.g., environmental air handling equipment, smoke dampers, elevators, fire-rated doors). The proper operation of these components is essential to the integrity of a building's fire alarm system.

Fire alarm systems can be configured with a single, central control unit or with distributed control units as the size of the facility dictates. Some control panels support an additional type of circuit for network communications. These circuits are used to interconnect multiple control panels to form a distributed fire alarm network.

Fire alarm control panels report three types of system conditions:

- Alarm – Indication that a manual pull station, a detector, or some other alarm-initiating device has been activated.
- Supervisory – Indication that a device being monitored by the fire alarm system (e.g., fire sprinkling control valve) has been changed in a way that affects building occupant safety.
- Trouble – Indication that a fire alarm system circuit has been interrupted or that a device has failed, been removed, or requires maintenance.

Control units are capable of two-way communications via analog and digital configurations. They receive, process, and make decisions based on detection device data. Depending on the programming, the control units transmit commands to alarm and control devices. Control units are usually microprocessor-based and require software to process data and make output selections based on programming.

Control units monitor (supervise) the integrity of the following circuits:

- Initiating device circuits – These circuits connect devices (e.g., manual pull stations, heat detectors, smoke detectors, fire sprinkling system water flow switches) to the central control panel. These circuits are used to transmit alarm conditions from the alarm-initiating devices to the central control panel.
- Notification appliance circuits – These circuits connect audible and visual alarm-indicating devices to the central control panel. These circuits are used by the central control panel to provide notification of alarm conditions to building occupants.
- Signaling line circuits – These circuits connect the central control panel to monitoring equipment at locations remote from the premises. These circuits are used to notify agencies responsible for responding to alarm and trouble conditions.

9.4.2.2 Requirements

All panels shall be tested and listed by a nationally recognized testing laboratory (NRTL) for the purpose for which it is intended.

9.4.2.3 Recommendations

Utilize experienced professional fire alarm system designers, such as a Professional Engineer (P.E.) or NICET certified professional. Refer to applicable codes (e.g., NFPA 72) for specific requirements of a fire alarm control panel.

9.4.3 Detection/Initiation

9.4.3.1 Overview

Detection and initiation devices are used to provide early warning of a fire hazard in a building or occupancy. These devices can be single units or be multi-criteria devices. System initiating devices utilized in fire alarm systems include the following:

- Smoke detection
- Heat detection
- Flame detection
- Fire-gas detection
- Human detection (e.g., fire alarm pull station)
- Water flow detection
- Supervisory switches (e.g., tamper, pressure)
- Manual alarm stations

9.4.3.2 Requirements

Detection and initiation devices shall be tested and listed by a NRTL for the application.

9.4.3.3 Recommendations

Utilize experienced professional fire alarm system designers, such as a P.E. or NICET certified professional. Refer to applicable codes (e.g., NFPA 72) for specific requirements of these devices.

9.4.4 Notification Appliances

9.4.4.1 Introduction

Fire alarm notification and signaling appliances protect lives by automatically warning occupants of a fire or related emergency condition, and signaling the need to evacuate the building or area. To achieve its intended purpose, fire alarm notification appliances need to function in a way that ensures the signal is correctly perceived and interpreted by building occupants.

Notification appliances used for fire alarm signaling are almost exclusively designed to operate on low voltage circuits. They are designed this way to continue to function normally on battery backup power in the event of a loss of primary power source from the fire alarm system.

The most commonly utilized notification appliances for fire alarm signaling are audible, visible, or combination audible and visible appliances. Notification appliances are manufactured in a wide variety of appearances, designs, and configurations, but are generally classified in the following categories:

- Audible appliances – bells, chimes, horns, speakers
- Visible appliances – strobes, digital signage
- Audible and visible appliances – chime/strobes, horn/strobes, speaker/strobes

9.4.4.2 Audibility/Intelligibility for Notification Appliances

9.4.4.2.1 Overview

Historically, the only requirement for notification appliances has been to meet audible criteria to notify building occupants of a fire emergency (e.g., sound from a horn). Over time, the fire alarm systems have evolved to include voice commands as a feature of the notification appliance. With the addition of voice commands, systems are now designed to be not just audible, but intelligible. Please note in the new 2016 Edition of NFPA 72, non-listed speakers can be used when a fire alarm speaker does not meet intelligibility requirements.

Many fire codes and standards now state that voice messages be intelligible, however they do not expressly define required levels of intelligibility. ISO 7240-16 *Fire detection and alarm systems — Part 16: Sound system control and indicating equipment* introduces the concept of a common intelligibility scale to assist engineers in designing intelligible systems. An additional source of information on intelligibility is the latest edition of the National Electrical Manufacturers Association's (NEMA) SB-50, *Emergency Communications Audio Intelligibility Applications Guide*.

9.4.4.2.2 Requirements

Public mode signaling shall achieve output levels of at least 15 dB above the average ambient sound level or 5 dB above the maximum ambient sound level, whichever is greater, lasting at least 60 seconds in duration.

Systems shall be designed based on actual measurements of ambient sound conditions and be intelligible.

Occupancies that involve sleeping arrangements require notification appliances that comply with a 520 Hz tone alarm to notify occupants of an alarm condition.

9.4.4.2.3 Recommendations

Utilize experienced professional fire alarm system designers, such as a P.E. or NICET certified professional. In designing an emergency voice system, an experienced professional in sound system design is recommended.

9.4.4.3 Visibility of Notification Appliances

9.4.4.3.1 Overview

Codes and standards have taken a prescriptive approach in describing visible requirements, which makes design of visible notification appliances a straightforward procedure. Even with these prescriptive requirements, a designer is expected to be cautious when designing these systems due to the various interior design schemes (e.g. furniture placement, high utilization of modular furniture systems, etc.).

9.4.4.3.2 Requirements

Fire alarm systems designers and installers shall refer to applicable documents for guidance related to codes and standards compliance (e.g., NFPA 72 has explicit guidelines on placement and functionality of visible notification appliances).

Devices shall be tested and Listed by a NRTL for the application.

9.4.4.3.3 Recommendations

A visible notification appliance is considered by codes to project its luminance outward evenly in all directions. Therefore, a wall-mounted appliance with a coverage pattern that extends an equal distance on either side of the device is recommended.

9.5 Communications Systems

9.5.1 Overview

With the convergence of building technology systems, fire alarm systems are being integrated with communications systems. Whether it is a paging system or an integrated emergency communications system, many codes (e.g., NFPA 72) now offer provisions to incorporate and interface a fire alarm system with these other building technology systems.

Please note if the paging or emergency communications system is not interfaced to the fire alarm system, code requirements (e.g., NFPA 72) may not apply; however, system designers can use codes as a guideline when designing these systems. Codes are not designed to prohibit new technologies from being used, rather they are implemented for life safety purposes.

9.5.2 Requirements

When designing any emergency communications system, a risk analysis is required. The risk analysis is based on the emergency response plan which is site specific. The AHJ shall approve the final system design.

Paging or emergency communications systems used for fire alarm notification shall meet the requirements of applicable fire alarm regulations and codes (e.g., NFPA 72) in addition to those of the paging or emergency communications system

9.5.3 Recommendations.

Designers should consult with the AHJ when introducing new technologies to show they meet or exceed code requirements.

If fire alarm speakers do not meet intelligibility requirements, other speakers may be used. However, it is recommended to have supervision of the speakers. As many of these systems can be quite complex, it is recommended to get the AHJ involved during the beginning design phases of the project.

There are several guidelines that have been published to help in the design of these emergency communications systems. These include the following:

- Partner Alliance for Safer Schools *PASS Safety and Security Guidelines for K-12 Schools*
- NEMA SB-40 *Communications Systems For Life-Safety in Schools*

NOTE: PASS is a volunteer alliance among the Security Industry Association (SIA), the National Systems Contractors Association (NSCA) and other industry professionals. The PASS K-12 team was formed for a singular purpose—to provide school administrators, school boards, public safety and security professionals with guidelines for a tiered approach to securing schools. These guidelines are the first of their kind in the education industry.

9.6 Pathways

9.6.1 Introduction

Codes may classify fire alarm systems signal pathways into various classes based on a number of criteria. The following requirements and recommendations are based on content from the NFPA 72 code.

NFPA 72 defines various pathways as any circuit, conductor, optical fiber, radio carrier or other means connecting two or more locations. Based on their performance, pathway designations fall into one of the following

- **Class A** – includes a redundant pathway, and operational capability continues past a single open. A single open fault and any other conditions that affect the intended operation result in an annunciation of a trouble signal. A single ground fault does not affect operational capability but will also be annunciated as a trouble signal. These pathways are commonly used for notification and signaling line circuits.
- **Class B** – does not include a redundant path, and operational capability stops at a single open. Conditions that affect the intended operation result in an annunciation of a trouble signal. A single ground fault does not affect operational capability but will also be annunciated as a trouble signal. These pathways are also commonly used for notification and signaling line circuits.
- **Class C** – includes one or more pathways, and operational capability is verified via end-to-end communications, but the integrity of individual paths is not monitored. A loss of end-to-end communication is annunciated as a trouble signal. These pathways are typically used with addressable devices and appliances.
- **Class D** – has a fail-safe operation where no fault is annunciated, but the operation is performed in the event of a pathway failure. An example of use for these pathways would be to a magnetic door holder.
- **Class E** – not monitored for integrity. These pathways are normally used for supplemental equipment only.
- **Class N** – includes two or more pathways where operational capability of the primary pathway and a redundant pathway to each device are verified through end-to-end communications. (Exception: When only one device is served, only one pathway is used). A loss of intended communications between endpoints are annunciated as a trouble signal. A single open, ground, short, or combination of faults on one pathway do affect any other pathway. Conditions that affect the operation of the primary pathway(s) and redundant pathway(s) are annunciated as a trouble signal when the system's minimal operational requirements cannot be met. Primary and redundant pathways are not permitted to share traffic over the same physical segment.
- **Class X** – includes a redundant pathway, and operational capability continues past a single open, a single short circuit, a ground fault and a combination open fault and ground fault. All result in the annunciation of a trouble signal. Any other condition that affects the intended operation of the path is also annunciated as a trouble signal. These pathways are typically used for signaling line circuits. There is one exception: requirements for ground faults do not apply to non-conductive pathways (e.g., wireless, optical fiber).

9.6.2 Class N

9.6.2.1 Introduction

With the emergence of building technology systems convergence, Class N was added to the 2016 edition of NFPA 72. Class N impacts the installation of structured cabling infrastructure systems when it is used in conjunction with a fire alarm system; therefore, this document will address this particular class of cabling in greater detail than the other classes previously listed.

NFPA 72 defines the requirements for Class N, but does not define the technology or techniques required to comply with those requirements.

9.6.2.2 Redundant Pathways

9.6.2.2.1 Requirements

Redundant pathways are required between network switches; however, on a section of Class N pathway that services or controls only one endpoint device, a redundant pathway is not required. While one redundant pathway is required, additional redundant pathways are allowed, but not required.

Note that all equipment on a Shared Fire Alarm Network shall be listed for fire alarm purpose, unless the equipment meets the conditions outlined for shared signaling line circuits With applicable fire alarm codes (e.g., NFPA 72).

Normally, a Class N endpoint device encompasses only one device or appliance and a redundant pathway is not required. If an endpoint services more than one device or appliance, it is required to have a redundant pathway (e.g. an amplifier servicing several speakers). Redundant pathways are not required within the same enclosure or raceway within 6 m (20 ft) in the same room.

9.6.2.3 Supervision

9.6.2.3.1 Requirements

Network infrastructure equipment that makes up a Class N network is not defined as Class N devices by NFPA 72. They are considered transport equipment (e.g., switches, routers, hubs) and do not require the specific supervision required for Class N devices.

General supervision is required as they are part of the supervised pathways that service the Class N devices themselves.

9.6.2.4 Secondary Power

9.6.2.4.1 Requirements

Secondary power requirements for Class N apply to all network transport equipment used for life safety and Class N devices. All secondary power sources shall comply with the 2016 edition of NFPA 72, Section 10.6.7, Secondary Power Supply.

9.6.2.5 Shared Pathways

9.6.2.5.1 Overview

Class N pathways utilize network transport devices and NFPA 72 defines levels for shared pathways. Networks are designated as a shared pathway level of 0, 1, 2, or 3 based on their performance. These pathway levels are defined as follows:

- Level 0 – Does not segregate or prioritize life safety data from non-life safety data.
- Level 1 – Life safety data is not segregated, but is prioritized over non-life safety data.
- Level 2 – Life safety data is segregated from all non-life safety data.
- Level 3 – Dedicated equipment for life safety systems.

An example of a Level 0 shared pathway is an unmanaged network. Using Quality of Service or other means, life safety data can be prioritized to meet Level 1 shared pathway. Life safety data can be segregated on a virtual LAN or other means to meet Level 2 shared pathway. By using dedicated equipment for the life safety system, Level 3 shared pathway is achieved.

Although Class N pathways are generally required to be Shared Pathway Level 3, based on the risk analysis and approval of the AHJ, they can also be Level 1 or 2. The general public is not to have access to Class N pathways.

Other considerations for Class N pathways are physical separation of redundant pathways and pathway survivability levels. Class N does not require physical separation of redundant pathways, but local codes, design specification or the AHJ may require it.

A single endpoint device that services an entire zone or area where failure would render that area incapable of initiating input signals or receiving output signals shall not be allowed unless approved by the AHJ.

9.6.2.6 Quality of Service (QoS)

9.6.2.6.1 Requirements

The fire alarm system shall provide a high level of QoS to ensure proper operation of life safety systems.

9.6.2.6.2 Recommendations

QoS settings should be set to the highest level in the electronic equipment within the IT network utilizing Class N.

9.6.2.7 Testing of Circuits

9.6.2.7.1 Overview

When a circuit is used for a Fire Alarm system, testing requirements vary based on the type of conductivity whether balanced twisted-pair or optical fiber cabling. The required initial field testing for each of the following suitable media types is as follows.

9.6.2.7.2 Requirements

Requirements for balanced twisted-pair cabling include;

- Wire map (e.g., continuity, pairing)
- Length
- Insertion loss
- NEXT loss
- ACR-F (formerly called ELFEXT)
- Propagation delay and delay skew
- Return loss
- Power sum near-end crosstalk (PSNEXT) loss
- PSACR-F (formerly called PSELFEXT)

Requirements for optical fiber cabling include;

- Attenuation
- Optical Bandwidth
- Length
- Polarity

9.6.2.7.3 Recommendations

Clearly label patch panel termination and patch cords utilized in equipment rooms.

Provide three (3) copies of documentation/As-built drawings.

Provide three (3) copies of test reports:

- One copy of report to be shared with Owner
- One copy of report to be stored in Fire Alarm Panel
- One copy of report to be stored in the Main Equipment Room

9.6.3 Class N Cabling

9.6.3.1 Requirements

Redundancy and Survivability shall meet applicable fire code requirements and/or as required by the AHJ.

Cable media shall meet the requirements as listed in Section 5.4.

9.6.3.2 Recommendations

When using Class N for a life safety system, it is recommended to use red colored patch cables. This distinction provides an identifying factor to the importance of the system and helps to prevent the unintentional disruption of service.

9.7 Circuits

9.7.1 Overview

There are three different classifications of circuits. These include the following:

- Initiating Device Circuits (IDCs)
- Signaling Line Circuits (SLCs)
- Notification Appliance Circuits (NACs)

Each of these classes is based on their performance capabilities under abnormal (fault) conditions. While each of these circuits are defined based on this criteria, the pathways associated with each of these circuits is as follows:

- IDCs – Class A, B or N
- SLCs – Class A, B, N or X
- NACs – Class A, B, N or X

9.7.2 Requirements

Based on an evaluation of performance capabilities under abnormal conditions, the governing laws, codes, standards and a site-specific engineering analysis, determines the class of circuit to be used. The designed system shall comply with national, state, and local codes and standards.

Devices shall be tested and listed by a NRTL for the application.

9.7.3 Recommendations

Experienced professional fire alarm system designers, such as a P.E. or NICET certified professionals, experienced with national, state, and local regulations and requirements of the AHJ, should be consulted to help assure compliance with applicable regulations and requirements.

9.8 Monitoring and Supervision

9.8.1 Overview

Fire detection and alarm system circuits are typically designed to be continuously monitored (supervised) to ensure a system's integrity. This supervision feature helps facility owners maintain systems in an operable condition and ensures the systems will provide the life safety functions for which they are installed.

In zoned systems, supervision is typically accomplished by current sensing. The central control panel supplies (sources) a small current that continually circulates through the system's circuit. The interruption of the circuit (e.g., removal of a detector or manual station) will cause current flow to change. The control panel, sensing a change in current, will initiate a trouble signal to indicate a problem has occurred with the system.

In addressable systems, supervision is accomplished by electronic polling of individual devices. In response to a query, each device reports its status to the central control panel.

Fire detection and alarm systems may be required to monitor or control auxiliary building components that are not part of the system. Examples of such components include:

- Fire and smoke dampers in heating, ventilating, and air conditioning (HVAC) ductwork
- Door closers (kickers) for doors in fire-rated partitions
- Flow devices on fire sprinkling equipment

An IP based system is inherently monitored and supervised in that the system is constantly checking end-to-end communications.

A monitoring or control module is used to interface these auxiliary components with the central control panel. Circuits that connect monitoring and control modules to the fire detection and alarm system control panel are supervised in the same manner as are detectors and manual pull stations. However, the interface circuit between a monitoring or control module and the auxiliary building component being controlled is usually unsupervised. These unsupervised circuits have the potential to be a weak link in the overall system of supervision.

Monitoring/supervision of the various classes of fire alarm systems include:

- Protected premises system
  This type of system can be locally or remotely monitored by the client or maintenance personnel but is not a supervised station class of system.
- Supervising station system
  This system is continuously monitored by a central monitoring company for any abnormal events.
- Household fire alarm system
  Residential occupancies that contain fire-warning equipment provide a reliable means to notify the occupants of the presence of a fire and the need to egress to a safe location.

Remote Monitoring may be provided by:

- IP-enabled fire alarm system
- Network-based monitoring
- Digital alarm communicator transmitter (DACT)
- Supervising station system
- Central station service

9.8.2 Requirements

Designed system shall comply with national, state and local codes and standards.

Monitoring for integrity between enclosures containing control equipment located within 6 m (20 ft) of each other where the conductors are installed in conduit or equivalently protected against mechanical injury is NOT required.

9.8.3 Recommendations

Experienced professional fire alarm system designers or engineers experienced with local regulations and requirements of the AHJ should be consulted to help assure compliance with applicable regulations and requirements.

9.9 Power over Ethernet (PoE) Implementation

9.9.1 Overview

Fire alarm equipment and devices designed to function on Class N may be powered from PoE.

9.9.2 Requirements

PoE devices shall comply with Section 5.4.4.

9.9.3 Recommendations

Refer to section 5.4.4 for a list of recommendations.

9.10 Class N Operations and Maintenance

9.10.1 Overview

Scheduled maintenance and abnormal operations shall be logged and reported in accordance with the 2016 edition of NFPA 72.

9.10.2 Requirements

Refer to the 2016 edition of NFPA 72.

9.10.3 Recommendations

Experienced professional fire alarm system designers or engineers experienced with local regulations and requirements of the AHJ should be consulted to help assure compliance with applicable regulations and requirements.

9.11 As-Built Drawings and Related Documentation

9.11.1 Overview

As-built drawings and related documents are important to the overall success and acceptance of the project. Refer to the AHJ and governing laws to make sure you have all of the required documentation to complete the project.

9.11.2 Requirements

Accurate as-built drawings shall be provided by the installer showing the actual installation when the work is complete. The drawings shall reflect the pathways utilized. The as-built drawings shall contain a copy of all manufacturer’s data sheets, system software, and device database. The as-built drawings shall also include battery calculations and NAC calculations.

9.11.3 Recommendations

Installers and designers should always follow project documents, manufacturer's recommendations and applicable codes and regulations. As-built drawings should utilize a set of industry recognized symbols or project specific symbols (e.g., NFPA 170).

10 Integrated Systems

10.1 Overview

This section includes concepts, systems, and processes related to the integration of ESS systems. Integration of ESS systems allows various systems to share information, command, and control with a range of other systems, including:

- Data networks
- Building automation
- Fire-life-safety
- Energy and lighting management
- Automated infrastructure management (AIM) systems

Integrated ESS systems are deployed in many environments, including:

- Cities
- Facilities
- Campuses
- Vehicles
- People

These integrated systems can utilize common infrastructure, input, output, or data networks for information transmission, including both wired and wireless information technology systems.

Integrating various IP based systems across multiple sites have been observed to provide the following benefits:

- Number of servers and storage requirements lowered
- Reduction in false alarms in video surveillance areas
- Risk mitigation by expediting maintenance and repair
- Time required investigating security incidents reduced
- Reduction in maintenance, monitoring and control costs
- Virtualization and emergence of new solutions
- Simplified user training

NOTE: A site's specific conditions may affect the ability to meet these values.

10.2 ESS Integrated Services, Design and Integration

10.2.1 Public Network Services

10.2.1.1 Introduction

Public network services are often referred to as the public switched telephone network (PSTN). This is the global network of circuit-switched telephone networks available to the general public. The PSTN consists of telephone lines delivering user services via some combination of infrastructure. This infrastructure includes optical fiber cabling, microwave transmission, cellular networks, communications satellites, and undersea telephone cabling, all of which is interconnected by switching centers (e.g., telephone company central office locations), thus allowing any telephony device (e.g., fixed line, mobile phone) in the world to communicate with any other such device.

The technical operation of the PSTN utilizes standards created by the International Telecommunication Union (ITU). These standards allow different networks in different countries to interconnect seamlessly. Industry standards provide for a global numbering system to assign telephone numbers. The interconnected networks and the global numbering system make it possible for any telephony device to connect to any other telephony device in the world.

10.2.1.2 Requirements

The integrated systems shall utilize one or more of the following types of networks for their information transmission:

- Public switched telephone network (PSTN)
- Personal area network
- LAN
- WAN
- Metropolitan area network
- Cellular wireless (e.g., TDMA, CDMA, GSM)
- Mesh wireless—licensed and unlicensed frequencies
- Point-to-point (PTP) wireless—licensed and unlicensed frequencies

10.2.2 Design and Selection of Components

10.2.2.1 Requirements

The functional requirements provide the criteria for the design and selection of components. The criterion is categorized based on performance, operational and functional considerations and codes and standards. The criterion shall include:

- Codes and standards
- Quality
- Capacity
- Performance

10.2.3 ESS Integration

10.2.3.1 Requirements

ESS integration shall integrate ESS systems using network protocols. The control systems of an integrated solution shall employ:

- Web servers
- Graphical user interfaces (GUIs)
- Database technologies
- Software components (e.g., intelligent agents)
- Similar decision support and active response systems

Integration of systems with fire, life or safety systems may cause the integrated system to be classified as a fire, life or safety system. Integrated systems shall meet all requirements of all applicable codes and AHJs.

10.3 ESS Components

10.3.1 Overview

This section details the ESS components and the networks, systems, and software involved in the integration of ESS systems. In addition to ESS components, there are other systems found at various sites that can be integrated into the ESS system.

10.3.2 Intrusion Detection System

10.3.2.1 Overview

IDS may include physical intrusion of premises for the purpose of monitoring and reducing threats to persons and property, as well as network-based IDS. Hardware- and software-based systems are specifically designed to monitor and control or mitigate malicious network attacks for the purpose of protecting the intellectual property and any integrated system used for monitoring, reporting on, and controlling a facility.

The following devices may serve as physical intrusion sensors:

- Contact closures (switch), including:
  - Magnetic
  - Pressure
  - Mechanical
- Motion sensors, including:
  - PIR
  - Microwave
  - Photoelectric
  - Laser
  - Ultrasonic
  - Proximity

The types of network IDS sensors include hardware and software devices connected to a LAN or WAN typically using TCP/IP. These systems are designed to monitor ports and network activity for specific malicious signatures. Once detected, the system may reset a TCP or user datagram protocol session, flag and disallow any future sessions originating from a suspected IP address, or report an alarm to a file server or a central management GUI without user intervention.

10.3.3 Access Control System

10.3.3.1 Recommendations

ACS systems may include:

- Card access control for buildings
- Emergency exit controls
- RFID for inventory and asset tracking
- Time and attendance
- Industrial and manufacturing systems

Many ACSs and IDSs already provide enterprise-level solutions that integrate these systems. The ACS is provided with inputs so that the sensors can be monitored for trouble and alarm conditions.

10.3.4 Video Surveillance System

10.3.4.1 Recommendations

Video surveillance systems may include:

- Remote video
- Advanced integrated surveillance systems
- Distributed integrated active remote multi-camera networks
- Database-integrated object recognition systems
- Binary change detection
- Active head tracking and face cataloging
- Video content analysis systems

Surveillance systems fall into the general categories of hardware control, analog matrix, digital video matrix, digital video management, and software as a service.

10.3.5 Physical Security Information Management System

10.3.5.1 Overview

Physical security information management (PSIM) is a product that integrates systems from various security system manufacturers and allows the integration of security into a single unified situation management platform. Figure 10-1 provides an example of a PSIM.

The digital video management system manages video content, while the PSIM system combines video management for security and surveillance applications with situation (incident and event) management. The PSIM system actually can act as a gateway to multiple systems and set up interface, interoperability, and event collection.

10.3.5.2 Requirements

Designs shall utilize the PSIM system as a user interface when multiple systems at a facility exist and require interoperability with a surveillance system.

10.3.6 Sensor-Based System

10.3.6.1 Overview

ESS sensor-based systems incorporate the use of various analog and digital devices that respond to physical changes or outside influences. This response may be in the form of generating an electrical signal, a change in state of an open or closed contact, or the fluctuation of resistance, capacitance, or current between two or more conductors.

10.3.7 Building Automation System

10.3.7.1 Overview

Refer to applicable standards (e.g., TIA-862-B) for specific information about BAS systems.

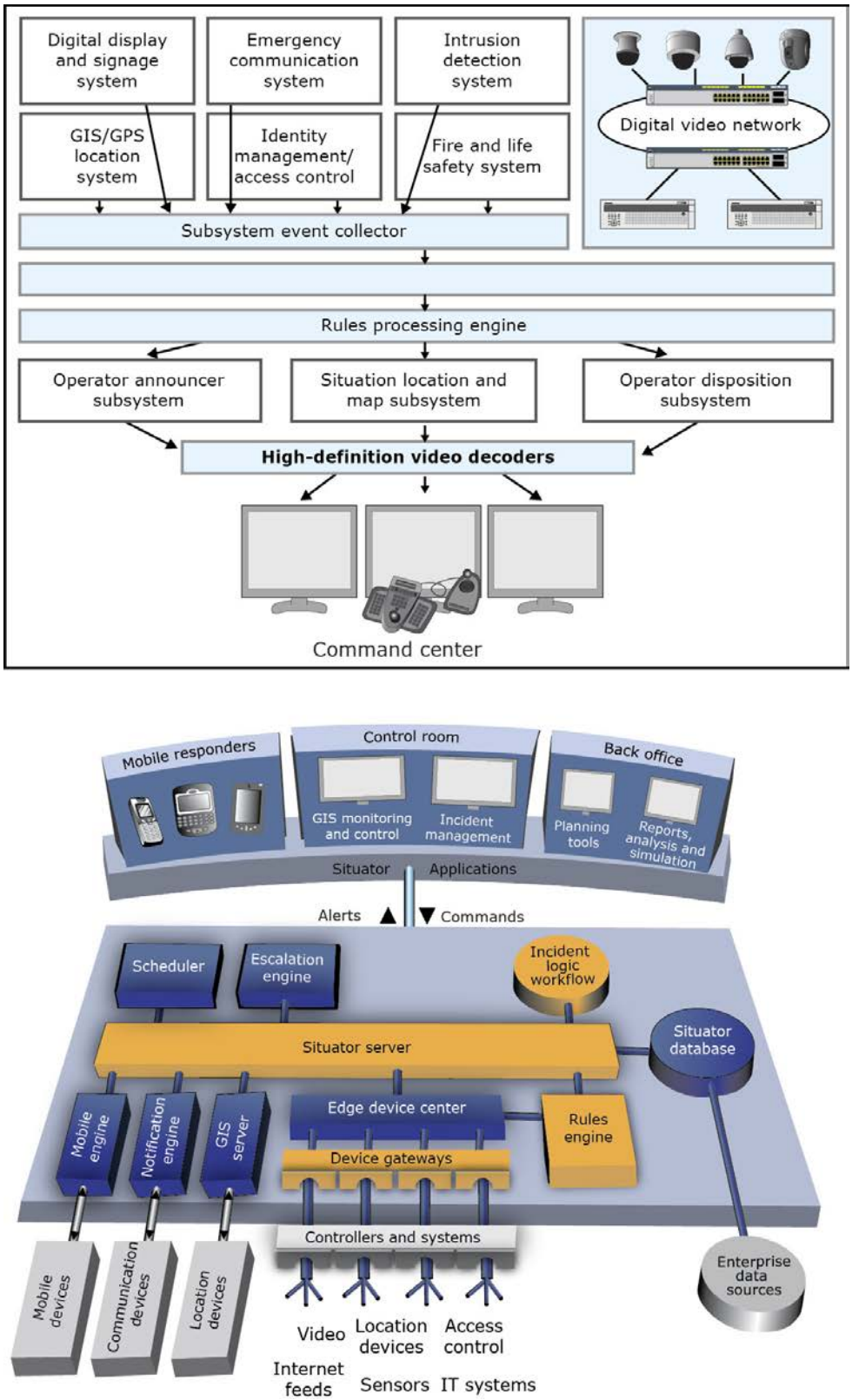

Figure 10-1
Sample Physical Security Information Management System

10.3.8 Location System

10.3.8.1 Recommendations

Location systems may be grouped by technology or method of deployment.

Automotive engineers work to reduce the number of collisions by introducing advanced safety systems that sense impending danger.

Systems being developed combine sensor technology with x-by-wire systems that use electronics to control braking, steering, and suspension and vehicle control systems that may sense the proximity of a pedestrian or animal. This combination introduces the opportunity to create automatic collision avoidance systems that will greatly increase the safety of our roadways. Some systems are already integrated into aircraft cockpits.

10.3.9 Global Positioning System

10.3.9.1 Overview

Location systems such as a global positioning system (GPS) provide two kinds of information:

- Physical
- Symbolic

A GPS provides physical positions. A physical position may be augmented to provide corresponding symbolic information with additional information, infrastructure, or both. GPS uses space satellites as reference points for Earth locations. Distances are measured from the three satellites used in triangulation calculations. The exact locations are pinpointed using these calculations.

GPS tracking works on the following principles:

- The basis of GPS, which is triangulation from satellites.
- To triangulate, a GPS receiver measures distance using the travel time of radio signals.
- To measure signal travel time, GPS needs very accurate timing, which it achieves by applying special methods.
- Along with distance, the location of the satellites needs to be determined.

10.3.9.2 Requirements

Designs incorporating a GPS shall allow for correction to compensate for any delays the signal experiences as it travels through the atmosphere.

For proper communications, a robust, continuously connected wireless national data network is required. As an alternative communications link, a satellite network is required for areas where a ground-based wireless signal is weak.

10.3.10 Automated Infrastructure Management (AIM) with other ESS systems

10.3.10.1 Recommendations

AIM should be considered as an additional means to enhance the security of ESS in a building. The following list of automated administration functions and features may be integrated into other ESS systems.

- Detect changes to patch cord connectivity
  Unauthorized changes to the patch cord connectivity should be detected and reported to the appropriate authority in real time. Real time event notification may be sent to the network manager using a variety of methods (e.g. email, text messaging, and SNMP traps). It is also useful to forward such events to network monitoring applications to enable a consolidated view of all activities on the network. For example an integrated system that incorporates inputs from multiple security systems is shown in Figure 10-1.
- Port status information
  All ports on the network including network equipment, switches, patch panels and telecommunication outlets should be monitored in real time for the purpose of detecting unexpected or unauthorized activities. Any port usage changes should be communicated to the network manager using variety of methods (e.g., email, text messaging, and SNMP traps.)
- Device alarms
  The AIM system should be capable of detecting and reporting device connection or device disconnection and identify the associated location. This information can be used to establish whether this is an authorized connection or disconnection in order to ensure that the security of the network is not compromised.

List continues on next page

- Security camera integration
  The AIM system should be capable of being integrated with security cameras, to activate these during unauthorized events and provide access to recorded content.
- Communication with other systems
  The AIM system should be able to communicate or exchange data with and consolidate information from other systems and databases. The information available to an authorized network manager should also be made available to an authorized program that needs AIM information.
- Emergency call origination location
  The AIM system should have the capability to be queried and report the location of a connected device based on a port and outlet connection. This location information may be utilized to enhance the ability of the voice/emergency response system to identify the originating location of a call.
- Secure communications and operation
  The AIM systems should protect itself from unauthorized access by using secure access to AIM components. This may include one or more of the following methods: log in security credentials at AIM access points, locked rooms/cabinets, access control systems for rooms/cabinets that contain AIM equipment, security cameras.

10.3.11 Software

10.3.11.1 Overview

The functionality and reliability of an integrated system relies heavily on the system management software and underlying system software. The selection of the system and software is a critical step in purchasing and implementing a project.

The software poses the biggest risk to most integrators due to the lack of in-house capabilities to make modifications to the software beyond the standard configuration. An additional concern is the lack of access to the source code required for vendors to make changes to commercial off-the-shelf software platforms, or integrators to make changes to proprietary software platforms

The development of an integrated system at the vendor level is often based on the current version of the database and operating system software available. The change from one operating system to another is a major undertaking by a vendor and of strategic importance in the marketplace.

There is often a tradeoff between delivering a system on the latest software platform and fielding a robust or reliable system. Some vendors offer choices in the database and operating software, and there are tradeoffs with any choice.

Similar to any technology-based product, significant problems may be encountered on systems deployed with recently released operating system platforms.

10.3.11.2 Databases

10.3.11.2.1 Overview

The selection of database software is typically based on availability from the hardware vendor or compatibility with existing systems, between integrated systems, or with client databases. Selections can be based on personal preference or experience of the integrator, client, or AHJ.

10.3.11.3 Control and Monitoring

10.3.11.3.1 Overview

Many vendors offer control or monitoring software in the form of an enterprise solution. This allows the control and monitoring of multiple ESS server systems from a central location. Some vendors provide management software to facilitate the integration, control, and monitoring of individual systems. Other systems facilitate the integration of traditional ESS systems with fire detection, building management, and human resources.

10.3.11.4 Scalability, Resiliency, and Reliability

10.3.11.4.1 Introduction

The ultimate goal in selecting a software platform is to meet not only the current system needs but also the needs of the system in the future. This is particularly true of an installation for a new client or a client in a new facility.

Systems are often expanded during the installation phase or just after when the client begins to understand the system capabilities. Expansion plans for the facility and the procurement of additional facilities play a role in determining the long-term system requirements.

The procurement of additional facilities or the installation of systems in additional existing facilities may warrant an enterprise approach to facilitate single point monitoring and control.

The anticipated number of devices and users will be a deciding factor in the selection as well.

The criticality of the system operation and assets protected also determines the software selection. The need for a fail-safe system often requires the use of servers with robust storage solutions such as redundant array of independent disks (RAID) systems. The implementation of these scenarios now or in the future will have a significant impact on the selection of a software platform.

10.3.11.4.2 Recommendations

The system should have the capability of being scaled to meet the current and future needs of the client.

10.4 System Configuration and Expandability

10.4.1 Overview

Planning for expandability can be incorporated into the design process. Input and output points will be identified in the design, but additional inputs and outputs are required during the installation phase to accommodate additional sensors, functions, and modifications to the original design.

An error, such as not providing adequate motion detection or an unaccounted tamper switch, can be costly if the hardware and software do not have room for expansion.

The addition of an inexpensive tamper switch may ultimately cost thousands of dollars to add an additional field device, power supply, or ESS infrastructure to support the new hardware.

10.4.2 Input/Output Matrix

10.4.2.1 Introduction

The completion of an input/output matrix is a vital step in determining system expansion requirements for larger complex systems.

10.4.2.2 Requirements

The matrix shall be configured for a specific system and needs to contain the following basic information:

- Input or output type and number
- Processor or field panel number
- Card reader type and number
- Zone number (input/output grouping)
- If an input or output is active 24 hours a day

10.4.3 Maps and Icons

10.4.3.1 Introduction

Maps and icons should be coordinated with the AHJ and end user to enhance the ability of the operator to monitor the system. The maps should be configured to provide an overview of the system and allow the operator to select or drill down into the submaps. Each alarm or event that needs a map display will need to be evaluated to determine the lowest level map to effectively display the location.

The display of a detailed map of a particular floor of a building may not suffice on a site with multiple buildings with similar layouts. The site map, or a portion thereof, may be the lowest level map to show the location of an event or alarm. The operator can then select the icon to display the detailed map.

The icon should readily display the status of an event or alarm and should change as the state of the associated device changes.

Another effective tool is to assign one icon per zone, area, or building on a site in a way that the site map provides an overall view of the status of the system. The operator can view one map to determine the status of a large area, while the submaps are only accessed to view particular devices.

10.4.3.2 Recommendations

The maps should be configured such that any additions to the system are readily incorporated.

The AHJ can provide input as to future plans, but the system maps should be configured to match the expansion capability of the system hardware as installed. The addition of event or alarm icons to the maps may necessitate a reconfiguration of the mapping system.

10.4.4 System Response Times

10.4.4.1 Requirements

The response times shall be calculated for peak use times. Distributed processing reduces the response times significantly.

10.4.4.2 Recommendations

The system response times should be calculated because they are an effective tool in determining the need for lighter system loading on a distributed system. The goal of system response times is to determine the processing and reporting times for alarms or system requests.

10.4.5 System Expansion Capability

10.4.5.1 Overview

The expansion capability of the system hardware is based on the as-built and future expansion capability. The as-built capability is the number of available physical connections, including:

- Inputs
- Outputs
- Card readers

The future capability is how much the system can be physically expanded by adding hardware.

The physical layout impacts the system expansion.

10.5 ESS Integration Process

10.5.1 Overview

In order to properly define and integrate multiple systems, operational and functional requirements are necessary. These requirements are the framework for the integrated system. They will be the basis against which all system expectations and testing will be measured.

Defining how the system is intended to behave is the most important step in the integration process. How each individual system is put together will impact the ability to make the systems work together. Each system will have to meet applicable standards and codes in addition to how the end user wants the system to function as a whole.

Before the design process begins, general requirements for how the final system configuration will function are expected to be defined. These general requirements can range from very simple to very complex.

10.5.2 Integration Process Team Members

10.5.2.1 Introduction

In order to properly define the process and generate the proper documentation to integrate various ESS systems, a team of knowledgeable persons and project stakeholders needs to be established.

10.5.2.2 Recommendations

Project stakeholders should include:

- ESS designer
- Operations personnel
- Information technology (IT) personnel
- Key facilities personnel
- Security personnel
- End users
- Financial stakeholders

10.5.3 Integration Process

10.5.3.1 Step 1: Develop a Requirements Traceability Matrix

10.5.3.1.1 Requirements

There shall be a discovery period with all of the integration process team members. The team members shall determine which systems are to be integrated and define the functional requirements.

The requirements traceability matrix is a document that defines the requirements and provides traceability between the approved requirements, design specifications, project scope and written direction regarding the project. The document is typically in a spreadsheet format. The columns shall be organized into two areas: requirements definition and implementation.

Traceability Matrix Definition Elements/Columns Requirements

The following items shall be used as column headings in a traceability matrix:

- *ID* – This is a unique ID number that is used to identify the traceability item in the matrix.
- *Associated ID* – This column is optional. This provides an additional ID to link other matrix or spreadsheet elements.
- *Requirement Source* – This column identifies the requirements origin. This can be a project scope, design guide, client interviews, or other applicable sources.
- *Functional Requirement* – This column shall contain a description of the functional requirement.
- *Status* – This column shall be populated with the current status of the functional requirement. This can be a yes or no field or a percentage of completion that parallels the project submission levels of effort.
- *Design Document* – This column contains the project document where the requirement is captured. This can be drawings, specifications or a report.
- *Interface Required* – This is a yes or no column. Not all requirements need an interface as requirements can be as simple as a design direction.
- *Systems Interfaced* – This column identifies the system or systems that are interfaced.

Implementation Elements/Columns Requirements

The following items shall be used as column headings in a traceability matrix:

- *Technical Specification* – This column shall provide a description of the technical specifications linked to the functional requirements.
- *System Component* – This column shall provide a description of the system components linked to the functional requirements.
- *Software* – This column shall provide a description of the software linked to the functional requirements.
- *Functional Requirement Location* – This column shall identify the location in the functional requirements document where the requirement has been implemented.
- *Quality Assurance/Quality Control (QA/QC) Matrix Document* – If used, this column shall provide a description of the document linked to the functional requirement. This is only used when linked to a separate QA/QC document.

10.5.3.2 Step 2: Develop an Integration Plan

10.5.3.2.1 Requirements

An integration plan is required to properly define the process. This written functional description shall define the expectations of the system and describe in detail the requirements of the integrated system versus the individual systems.

The integration plan shall contain the following:

- *Title Page* – The title page should contain the following information:
  - The company for which the integration plan was developed
  - Contract number or document tracking number
  - Date that the document was formally approved
  - The organization responsible for preparing the document
  - Revision version and date issued
- *Purpose of the Document* – The integration plan provides a brief statement describing the overall purpose of the document. It is the plan for integrating the components and sub-systems of the project prior to verification
- *Scope of the Integration Project* – This section gives a brief description of the planned project and the purpose of the system to be built. Special emphasis is placed on the project's deployment complexities and challenges.
  This section may be lifted from earlier documents. It is important only to people [stakeholders] who will be introduced to the project for the first time by this document.
- *Integration Strategy* – This section provides an overview of what the high level plan is for integration and, most importantly, why the integration plan is structured the way it is. The Integration Plan is subject to several constraints, sometimes constraints that conflict with one another. It is part of the larger process of build, integrate, verify, and deploy, all of which shall be synchronized to support the same project strategy. For even a moderately complex project, the integration strategy, based on a clear and concise statement of the project's goals and objectives, is described at a high, but all-inclusive, level. It may also be necessary to describe the analysis of alternative strategies to make it clear why this particular strategy was selected.

The following section describes the integration process. It identifies what components are integrated at each step and gives a general idea of what threads of the operational requirements are covered. It ties the plan to the previously identified goals and objectives so the stakeholders can understand the rationale for each integration step. This section also defines the schedule for all the integration efforts.

- *Integration* – Define and explain each step in the integration process. The intent is to identify all the needed participants and to describe their responsibilities.
  Each of the integration steps should identify:
  - The location of the activities.
  - The project-developed equipment and software products to be integrated. Initially this is just a high level list but eventually the list shall be exact and complete, showing part numbers and quantity.
  - Any support equipment needed for this integration step, such as:
    - Special software
    - Test hardware
    - Software stubs
    - Drivers to simulate yet-to-be-integrated software components
    - External systems

    NOTE: The same support equipment is most likely needed for the verification phase.
  - All integration activities that need to be performed after installation, including integration with on-site systems and external systems at other sites.
  - A description of the verification activities that occur after integration.
  - The responsible parties for each activity in the integration step.
  - The schedule for each activity.

10.5.3.3 Step 3: Develop a Testing and Commissioning Plan

10.5.3.3.1 Requirements

All systems shall be verified that the installed components are integrated and functioning as set out in the design. The following is a list of all documents used to develop a testing and commissioning plan. This almost always includes the integration plan and the requirements documents. Other reference documents, such as descriptions of external systems, standards, a concept of operations, and manuals will need to be included.

The testing and commissioning section of the plan provides details on how the testing is accomplished. In addition the plan defines:

- Who does the testing
- When and where it is to be done
- The responsibilities of each participant before, during, and after each test
- The hardware and software to be used
- The documents to be prepared as a record of the testing activity
- How testing failures are identified and corrected.

The following information shall be included in this section:

- A description of the participating organizations and personnel and identification of their roles and responsibilities. This may include for example, a test conductor, test recorder, operators, or engineering support.
- Identification of the location of the testing effort including the place or places where the testing progress shall be observed.
- The hardware and software configuration for all of the test cases, including: hardware and software under test and any supporting test equipment, software, or external systems. Several configurations may be necessary.
- Identification of the documents to be prepared to support the testing, including: verification procedures, a verification report, and descriptions of special test equipment and software.
- Details on the actual conduct of the testing, including:
  - Notification of participants
  - Emphasis on the management role of the test conductor
  - Procedures for approving last minute changes to the procedures
  - The processes for handling a test failure, including: recording of critical information, determination of whether to stop the testing, restart, or skip a procedure, resolution of the cause of a failure, and determination of the retesting activities necessary as a result of the failure.

10.5.3.3.2 Test Cases

10.5.3.3.2.1 Requirements

Identify the specific tests or groupings of tests to be performed. These tests and performance criteria are identified in the Requirements Documents. There may be several individual requirements that are defined and they can be verified in one test case.

They shall be related and combined into a specific set of test procedure actions.

10.5.3.3.2.2 Recommendations

Each test case should contain at least the following information:

- A description name and a reference number
- A complete list of the requirements to be verified. For ease of tracing of requirements into the verification plan and other documents, the requirements are given numbers. They can be accurately and conveniently referenced without repeating all the words of the requirement.
- A description of the objective of the test case, usually taken from the wording of the requirements, to aid in the understanding of the scope of the test case.
- Any data to be recorded or noted during the test, such as expected results of a test step. Other data, such as a recording of a digital message sent to an external system, may be required to verify the performance of the system.
- A statement of the pass/fail criteria. Often, this is just a statement that the system operates per the requirements.
- A description of the test configuration. That is a list of the hardware and software items needed for the test and how they should be connected. Often, the same configuration is used for several tests.
- A list of any other important assumptions and constraints necessary for conduct of the test case.

10.5.3.3.3 Verification

10.5.3.3.3.1 Introduction

There are steps to set up each verification configuration, including, but not limited to:

- Tuning of the hardware
- Configuring and starting the software
- Starting the special test software
- Set-up steps at each external system to be used

There are steps to be taken by the ESS designer for each verification case. Each step includes:

- Operator action to be taken
- Expected results
- Pass / fail entry space
  The ESS designer records whether or not the expected result occurred. If the expected results are not observed, then the procedures for dealing with failures are contained in the Testing and Verification Plan.
- A trace of each verification step from a verification case in the applicable verification plan and a trace from a requirement in the applicable requirements document.

10.5.3.3.3.2 Recommendations

If possible, acceptable limitations should be documented. These documents should be dated and treated as a living document. As parties on the project change, the functional description can be used to introduce new members to the project. Once an initial functional description is filed, a method for changing the document should be devised and implemented.

Once the general system description has been developed, the engineering and design process for the integrated system should begin. If the system is not a legacy system, all of the subset systems should be designed with the overall integration in mind.

Each system can be designed independently and may account for additional recommendations for integration prior to design completion. As these systems are built, any inherent flaws or newly exposed issues can be investigated and changes can be implemented to the functional description, if necessary.

Obtain references of operational systems that meet the same system requirements (or similar requirements) and request the ability to contact the end user. Discuss the limitations of any item that may impact the system functionality. An existing process will not necessarily work when trying to implement an integrated system with new technologies.

The architectural design should be reviewed and evaluated for spacing requirements, control room layouts, and access points. The design of the individual systems also should be in accordance with the need to integrate them together. Panel locations and network connections become important when trying to eliminate cabling or cross-system connection points.

11 Risk Management and Risk Assessment

11.1 Introduction

This section is intended to provide guidance when performing a risk assessment.

A security survey or analysis should be completed during the preplanning and planning stages of construction, then annually upon occupancy. The following are items typically identified during a security survey:

- The identification of assets
- The identification of natural, technological and human threats
- The probability of risk
- The past and future losses of the complex or building
- The potential impact of losses and risk
- Possible countermeasures
- Cost/benefit analysis of proposed countermeasures

11.2 Requirements

The designer shall identify the risk management policy.

- If a risk assessment has been completed, the designer shall utilize this document as a guide to identify the assets that are to be protected.
- If the risk assessment has not been completed, the designer shall thoroughly assess the assets to be protected, environment, and any potential risks that exist or could develop.

The designer shall analyze architectural and operational security. The impact of protection shall be compared with the impact of loss. The designer and integrator shall consider existing systems and ensure compatibility with any new systems.

The designer shall detail the conditions that the installer is likely to encounter.

The designer shall compile the identified threats and risks to the assets and provide appropriate mitigation techniques or strategies.

11.3 Additional Information

There are various types of assets. Examples include:

- People – Tenants, customers, employees, contractors, guests, and in some instances, even trespassers
- Property – Real and personal property of monetary value
- Operations – Patents, processes, reputation, and goodwill
- Information – Proprietary data, trade secrets, and business plans

There are various types of threats and risks:

- Threat is an indication of an event or the intent to do harm or damage.
- Risk is a vulnerability to or potential for loss from a threat or event.

There are four types of mitigation strategies: physical, electronic, operational and logical

- Physical – Physical countermeasures include doors, gates, fencing, landscaping, lighting, glazing, infrastructure, vehicular standoffs and protection, locking mechanisms, and air intake, separation, partitioning, and distribution. The concept of crime prevention through environmental design also falls within the realm of physical security countermeasures.
- Electronic – Electronic countermeasures include card readers, cameras, electrified locking mechanisms, sensors, and other electronic devices.
- Operational – Operational security countermeasures include, guard post requirements, patrols, training, policies and procedures, and emergency preparedness and contingency factors.
- Logical – Countermeasures include, application and software vulnerability testing, source code analysis, application of patches and updates, and user training. This component is typically a specialized area under information security.

This page intentionally left blank

12 Commissioning

12.1 Overview

Commissioning is often one of the most neglected aspects of system installation. A system that is properly tested and commissioned will provide the ESS designer, installer, and client with a system that functions correctly, meets the client's requirements, and can help foster a continuing professional business relationship between the ESS designer and client for future work.

Commissioning an ESS system should clearly identify real and potential issues with the physical security systems and the affiliated subsystems during all phases of the project.

Commissioning verifies that the ESS systems operate consistent with the contract and specification documents and must include:

- Operation and maintenance documentation.
- Cleaning.
- Labeling devices, cabling, and equipment.
- Testing, adjusting, and settings.
- Training for client personnel.

12.2 Documentation

12.2.1 Overview

Clients and contractors alike often overlook the importance of this commissioning documentation, which is critical for the successful operation and maintenance of the installed system.

12.2.2 Requirements

Documentation must be produced to support each phase of the commissioning process, including the preliminary testing and calibration plan. The plan must include each device in the system (e.g., access control devices, door position switches, intrusion detection points, video cameras, intercoms). The plan must be based on the manufacturer's standard written commissioning procedures and include the manufacturer's standard field checkout sheets as part of the final project documentation.

In addition to testing each device, the commissioning technician shall also test all system bonding and grounding, copper cabling, and optical fiber cabling.

12.2.2.1 Operation and Maintenance Manuals

The operation and maintenance manuals must include detailed installation, operating, troubleshooting, and maintenance procedures. Security contractors should not simply submit manufacturers' user manuals as the required documentation. It is important that security contractors also prepare site-specific instructions for routine and emergency operations and maintenance.

The operation and maintenance manuals also should contain complete warranty information, including the client's responsibilities for maintaining the warranty in full force. Warranty cards or other documents that are required to be returned to the manufacturer must be completed by the security contractors and mailed back with copies provided in the final documentation given to the client. The manufacturers of each system component must be listed along with contact details and part numbers, including any custom manufactured components.

Additionally, any certifications provided by the manufacturer that indicate compliance with any regulatory requirements, codes, or standards shall be included in the operation and maintenance manuals.

12.2.2.2 Record Drawings

Record drawings setting out as-built conditions of the systems must be included in the manuals. As-built drawings are shop drawings and consolidated information from the marked up set showing the final as-built conditions. These drawings are to be used and kept current throughout the life of the system.

Record drawings should contain the manufacturer and model number of each component as well as its location and orientation, raceway, and cable tray locations and sizes. The record drawings must also include the identification of each component and cable termination that corresponds with the cable labeling and component nameplates. Equipment loading schedules, clearly identifying terminations and spare capacity, are also a critical part of accurate record drawings that are invaluable in the maintenance and future moves, adds, and changes (MACs) to the system.

12.3 Cleaning

12.3.1 Overview

A major task in commissioning security systems is the cleaning and removal of dust, dirt, and temporary covers.

12.3.2 Requirements

All devices and enclosures, including those used in outdoor applications, must be inspected to ensure that the finish has not been damaged during the installation. The cleanliness of the system must be maintained by the security contractor until the date of completion and final acceptance by the client for all of the work.

12.3.3 Recommendations

All foreign debris should be removed from the equipment and enclosures. The cleanliness of outdoor mounted video surveillance camera domes is extremely important and should be regularly maintained.

12.4 Labeling Components

Labeling the equipment and cables is a vital part of ESS system commissioning. Labeling will support the relationship between components and as-built or record drawings and prove their value in future repair, troubleshooting, or MACs of an ESS system.

12.4.1 Requirements

Components require labeling with identification numbers or letters that accurately correspond to the drawings. Cables must be marked with machine-printed permanent labels at each end. Cables and terminations should be marked in accordance with applicable standards (e.g., TIA-606-B, ISO/IEC 14763-2).

Labels and identification plates affixed to rack- or wall-mounted ESS equipment shall be located so that they are easily read. Electrical circuits feeding ESS equipment must be clearly identified at electrical receptacles, junction boxes, and distribution panels.

12.4.2 Recommendations

Enclosures and other large components typically should have engraved plastic or metal identification plates.

12.5 Testing

12.5.1 Acceptance Testing Plan

The acceptance testing plan will be used by the client during the final acceptance test as part of the turnover documentation.

12.5.1.1 Requirements

Testing documentation must include full details of all commissioning tests as well as factory testing reports provided by the manufacturer with the equipment.

The plan needs to 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.

12.5.1.2 Recommendations

Clear acceptance testing guidelines should be provided in the construction specification documents. The guidelines must define the performance requirements for the ESS system.

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.

12.5.2 System Testing

12.5.2.1 General

Testing occurs in the stages described in the following sections, with each section having additional requirements or recommendations.

12.5.2.1.1 Testing Requirements

Equipment must be calibrated according to the manufacturer’s recommendations and whenever damage is suspected. Calibration certification must be kept on record and copies for each tester provided in turnover documents.

12.5.2.1.2 Testing 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.

12.5.2.2 Preinstallation Testing

12.5.2.2.1 Overview

Preinstallation tests may reveal components that have been damaged in shipment and need to be replaced. Some subsystems may have components that have been pretested prior to installation. Examples of such subsystems are operable vehicle barriers, gates, and other major subsystems.

12.5.2.2.2 Recommendations

Components (e.g., video cameras) also should be run through a quick functional test prior to installation. Systems that require calibration or adjustment can be serviced in the shop instead of in the field.

12.5.2.3 Preliminary Testing and Calibration

12.5.2.3.1 Requirements

Each alarm point shall be tested. For example, for intrusion detection and video camera call-up and recording:

- Video cameras shall be tested for resolution, light sensitivity, focus, and where applicable, pan, tilt, and zoom (PTZ) control.
- The graphical user interface system response shall be tested for functionality.
- Intercom systems shall be tested for proper operation as well as sound quality. This is followed by a burn-in period.

12.5.2.3.2 Recommendations

ESS 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. Some examples are testing each access control device for door prop alarms, forced door alarms, and valid and invalid card reads.

12.5.2.4 Burn-in Period

12.5.2.4.1 Recommendations

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 operate 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. The acceptance test should be performed after the successful completion of the burn-in period. Any components that are replaced also should be subject to a burn-in period.

12.5.3 Acceptance Testing

12.5.3.1 Overview

All points, (e.g., access control points, intrusion detection points, video cameras, intercom systems) require testing and observation to ensure that they operate as required in the construction documents.

12.5.3.2 Requirements

Acceptance testing is to be complete and test documentation approved by the client prior to the project completion.

In order to account for all lighting conditions, video cameras must be examined during the day and at night.

12.5.3.3 Recommendations

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 may also include a "defeat the system" test to demonstrate that there are no potential shortcomings within the hardware and software system that would compromise the integrity of the system under normal operating conditions.

12.5.4 Retesting Equipment and Systems

The commissioning technician will need to correct any deficiencies identified by the client. Upon completion of all corrections, the equipment shall be retested to demonstrate proper operation, integration, and performance. The security contractor should provide all the labor and materials required for any necessary retesting. Verification of proper system operation and performance should be completed during the preliminary testing stage to avoid retesting. The construction documents should identify that the security contractor is responsible for the client's costs to supervise and observe any retesting of failed system components.

12.5.5 Warranty Periods

Installation companies should be aware that equipment warranty periods are an opportunity to make required adjustments to systems and components. Additionally, operation and maintenance manuals, as well as the as-built drawings, should be updated to reflect any modifications made during the warranty period.

A final warranty walk-through should be undertaken in the last quarter of the warranty period to correct any deficiencies and make required adjustments to the system.

12.6 Additional Commissioning Tasks

The ESS hardware and software installation must be inspected both visually and electrically. The items most commonly subject to verification during commissioning ensure that:

- The system has been installed in accordance with the specifications and drawings and follows the manufacturer's recommendations.
- Record drawings are completed and provided to the architect and engineer for use during testing.
- All test reports are given to the architect and engineer for review.
- Headend equipment and intermediate ESS equipment are installed as indicated in the project documents. If this was a direct sell to the end user without documentation, at a minimum, lockable cabinets should be installed within communications equipment rooms (ERs). They must be kept separate from the other devices housed in the ER.
- All cabinets are clean inside.
- System software licenses have been provided for the specified number of equipment and personnel.
- ESS equipment matrix has been developed, and all information has been properly programmed.
- Directories for each panel, listing the card reader interface slot locations, names, and utilized channels, are provided.
- All low-voltage security cables are installed in conduit, boxes, and locked enclosures when required and meet all applicable codes.
- All enclosures, panels, and field equipment are properly labeled.
- All cable and termination points are properly labeled. Tag numbers on record drawings also should be provided.
- All hardware is properly installed and meets the manufacturer requirements for installation.
- All power supplies are hardwired. Plugs should not be used unless indicated in the drawings or specifications.

Additional tasks related to system verification include:

- Checking all electrical circuits of the various devices for proper wiring polarity, grounding (earthing), and activation. An ESS designer should ensure that proper battery backup is installed to provide operation for a specified period of time during power outages. Test the system with a simulated power failure to verify operation of power backup and establish that all fail-safe criteria are being met.
- Verifying that each access point meets all of the programmed requirements for that location, that the system logs the event, that the door is unlocked, or that the unlocking is disapproved and alarm is reported. This verification is performed using the access control matrix and cards from each access class. The same procedure should be performed with the keypads using both valid and duress codes.
- Simulating alarm conditions and verifying that all doors function properly. An ESS designer should verify that all door open/closed status conditions are properly represented in the system.

List continues on next page

- Verifying that surveillance cameras are properly positioned to capture the required event video information. An ESS designer should ensure that the recordings are time and date coded and saved in a digital video recorder with sufficient data storage capability, in a secure location, and connected to a backup power supply.
- Verifying that all of the electrical (e.g., door locks, request to exit) and mechanical hardware (e.g., crash hardware) at all of the access points function in accordance with the manufacturers' specifications. An ESS designer should verify that low-voltage cables are not exposed and that all equipment is installed in lockable cabinets. All card readers and keypads should be tamper proofed.
- Systems (e.g., IDS) might perform differently under various weather conditions; therefore, they should be tested to the fullest extent possible under all conditions.

A "defeat the system" test may be required by a client to verify system hardware and software integrity prior to acceptance of the system.

If any failures in the electrical or mechanical operation of the ESS system are noted, a retest must be scheduled. A corrective action plan must be established, and a retest should be performed with passing results and added to the documented file.

During the system's operation, all event logs should be regularly analyzed, and repeat events should be decreased or eliminated. The security system performance should be retested periodically to ensure that all functions comply with the original specifications.

12.7 Training

Typically, the system training is the responsibility of the system's integrator or installation contractor. The goal of the following information is to provide a holistic view of an ESS project and explain how an ESS design may affect the system's operation.

For more information on training, see Appendix E.

This page intentionally left blank

Appendix A Cabling Pathways (Normative)

This appendix is normative and is considered part of this standard.

A.1 Overview

This section describes the telecommunications cabling pathways and related telecommunications spaces necessary to support ESS systems. ESS is one of several subsets of systems covered by the term "telecommunications". While the scope of this standard is limited to the telecommunications cabling, pathways, and spaces associated with ESS systems, this standard significantly influences the design of other building services, such as electrical power. This standard also provides minimum requirements for the size of telecommunications spaces in support of ESS systems. When designing and installing cabling pathways, it is important to ensure that the route is verified to drawings and specifications prior to actually installing the cabling pathway support structures.

Cabling pathway system design and implementation involves the cabling pathway (e.g., cable tray, conduits, ducts, open spaces using non-continuous supports [J-hooks]) and the locations of related telecommunications spaces (e.g., an ER that provides access to cable and connecting hardware, ESS equipment and their interconnection or cross-connection to ESS cabling systems). Cabling pathway components are expected to accommodate all standards-compliant cabling and the potential need for change during the life cycle of the cabling system and building.

This standard offers a number of pathway design alternatives for ESS pathways and spaces. Qualified ESS systems designers are responsible to select the appropriate ESS pathway infrastructure system design based upon the ESS applications to be supported.

The backbone cabling pathways are those portions of the telecommunications cabling pathway system that permits the placement of backbone cabling between the building entrance location and all additional telecommunications spaces within the building (e.g., equipment room, telecommunications room, telecommunications enclosure). The horizontal cabling pathways are the portions of the telecommunications cabling pathway system that permits the placement of horizontal cabling between the horizontal cross-connect (floor distributor) typically located in the TR and potentially passing through the optional HCPs and terminating at equipment outlets located in a coverage area.

Designers and installers are expected to ensure that the cabling pathways and spaces:

- Allow for the accommodation of change over the facility's life cycle with the goal of reducing long-term maintenance and operational costs.
- Consist of standards-based methodologies and components.
- Meet or exceed applicable codes, standards, regulations, and complies with AHJ rulings.

Cabling pathways may include:

- Continuous cabling pathways (e.g., conduit, cable tray, surface raceway) used for containment of telecommunications cabling.
- Non-continuous cabling pathways (e.g., J-hooks) through which cabling is placed between physical support or containment components.

A.2 Types of Cabling Pathways

A.2.1 Introduction

There are many types of cabling pathways. While this standard is not intended to define a list of approved cabling pathway types, this standard does address the use of cabling pathways specifically for the purpose of distribution of ESS cabling. These cabling pathways may be used exclusively throughout a project or in combination with any number of additional cabling pathways. The following is a list of cabling pathways, which includes:

- Cable tray (e.g., solid bottom, ladder, mesh, center spine, etc)
- Non-continuous pathways (e.g., J-hooks)
- Conduit (e.g., metallic, non-metallic)
- Surface raceway (e.g., metallic, non-metallic)
- Duct (e.g., wall duct, floor duct, trench duct, cellular floor)
- Access floor (also referred to as raised floor, computer room floor)
- In-floor systems such as floor boxes, poke throughs (e.g., concealed access, flush access, surface access)
- Catenary (e.g., cable suspended from its end points used to attach cabling)

This appendix does not restrict nor endorse any particular type of metallic or non-metallic cabling pathway products or systems. For any questions related to specific cabling pathway types or applications that may not be approved for use, consult with the AHJ.

A.2.1.1 Requirements

Except where otherwise specified, all cabling pathways shall adhere to the specifications of relevant cabling and containment standards (e.g., TIA-569-D, CENELEC EN 50174-2, ISO/IEC 14763-2).

All of the following general cabling pathway requirements shall be met:

- ESS pathway types, sizes, and configurations shall accommodate the initial installation of ESS cabling and related bend radius requirements, with an allowance for 100% growth.
- ESS pathways shall not be located in elevator shafts or other locations that may require specialized tradespersons to permit access to the ESS pathways.
- ESS pathway specifications shall accommodate the applicable seismic zone requirements in accordance with the AHJ.
- Where premises cabling is intended to be used, building ESS pathways shall be installed in “dry” locations.
- Where outside plant (e.g., campus) or indoor/outdoor cabling is intended to be used, building ESS pathways shall be suitable for use in the type of environment (e.g., damp, dry, wet) in which they are installed. See applicable codes, standards or regulations (e.g., NFPA 70 Article 100) for definitions of damp, dry and wet locations.
- Firestop assemblies, where required, shall be maintained when penetrated by cables, wires, and ESS pathways. See the specifications of relevant cabling pathways and containment standards (e.g., TIA-569-D, CENELEC EN 50174-2, ISO/IEC 14763-2) for additional guidance.

Regardless of the type of cabling pathway(s) that are selected for a given project, the telecommunications cabling bend radius and pulling tension requirements shall be met. See Table A-1 below for balanced twisted-pair cabling bend radius and pulling tension requirements. See Table A-2 below for optical fiber cabling bend radius and pulling tension requirements.

Cable manufacturers bend radius and pulling tension requirements may vary from Table A-1 and Table A-2. Where bend radius and tension requirements vary, values used should be the most conservative (i.e., largest applicable bend radius, smallest tensile load).

The maximum depth of telecommunications cabling (e.g., balanced twisted-pair, optical fiber) installed in cabling pathways shall not exceed 150 mm (6 in) for a solid bottomed cable tray pathway regardless of the depth of the cable tray pathway.

For cabling pathway systems that are not solid bottomed, the maximum depth of installed cabling shall be determined by the spot loading and pressure it exerts on the support points of the pathway system. See Table A-3 for maximum allowable cabling stacking height in cabling pathways.

Table A-1 Balanced Twisted-Pair Cabling Bend Radius and Pulling Tension Requirements

Cabling/Cord Types	*Required Minimum Inside Bend Radius Under No Load (No Stress)*	*Required Minimum Inside Bend Radius Under Load (Stress)*	*Recommended Maximum Tensile Load Under Load (Stress)*
4-pair, balanced twisted-pair patch/equipment cord	One times the cord cable outside diameter	One times the cord cable outside diameter	Follow manufacturer specifications
4-pair, balanced twisted-pair cables	Four times the cable’s outside diameter	See Note 1	110 N (25 lbf)
Multipair balanced twisted-pair cables	Follow manufacturer specifications	Follow manufacturer specifications	Follow manufacturer specifications

Note 1: Consult the applicable cabling standard(s) applicable at the site, as well as manufacturer’s recommendations for the specific cable.

Table A-2 Optical Fiber Cabling Bend Radius and Pulling Tension Requirements

Cable Type and Installation Details	*Maximum Tensile Load During Installation*	*Minimum Bend Radius While Subjected to Maximum Tensile Load (During Installation)*	*Minimum Bend Radius While Subjected to No Tensile Load (After Installation)*
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 directly buried, trenched or blown into ducts	440 N (100 lbf)	20 times the cable outside diameter	10 times the cable outside diameter

Table A-3 Maximum Allowable Cabling Stacking Height in Cabling Pathways

L *Distance between points of support*	*H* *Maximum stacking height in cable pathways*
0 mm (0 in)	150 mm (6.0 in)
100 mm (4 in)	140 mm (5.5 in)
150 mm (6 in)	135 mm (5.4 in)
250 mm (10 in)	130 mm (5.0 in)
500 mm (20 in)	110 mm (4.4 in)
750 mm (30 in)	100 mm (4 in)
1000 mm (40 in)	90 mm (3.5 in)
1500 mm (60 in)	75 mm (3 in)

Where:

L = Distance between points of support rounded to the nearest 50 mm (2 in)
H = 150 mm / (1 + L × 0.0007 mm), H = maximum stacking height (in mm) rounded to the nearest 5 mm, or
H = 6 in / (1 + L × .00003 in), H = maximum stacking height (in in) rounded to the nearest 0.1 in

A.2.2 Cable Tray Pathways

A.2.2.1 Introduction

Cable trays are generally described as structures with pre-fabricated components for supporting and routing cables or conductors that are pulled or laid in place after the pathway has been installed as a complete system.

There are many types of cable tray pathways, typically constructed of steel or aluminum. There are a variety of methods available to securely attach cable trays to the building structure. While this appendix is not intended to define a list of approved cable tray pathway types, this appendix does address the use of cable tray pathways specifically for the purpose of distribution of ESS cabling. These cable tray pathways may be used exclusively throughout a project or in combination with any number of additional cabling pathways. Following is a list of cable tray pathway types:

- Solid bottom cable tray provided with or without a cover of various dimensions
- Ladder style cable tray of various types and dimensions (e.g., bar stock, tubular)
- Mesh style cable tray of various types and dimensions
- Center spine cable tray with singular rail design or multiple rail design of various dimensions
- Additional types or styles of tray not described in this appendix

A.2.2.2 Requirements

When cable tray is installed and attached to any building structure, it shall be supported at intervals specified by the manufacturer. These support intervals may depend on the load the cable tray is designed and manufactured to support.

Cable trays of all types shall be bonded per the AHJ requirements whether the cable tray is used for electrical power wiring, telecommunications cabling (includes ESS cabling) or both.

Cable tray fill ratio shall not exceed 50%. The maximum fill depth of any cable tray shall be 150 mm (6 in).

Cable trays installed above equipment rack and cabinet heights, shall protrude straight into the telecommunications space (e.g., ER, TR), without a bend, at a height that is in accordance with the customary practices of the location where the installation takes place. For example, it is customary in many parts of the United States to place the cable tray system at least 2.4 m (8 ft) AFF.

A.2.2.3 Recommendations

Cable tray pathways addressed here may be located below or above the ceiling or within an access floor system in either plenum or non-plenum applications.

Cable tray pathways should provide fixed or movable dividers to separate ESS cabling from electrical cabling. Movable dividers are more advantageous than fixed dividers because they can dynamically accommodate change over the lifecycle of the building.

A.2.3 Non-continuous Pathways

A.2.3.1 Introduction

Non-continuous pathways (e.g., J-hooks) provide a base that is wide enough to distribute the cable bundles weight to prevent damage. They may be constructed of metal, plastic, or fabrics and have various configurations for use in different environments. Sizes are available to support a variety of cable bundle sizes.

A.2.3.2 Requirements

Non-continuous pathway devices shall not be spaced more than 1.5 m (5 ft) apart, on centers.

These non-continuous pathway devices shall not be attached to the ceiling grid support system or any other support system that is not exclusively provided for the purpose of fastening the non-continuous pathway devices.

Non-continuous pathway devices shall be securely attached to the building structure or to support structures directly attached to building structure. Specifications concerning the weight carrying capacity of the attachment device and the support system may be subject to plan review by the AHJ. Designers and installers shall be prepared to demonstrate compliance with applicable codes and regulations to satisfy the AHJ that the system is capable of supporting the calculated weight at the maximum fill of the system.

Inaccessible ceiling areas, such as lock-in type ceiling tiles, drywall or plaster ceilings, shall not be used as distribution pathways. Ceiling tiles shall be of the removable or lay-in type. In the event that the ESS pathway transverses inaccessible areas, a permanent pathway shall be installed as a part of the building construction that is sized to accommodate the maximum possible number of telecommunications cables anticipated to pass through such space.

Cabling shall not be laid directly on the ceiling tile or ceiling rails or in any support structure or support system that is not specifically and exclusively designed for the purpose of supporting telecommunications cabling.

A clear vertical space of at least 75 mm (3 in) shall be provided between the non-continuous pathway devices and the ceiling tiles and ceiling grids.

A.2.3.3 Recommendations

Areas above ceilings may be used as ESS pathways for telecommunications cables as well as spaces for connecting hardware where allowed by the AHJ.

Non-continuous pathways (J-hooks) should be installed on a spacing of 1 m (3 ft) to 1.5 m (5 ft) centers, additional supports may be required. Non-continuous pathways (J-hooks) should be capable of providing the following features:

- Individual color-coding to distinguish between types of services supported (e.g., ESS cameras, ESS access control, fire-life-safety wiring).
- Capability of stacking in series and mounting in back-to-back configurations in various environments (e.g., threaded rod, I-beam, side of wire basket tray, wall, ceiling, floor).
- Option for a wire/cable retention device to help contain wires/cables within the device.
- Rounded edges to help avoid damage to wires/cables placed or pulled through device.

A.2.4 Conduit Pathways

A.2.4.1 Introduction

A conduit system may be used for horizontal or backbone cabling distribution. In horizontal cabling distribution, these conduit systems consist of conduits installed from the applicable telecommunications space (e.g., ER, TR) to the telecommunications outlets or coverage area outlets in the floors, ceilings, walls, columns, or furniture in a building. In backbone cabling distribution, these conduit systems consist of conduits installed from one applicable telecommunications space (e.g., ER, TR) to another applicable telecommunications space (e.g., entrance facility, TE). Codes, standards and regulations recognize for use, many types of metallic and non-metallic conduit. Consult local AHJ and related guidelines for compliance with applicable codes, standards and regulations.

Conduit systems are comprised of sections of ducting (typically circular in shape) with varied accessory items. One such conduit accessory item is a conduit body. A conduit body is a fitting available in several styles and configurations. Two common styles of conduit bodies are the 'C', or straight inline fitting, and the 'LB', or 90-degree bend with removable cover. Conduit bodies may provide a convenient and compact change in direction for electrical wiring. However, they should not be used to change direction for telecommunications cables as they are likely to compromise minimum bend radius requirements.

A.2.4.2 Requirements

Conduit as a horizontal cabling pathway system for ESS cabling shall be specified and provided when:

- It is required by applicable code as enforced by the AHJ.
- Special mechanical protection is required and not satisfied by other pathway types.

The maximum length of non-flexible conduit between pull points shall not exceed 30 m (100 ft).

A maximum of two 90-degree bends shall be placed in any conduit segment between pull points. A third bend shall be acceptable in a conduit segment if one of the following is present:

- The conduit segment does not exceed 10 m (33 ft).
- The conduit fill ratio is derated by 15% for the third bend.
- One of the bends is located within 300 mm (12 in) of the cable feed end. (This exception only applies to placing operations where cable is pushed around the first bend).

Conduits shall be installed in such a manner as to remove sharp edges and have insulated bushings installed where applicable (e.g., metallic conduit).

Conduits shall be installed with synthetic, mildew resistant pull string or pull rope that has a tensile rating of no less than 320 N (72 lbf). A swivel pulling eye shall be connected to the pull string or pull rope which is attached to the cable to prevent twisting forces on the cable. The pulling tension shall not exceed the cable manufacturer's requirements.

Although it is not recommended to be used, if flexible metal conduit is used, the maximum length of any segment shall not exceed 6 m (20 ft). The flexible metal conduit diameter shall be increased by one trade size relative to the size of the corresponding non-flexible metal conduit if it is selected in place of a non-flexible conduit pathway. The trade size of the flexible metal conduit shall be based on applicable fill percentages according to the AHJ. This flexible metal conduit de-rating is intended to accommodate potential cable abrasion caused by the movement of the flexible metal conduit during installation.

If an armored cable assembly is provided prewired inside of the flexible metal conduit, the 6 m (20 ft) rule need not be applied in such cases. The reason for this is that integrated cable/pathway designs eliminate or sufficiently diminish the wire/cable abrasion attributes of a flexible metal conduit.

Conduits protruding through the floor in the telecommunications space shall be terminated at a height above the floor surface that is sufficient to protect cabling and firestop materials from liquid spills.

A.2.4.3 Recommendations

In-floor conduit systems are especially inflexible when installed in concrete. In-floor conduit systems should be considered only when all other means are unacceptable.

Polyvinyl chloride (PVC) conduit should not be used inside commercial buildings unless placed in a cavity that is to be filled with concrete. Refer to the AHJ for permitted conduit materials.

Flexible metal conduit (e.g., metal flex conduit) is not recommended for use with telecommunications cabling. Flexible conduit should only be used in situations where it is the only alternative, as it is prone to creep or shift during cable installation and increases the likelihood of cable sheath damage.

Factory-manufactured metallic conduit bends instead of field-manufactured metallic conduit bends are recommended when conduit installation applies. There are two disadvantages of field-manufactured metallic conduit bends:

- Specialized equipment is used to accomplish the required angle of bend.
- Field-manufactured bends typically result in an elliptically shaped cross-section, rather than being completely round like factory-manufactured metallic conduit bends.

In the event a field-manufactured metallic conduit bend becomes elliptical, it should be replaced or de-rated to the next smaller trade size conduit for cable fill calculation purposes.

If conduit bodies are used, a telecommunications style conduit body with a smooth internal bend radius for preventing cable damage should be used in place of the electrical style conduit bodies.

Cable pulling tensions may be reduced by using lubricants. Care should be practiced in lubricant selection, taking into consideration compatibility with cable jacket composition, safety, lubricity, adherence, stability, and drying speed.

A.2.5 Surface-mounted Pathways (Perimeter Raceways)

A.2.5.1 Introduction

Perimeter raceways are surface-mounted pathways, often installed at baseboard, chair-rail, or ceiling height, that may contain power and equipment outlets. Surface raceway systems may be used as a distribution system within and between rooms and may extend from building pathways to furniture pathways to connect furniture partitions or furniture systems. Surface mounted raceway passing between rooms or penetrating walls are expected to conform to the requirements of the AHJ in terms of fire and acoustical ratings.

This type of raceway is available in metallic and non-metallic materials and in many sizes and configurations. This raceway is typically available in two sections - a base and a cover. The base is installed on the floor, wall, or ceiling surface using fasteners. The cabling is installed and then the cover is installed over the top of the cabling. Typically, the cover is held in place by snapping it over the base. Some surface raceways include bend radius control to ensure compliance with minimum bend radius requirements of telecommunications cabling.

Secure raceway systems are also available. There are generally two types of secure raceway systems:

- Physically secure
  - Covers slide onto the base(s) at access points consisting of lockable surface boxes; the covers cannot be removed without access to the boxes.
  - Covers may be secured to the base with fasteners employing a “safety screw” type head requiring special tooling to tighten or remove.
- Electronically secure
  - Tamper detection software and hardware are used to identify a potential security breech.

A.2.5.2 Requirements

When outlets of any type are provided as part of a perimeter raceway system, the outlet height shall comply with the requirements of the applicable codes, standards, and regulations (e.g., ADA).

Electrical style surface raceway corners (e.g., inside corners, outside corners) shall not be used with telecommunications cabling (e.g., balanced twisted-pair, optical fiber) due to potential cable bend radius violations that may be caused by the use of electrical style surface raceway corners.

Telecommunications style surface raceway corners (e.g., inside corners, outside corners) shall be used with telecommunications cabling (e.g., balanced twisted-pair, optical fiber). Such systems provide smooth rounded corners to accommodate the bend radius requirements of such telecommunications cabling.

Surface raceway systems consist of bases, covers, associated fittings, and accessories. Fittings (e.g., coupler, corner, end cap, adapter, device box) shall be used to connect, change direction, or terminate a surface raceway. Accessories shall provide the means of mounting specific or generic devices (e.g., service area outlet, conduit connection) either internal or external to the raceway system.

Surface raceway systems shall be configured as either single-channel or multi-channel systems. Single-channel systems shall be designed and used for either telecommunications cabling or power cabling. Multi-channel systems shall contain divider wall(s), either pre-configured or modular.

For planning perimeter pathways, the maximum pathway fill shall be 40%. Pathway (raceway) fill is calculated by dividing the summation of the cross-sectional area of all cables by the most restrictive cross-sectional area of the raceway system (typically located at 90 degree corner sections). This fill capacity does not consider the additional constrictions caused by service area outlets.

Single lengths of metallic surface mounted raceway sections shall be bonded and grounded in accordance with applicable codes, standards and regulations (e.g., NFPA 70) as well any additional requirements of the local AHJ. In addition, adjacent sections shall be contiguously bonded to one another as a function of product design or with external bonding conductors.

A.2.6 Duct Raceway Pathways

A.2.6.1 Overview

Duct raceway pathways may include wall duct, underfloor duct, trench duct, cellular floor and other types of duct raceway pathways not listed here.

Wall duct is a flush, in-wall raceway system designed to support electrical and communications cabling infrastructure. Its primary advantage over conduit is its cabling lay-in features. Wall duct offers continuous covers so cables can be installed, and later accessed and changed, by simply removing the covers.

Underfloor duct systems include a network of metal raceways embedded in concrete, which facilitates the distribution of horizontal cabling (e.g., between TRs or TEs and work areas).Trench duct is a flush, in-floor raceway system designed to support electrical and communications cabling infrastructure. It is commonly used as a feeder for the cells of a cellular steel floor system, a feeder for the distribution ducts of an underfloor duct system and a flush self-contained raceway system for computer room areas, laboratories, and medical imaging facilities.

Cellular floor systems are generally utilized for in-floor raceway design in elevated steel framed construction. The cellular floor structural members support the concrete floor slab, with the cells becoming the distribution raceways. Cellular floor systems are typically fed from the floor serving TR by trench headers, which have removable steel cover plates at the top of slab elevation. Preset inserts and afterset inserts are the two methods used for work area activation. Cellular floor systems may also be used for slab-on-grade applications to maintain the large feed and distribution areas typical of elevated floor design.

A.2.7 Access Floor Raceway Pathways

A.2.7.1 Introduction

Access floor systems consist of modular floor panels supported by pedestals, an assembly of pedestals and stringers, or an integral pedestal and floor panel. Access floor systems are typically used in telecommunications spaces such as the computer room area within a data center. Access floor pathways may include systems referred to as raised floors or computer room floors and other types of access floor pathways not listed here.

A.2.7.2 Requirements

Minimum clearance between the top of the cabling pathway system and the bottom of the access floor tile in cabling pathways under an access floor shall be 75 mm (3 in).

When used in a telecommunications space (e.g., ER, TR), the minimum finished floor height shall not be less than 150 mm (6 in) above the slab.

A.2.7.3 Recommendations

The minimum finished height of access flooring is a variable that may depend on the selected access flooring manufacturers' range of products, the use of the access floor system and the access floor system location.

When access flooring is used in:

- General office areas, the finished floor should be 200 mm (8 in) high or higher. This height is necessary to provide sufficient space for cable trays and other means of cable management.
- A computer or control room environment where the plenum is used for heating, ventilating, and air conditioning (HVAC), the finished floor height should be 300 mm (12 in) or greater.

Regardless of the height of the finished floor, a minimum of 50 mm (2 in) of free space should exist between the top of the cable tray side rails and the underside of the stringers. If cable trays with covers or raceways are used, the free space above the tray should allow for easy removal of covers.

For cable management, the following methods of containment for main runs should be considered:

- Dedicated routes
- Enclosed raceway distribution
- Zone distribution
- Cable trays
- Cable matting

NOTE: Applicable codes, standards, regulations, and AHJs should be consulted for compliance with flame spread and smoke index properties of cables used in cabling pathway systems.

Connecting hardware or telecommunications equipment should not be placed in the access floor space. The only allowable exception is for connecting hardware as part of a consolidation point or HCP.

The space under an access floor may be used as an air-handling plenum for distributing conditioned air throughout the room or, in some cases, the entire office area. Compliance with AHJ should be anticipated.

If the space under an access floor is not used as an air-handling plenum, most codes allow certain types of telecommunications cables to be used without special enclosure requirements. This is also true for an above-ceiling interstitial space that is not used for air handling.

Proper placement of cable trays and telecommunications cabling in the space under an access floor is essential to ensure that adequate airflow is maintained. The underfloor air space should not be blocked by cable bundles thereby causing air dams.

In office areas, code requirements may be different for telecommunications spaces (e.g., ERs or TRs) where special fire suppression systems may be installed.

Whenever possible, the floor plan should be designed so that the telecommunications space (e.g., ER or TR) is adjacent to the access floor area that it will serve. Threaded sleeves or conduit or equivalent should connect the telecommunications space to the access floor area.

If the telecommunications space and the access floor area it serves are not adjacent, other connection methods should be considered. The interconnecting pathways should adequately serve the access floor area.

The manufacturer's guidelines should be consulted to ensure compatibility between access floor components and service fittings. Firestop integrity should be maintained in all rated building structures that are penetrated by cabling or pathways.

All metal parts of an access floor should be bonded to ground. For bonding and grounding, follow the access floor manufacturer's guidelines and all applicable building and electrical codes and standards.

A.2.8 In-floor System Pathways

A.2.8.1 Introduction

In-floor system pathways may include product categories referred to as floor boxes or poke throughs offering concealed access, flush access or surface access. In-floor systems pathways may also include systems not listed here.

A.2.8.2 Requirements

For planning in-floor system pathways, the maximum pathway fill shall be 40%.

A.2.8.3 Recommendations

The manufacturer's guidelines should be consulted to ensure compatibility between in-floor system components and service fittings. Firestop integrity should be maintained in all rated building structures that are penetrated by cabling or pathways.

A.2.9 Catenary Pathways

A.2.9.1 Overview

Catenary pathways are generally defined as metallic or non-metallic cables suspended from its end points used for the purpose of attaching cabling.

A.2.10 Utility Columns (Power Poles)

A.2.10.1 Overview

Utility columns provide pathways for wires and cables extending from the ceiling to the service area.

A.2.10.2 Requirements

When utility columns are used, the main ceiling rails shall be rigidly installed and braced to overcome movement, both vertical and horizontal.

A.2.10.3 Recommendations

Utility columns should be attached to and supported by main ceiling support channels. They should not be attached to the transverse or short length channels unless they are also rigidly secured to the main support channel.

A.3 General Installation Practices

A.3.1 Requirements

The following requirements offer cautionary guidance for the design and installation of cabling infrastructure associated with ESS pathways.

- All cabling pathways shall be securely supported.
- Consider seismic requirements when designing support systems.
- Cable ties shall not be used to support cables.
- Installer shall fill penetrations of non-fire rated assemblies with noncombustible materials.
- Exposed raceways shall be installed parallel or perpendicular to building structure (e.g., walls, ceilings).
- Sleeves shall be installed when penetrating walls where future upgrades are anticipated.
- Installer shall restore walls, floors, and ceilings to fire, smoke and acoustical rating prior to penetration using approved materials and methods.
- Installation of ESS device boxes, enclosures and pull boxes shall be coordinated with other trades (e.g., electrical, mechanical) including drywall.

A.3.2 Recommendations

The following recommendations offer cautionary guidance for the design and installation of cabling infrastructure associated with ESS pathways:

- Use as few bends as possible between pulling points,
- Clean raceway prior to pulling conductors, if contaminated,
- When using fasteners, consider the weight of material, weather conditions, vibration and operation forces,
- Select tamper proof hardware (e.g., bolts, screws, etc) where applicable, and
- Designers and installers should be aware of the locally applicable installation practices for the chosen pathway in accordance with the AHJ. The BICSI *Information Technology Systems Installation Methods Manual* may be used to acquire guidance.

This page intentionally left blank

Appendix B Electronic Safety and Security (ESS) Design Fundamentals (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

The ability to use and integrate the various practices, methodologies, and devices constitutes the practice of safety and security design. Many elements of design are unique to the protection of life and property, and others are multidisciplinary.

The ESS designer should have a firm grasp of the fundamentals and be able to incorporate aspects of the trades brought into the ESS design by other professionals. Depending on the expertise or knowledge of the ESS designer, additional support may not be necessary. The physical and electronic safety and security should work as a comprehensive package. The ESS designer should understand how they influence each other to have a successful project.

B.2 Elements

B.2.1 Access Control

Access control is important for overall personal safety and the protection of physical and intellectual property. Access control devices can include entry point locks, integrated electronic devices controlling a single door or room, or a complex system of interconnected electronic devices controlling a zone, building, or campus. ESS designs can be affected by each individual's location and the level of security desired.

B.2.2 Intrusion Detection

Intrusion detection is often viewed as part of the access control system because most door controls for access control can alarm when the door is left open or opened without a valid card read. However, it is a stand-alone system that should be evaluated to its own standards and levels of due diligence.

These systems use everything from simple switches to complex devices that detect motion, heat, glass breaking, or other nonstandard occurrences in the area to detect the presence of persons in secure zones. Intrusion detection systems can generate simple local or paging alarms or can be integrated with other systems to provide more active responses (e.g., turning on cameras or lighting).

B.2.3 Surveillance

Video surveillance is a widely used technology within ESS systems. Video surveillance involves the use of cameras for watching or controlling assets. It is the process of image:

- Capturing
- Transmitting
- Processing
- Viewing
- Recording

This technology requires knowledge of cameras and their placement, as well as knowledge of image transmission and recording principles.

B.2.4 Fire Detection and Alarm

Fire detection and alarm involves the early detection and notification of life safety threats. Fire detection and alarm requires that the ESS designer have a thorough knowledge of specific codes, statutes, and the requirements of the applicable AHJ.

B.2.5 Integrated Systems

Integrated systems cover concepts, systems, and processes related to the convergence of ESS systems or their integration with other building systems. Through integration, ESS systems begin to interact with other building systems. Integrated ESS systems are deployed in a wide variety of environments, including:

- Facilities
- Campuses
- Vehicles
- Persons

B.2.6 Special Systems

With the convergence of systems to the network, the addition of specialty systems such as nurse call, RFID tracking, intercom, and mustering will sometimes fall under the responsibilities of the ESS designer.

B.2.7 Network Security

As more systems migrate to the network, the issues of protecting those systems should be addressed. Isolation can provide protection but at the cost of remote access. Remote access to a network allows the possibility of outside interference and harm. Firewalls, encryption, virtual private networks (VPNs), and other methods of protection are available.

B.3 Types of Projects

An ESS project may be a new construction or a retrofit for an existing facility. Types of designs facing the ESS designer may include:

- Original design
- Retrofit of an existing plan
- Upgrade or replacement of an existing system

To successfully complete a project, the ESS designer should be able to interact with building owners, tenants, architects, engineers, and security professionals. The ESS designer also may need to consult end users and other stakeholders.

B.4 Current and Future Trends in Safety and Security

Several areas in safety and security design are affected by rapid growth in technology, including:

- Information technology
- Physical security
- Integration of access control and BAS
- Surveillance

B.4.1 Information Technology

Most of the systems today have migrated to the use of the network for communications protocol between the servers and control panels. Some are hybrid systems where there are limited gateways to the network and the devices communicate through older protocols for the subsystem communication. The ESS designer should understand the system communication methods, the required infrastructure particular to the specific system installed, and how network outages will impact system functionality. The ESS designer should understand the impact of the project on the client's IT networks. The impact may be financial, operational, and physical (e.g., switch ports, bandwidth, cabling). The ESS designer also should have a reasonable understanding of network terminology, architecture, and function. Coordination with the client's IT department is important for ensuring the success of any safety or security project that has an impact on the IT network.

B.4.2 Physical Security

Physical security involves measures that deter, detect, delay, mitigate, or notify any attempt to injure, damage, modify, or remove an asset or person. This includes damage by accident, fire, environmental elements, crime, vandalism, and industrial espionage. It can be a simple device or multiple layers of electronic measures.

Strong security measures also come at a cost, and there can be no perfect security. It is up to a security designer to balance security features and a tolerable amount of personnel access against available resources as well as the risk to assets that are to be protected.

Depending on the situation, consulting with architects, engineers, and hardware designers may be necessary for physical security considerations. This reference manual will describe, in detail, situations and hardware types for general building applications being governed by conventional codes. In some special situations (e.g., military, correctional facilities, hospitals), codes commonly used for commercial buildings may not apply.

B.4.3 Integration of Access Control and Building Automation Systems

The client often will require multiple levels of access within a space, and personnel may require access to a number of different areas, rooms, or spaces. Access levels may change over time, and may impact or be impacted by other building systems. When an ACS is integrated with one or more BASs, the design goals require a more holistic approach.

Observing the client's space and surrounding areas has always been a major aspect of access control as part of the security system. Understanding how the electronic access control system integrates with the BAS and subsystems in the surrounding areas is becoming a major factor in the design of electronic access control system s.

B.4.4 Surveillance

Surveillance systems record activities in the client's targeted areas for local or remote review.

Modern camera systems may be:

- Digital
- Analog
- Digital/analog hybrids
- IP cameras

Many factors will affect the selection, including:

- Court admissibility
- Network impact
- Available space within buildings to house equipment

B.5 Electronic Safety and Security System Development Basics

Safety and security system design is developed in a layered approach. The personnel involved change in each layer and the guidelines and standards also change in each layer. There are physical and electronic safety and security measures to consider when developing the complete system design.

The electronic safety and security system may consist of several different and independent systems providing an integrated package residing on the same infrastructure as other systems. This allows for increased functionality and reduced costs. While almost all systems connect to a TCP/IP network at some point, many of them have system components that have their own wiring and infrastructure standards. These should be identified and developed independently.

The ESS infrastructure should be evaluated for the type of cabling, bandwidth requirements, redundancy, reliability, and other relevant needs. For example, video surveillance systems have bandwidth requirements at the camera, video streamer, server(s), and viewing station(s). Different system address video compression, video format, fail over requirements, and viewing in different manners and yet all of these systems use the same ESS infrastructure. Design and implementation of the ESS system infrastructure can greatly impact the functionality of the ESS system and any other system that shares that infrastructure.

This page intentionally left blank

Appendix C Wireless Transmission (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

Wireless transmission can aid in meeting the needs for rapid deployment of ESS systems and devices, such as intrusion detection systems and surveillance cameras. These technologies can be limited to line of sight applications, requiring careful site surveys to determine potential signal obstructions.

A formal risk assessment and security master program will identify the appropriate deployment of wireless technologies. Security master plans may not allow the use of wireless technologies due to the critical nature of the transmitted data.

Wireless frequencies are used for specific applications. Some examples of wireless technologies are:

- 900 MHz and orthogonal frequency division multiplexing (OFDM) technologies for outdoor multipoint
- 2.4 GHz for in-building wireless
- Above 40 GHz for short-haul, high-speed PTP communications

Three primary types of wireless technologies are used for transmitting video signals:

- Radio frequency
- Free space optics
- Microwave

C.2 Radio Frequency Transmission

C.2.1 Introduction

RF transmission typically uses low-power unlicensed radio transmitters and receivers to convey the surveillance signal and typically operates in the 2.4 GHz or 5.8 GHz band.

Unlicensed wireless network equipment has less power output than licensed equipment. The 2.4 GHz and 5.8 GHz frequency bands are used for wireless deployments for the unlicensed spectrum. Although the spectrum range below 2.4 GHz has unlicensed space available, these frequencies are used primarily by amateur radio operators, 900 MHz wireless Internet service providers, and SCADA communications. The unlicensed frequencies above 5 GHz are used primarily in short-range, high-speed, PTP communications at ranges of 1.6 km (1 mi) or less.

Among the unlicensed spectrum, 2.4 GHz and 5 GHz are the most popular for wireless PTP and point-to-multipoint data networks. The frequency 2.4 GHz is primarily an indoor standard for multipoint, and 5 GHz is primarily for outdoor PTP and high-speed multipoint. There are 5.3 GHz technologies available for both PTP and multipoint links, as well as for indoor applications.

C.3 Free Space Optics

C.3.1 Introduction

Free space optics utilize many of the same principles for transmitting video signals that an optical fiber cabling system does. However, the media is open space rather than a strand of optical glass. A light source is modulated with the surveillance images and projected through a lens to a receiver some distance away. The light source is then gathered by another lens and focused on a photosensitive cell for demodulation. The primary drawback is the failure of the link to operate in environmental extremes (e.g., heavy rain and fog).

These systems are typically utilized for disaster recovery and to provide redundancy to an existing system.

C.4 Licensed Microwave Radio Transmission

C.4.1 Overview

Licensed microwave radio transmission is a reliable means for wireless transmission of surveillance signals. The system operates on a protected frequency assigned by the government agency that required the issuance of a license and is less susceptible to interference from other RF sources.

The licensed spectrum, up to 3.5 GHz, is used primarily for multipoint applications.

They offer speeds up to 10 Mb/s per subscriber and are not commonly used in private telecommunications applications. PTP licensed wireless networks are found in the 6 GHz to 40 GHz ranges and can offer speeds of 10 Mb/s to 1 Gb/s. The 6 GHz and 11 GHz frequencies are used primarily for public safety applications. The 18 GHz and above frequencies are used primarily in the private sector for PTP applications.

C.5 Frequency Selection

C.5.1 Introduction

Determination of specific frequency utilization depends on many variables. In multipoint licensed applications, the choice of frequency is less important, as set frequencies are available for carrier grade systems and applications. Selection of a particular frequency is more of an issue with outdoor point-to-multipoint and PTP wireless design. Only after identifying the following items can the exact frequency be chosen:

- Overall environment
- Existing RF
- Bandwidth considerations
- Distance or coverage area

Licensed systems are a good choice when the proposed system requires a high rate of reliability (e.g., video surveillance). Licensed frequencies assure that the system will be clear of and protected from interference. Unlicensed frequencies are a good choice when budgets do not allow for licensed technology, antenna size is an issue, or licensed frequencies are not available for a given area. The carrier grade multipoint frequencies are used in most areas worldwide but are available to buy from other carriers holding the licenses. The PTP licensed frequencies are available and are classified by the government agencies for use in many areas. It is important to understand the license process and government agencies' rules regarding these frequencies before designing a system.

When dealing with licensed frequencies, certain parameters apply, including:

- Transmitter power
- Minimum antenna size
- Coverage area

These factors play into the overall design possibilities. Government agencies have rules for certain areas of the country that may further limit the minimum antenna size, beam width, and output power. There also are protected zones in the country where further restrictions apply for the use of certain frequencies. Unlicensed frequencies can have drawbacks. They are not protected from interference and have less output radio power than licensed frequencies. In many cases, they are less secure because the equipment is widely available and less expensive. Careful consideration should be given when selecting unlicensed frequencies. Proper selection of equipment and technology coupled with the configuration of the frequency channel and proper application of the systems security features can make unlicensed wireless technology as secure as a licensed system.

Appendix D Cloud Computing (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 Overview

The term cloud computing is used to describe all types of Internet-based resources and services, including storage. While the concept of cloud computing originated in the 1950s, it was not until the early 2000s when high-capacity networks, low-cost computers and storage devices, and the growth of the Internet provided the catalyst for the widespread adoption of hardware virtualization and service-oriented architecture.

The main enabling technology for cloud computing is server virtualization. Server virtualization is the process of running multiple operating systems (OS) simultaneously in a single server. Virtualization software is used to share the physical resources of the server among the virtual environments. Instead of operating several servers at a light load, their OS can be installed virtually in a single server (referred to as server consolidation). As long as the consolidated server has adequate physical resources (e.g., processing capacity, memory), the migration from physical to virtual is transparent to users.

Cloud computing provides flexibility in how certain functions of an ESS system may be provided by removing the need for specific site infrastructure, equipment, and support.

D.2 Services

Within cloud computing, a specific function is generally called a service. The type of service may vary, and some may not have an easily recognizable connection to cloud computing. However, a generally accepted nomenclature has evolved to impart some clarity where services provided by the cloud function are expressed as *X as a service* (*XaaS*). While *X* may represent anything, *X* also may be replaced by the first letter or combination of letters of the

specific service provided, including:

- S (software).
- I (infrastructure).
- P (platform).
- DC (data center).
- SEC (security).

The most established service of cloud computing is software as a service (SaaS), which can be deployed generally across all systems or specific to a particular system.

D.2.1 Software as a Service (SaaS)

Within SaaS, cloud providers install and operate application software in the cloud, and users or equipment access this software from cloud clients. Cloud users do not manage the cloud infrastructure and platform where the application runs, which eliminates the need to install and run the application on the user's own computers and simplifies maintenance and support.

The ESS designer has a growing diversity of SaaS solutions where security and safety applications and data may be delivered through the cloud.

D.2.2 Physical Access Control as a Service

Physical access control as a service can offer transaction data of users entering or exiting a facility. It also makes available card, biometric data, and visitor management services in the case of managed access control systems (ACS). The emergence of the mobile device credential will continue to become a consideration by large card populations as a way to reduce costs.

The following are examples where door entries recorded and managed by the ACS are useful cloud-based services:

- The user has external doors that are unlocked or unsupervised and pose a risk to the facility.
- Video clips of anyone entering a door within a specific timeframe can be captured and stored off-site.
- Other problem areas can be monitored easily without the major investment required by digital video recorders (DVRs).

D.2.3 Video Surveillance as a Service (VSaaS)

Video surveillance as a service (VSaaS) delivers a solution that provides observation, forensic review, and recognition functions to users through desktop or mobile platforms.

A managed VSaaS adds services that use video data verify an alarm, safety, and environmental conditions.

Areas where VSaaS may be applicable include:

- Loss prevention
  - Can be positioned as a redundant level of security to augment an existing surveillance system especially in high-value areas
- Retail, fast-food, and convenience stores
  - Snapshot of business in store and drive-thru
  - Verification of deliveries and operational hours
  - Protection of cash and assets
  - Recorded video in the camera internal storage, on local network-attached storage, and in the cloud, so there is no DVR to steal or confiscate in the event of a crime
- Data centers and areas of sensitive data storage
  - Server maintenance video audit trail
  - Record of who is accessing restricted areas
- Guard force automation
  - Remote monitoring leads to better labor distribution
  - End user can watch and spot-check security forces in action from anywhere
  - Quick deployment of video solution for temporary monitoring during events
- Property management
  - Use VSaaS to monitor a campus of multiple buildings and enable a centralized guard force, reducing costs
  - Use visitor management as a service (VMaaS) to speed up visitor and contractor entries

D.2.4 Visitor Management as a Service (VMaaS)

VMaaS is often incorporated in ACS service provider offerings and includes services specific to improving facility entry by contractors and temporary employees. VMaaS was one of the first security- and safety-related functions deployed in cloud computing.

VMaaS typically works by having visitors requesting entry to a facility accessing a web-based portal where they enter data (e.g., driver's license or identification number, vehicle license plate identification) that may be physically verified when they enter a facility. The cloud-based VMaaS application then exchanges data with the on-site physical ACS, visitor enrollment kiosk, portal, or identification enrollment center.

D.2.5 Voice over Internet Protocol as a Service

Voice over Internet protocol (IP) as a service is a relatively new offering for communications and telephony solutions with a small number of terminals (handsets). This can include door intercoms, maintenance intercoms, and intercoms that connect computer and security control rooms.

D.2.6 Mass Notification as a Service/Emergency Messaging

Nonvoice mass notification as a service or emergency messaging has been a popular cloud-based offering for higher education campuses. A user can enroll a mobile device through an application and enhanced facility; weather, emergency, and other information is pushed to the handheld mobile or other device. Non-voice emergency communications as a service also requires mobile device enrollment but makes available additional enhancements that may be used together with video surveillance for improved situation awareness.

Emergency communications systems that incorporate handheld mobile devices for personal emergency messaging and monitoring personal status may communicate to either public or private cloud environments. These systems are now able to link directly to centralized video surveillance systems (VSS) to pull up and activate cameras and video feeds closest to the personal or other emergency. Pictures sent to this service from a mobile device may be an invaluable tool, often used with VSS. Security and law enforcement professionals can have more opportunities to place persons of interest at a crime scene or event.

D.2.7 Physical Security Information Management

Physical security information management in the cloud and central station automation in the cloud are related services and invaluable tools for the ESS designer. These systems offer an aggregation point for intrusion detection, digital media content, ACS, and environmental and safety data for high situation awareness. Video verification of alarm events is an important function offered by central station automation in the cloud. It is a requirement by numerous authorities having jurisdiction (AHJs) and public safety answering points to dispatch first responders to an incident scene or event.

D.3 Infrastructure Management of Cloud Services

Infrastructure management of cloud services may range from the user performing full management on-site to the utilization of numerous service providers with minimal user involvement. There are typically three types of managed services:

- Self-managed
- Hosted
- Managed

D.3.1 Self-Managed Services

In this environment, the user has complete control of all aspects of storage and network infrastructure and maintains data on-site for higher security. In this case, the user trades cost for the flexibility to match specific hardware to each application. Since many security and safety solutions are becoming less dependent on a specific manufacturer for storage, computing, and network platforms, this selection is typically specified by the user's information technology department.

D.3.2 Hosted Services

A provider of hosted services delivers a combination of traditional IT functions (e.g., infrastructure, applications [SaaS], monitoring, storage) over the Internet or other wide area networks.

This approach enables customers to consolidate and outsource storage, computing, infrastructure, and security and safety applications to the service provider, which may lead to lower personnel costs to manage the solution and respond to demand and scheduled maintenance and unforeseen events, including the following:

- Capitalization and depreciation of the costs associated with storage, computing, infrastructure, and security and safety applications
- Recurring facility costs, including environmental monitoring, loss prevention, electricity, and heating, ventilation, and air-conditioning
- Continual and periodic assessment to determine storage, computing, and space limitations as demand grows and shrinks

Hosted services typically have higher scalability, elasticity, and agility compared with self-managing services. However, every service provider is unique, and the services offered, performance, and service level agreements (SLAs) vary greatly.

D.3.3 Managed Services

A managed service provider (MSP) manages and assumes responsibility for providing a defined set of services to its clients either proactively or as the MSP (not the client) determines that services are needed. Sometimes, MSPs are contracted to manage multiple staffing vendors and to measure their effectiveness in filling positions according to a customer's standards and requirements. In effect, the MSP serves as a neutral party that offers the customer a complete workforce solution while ensuring efficient operation and leveraging multiple staffing companies to obtain competitive rates.

An MSP for security designs offers a security and safety solution that minimizes staff requirements of the user that consumes the services. For example, in the case of information security, managed security services are network security services, response staff, and help desk support outsourced to a service provider. Such a provider delivers a fully outsourced solution and protects information assets while reducing or eliminating workload on internal data security staff.

As with hosted system providers, MSPs vary greatly in the services offered, performance, and SLAs.

D.3.3.1 Managed Service Example - Physical Access Control Systems

In the case of managed physical ACS, the typical services provided could include the following:

- Electronic physical ACS database management, including add, delete, or modify employee, tenant, student, or visitor data
- Monitoring of ACS controllers and readers
- Remote activation, lockdown, or release of secured openings
- ACS card management and replacement
- Storage and reports of all ACS transactions for incident review, monitoring, and compliance audits

D.3.3.2 Managed Service Example - Video Surveillance Systems (VSS)

Managed VSaaS can be classified by the basic functions provided by the video management systems: observation, forensic review, and recognition. In all cases, personnel other than the user's staff perform the work. Some of the services delivered with a managed VSaaS include the following:

- Continuous and event-based monitoring of specific video sources (observation function)
- Review of DMC associated with intrusion, safety, or environmental alarms (forensic review and video verification of an alarm condition)
- Monitoring of specific video sources like cameras equipped with specialized video analytics like perimeter/crossline detection or activity/motion detection (recognition function)
- Acquisition, decoding, and storage of alphanumeric information, such as license plate data, for access control or potential event review (recognition function)
- Monitoring the health, status, storage, and available resources of the network cameras and power over Ethernet devices connected to the network or Internet

D.4 Selecting an Infrastructure Management Model

When selecting an infrastructure model, items that the ESS designer needs to consider are the:

- Amount of personnel the user has and the level of involvement the user desires in managing the security and safety solution.
- Service provider's SLA for data backup, recovery services, performance, system availability, and security.
- Ability of the service provider's infrastructure to access and move information.
- Type, amount, and additional requirements of private and confidential data and the provider's capability of handling that information.
- Compliance with corporate governance and specifications, the AHJ, and any applicable codes and standards specific to the user. For example, two standards often required for retail transactions are the Statement on Standards for Attestation Engagements No. 16, *Reporting on Controls at a Service Organization*, and the Payment Card Industry Data Security Standard.
- End user's current and projected requirements for a service's ability to expand as well as meet changes in the user's needs.
- Locations where the security or safety solution will be deployed.
- Quantities of security or safety devices to be utilized.
- Availability of Internet connectivity or connectivity via private network.
- Locations and operational requirements for accessing video, security, and safety device data for remote viewing, mobile intelligence, and situation awareness.
- Amount of customization required of the service provider's solution for the user's specific needs.

D.5 Cloud Deployment Models

In addition to how services are managed, the location or deployment of services also needs to be considered. Unlike a physical deployment where equipment is located in a particular location serving a specific user, virtualization and cloud deployment may have locate services anywhere from one server specific to the user to multiple servers in multiple locations supporting multiple users.

D.5.1 Private

Private cloud is cloud infrastructure operated solely for a single organization, whether managed internally or by a third party and hosted internally or externally. This model gives companies a high level of control over the use of cloud resources while bringing in the internal and external expertise needed to establish and operate the environment. Private clouds are deployed where the requirement to provide a high level of trusted and controlled services are needed.

D.5.2 Public

A public cloud provides services over a network that is open for public use. Technically, there may be little or no difference between public and private cloud architecture. However, security considerations may be substantially different for services (e.g., applications, storage) that are made available by a service provider for a public audience and when communication is effected over a nontrusted network. Most public clouds offer access only via the Internet.

D.5.3 Community

Community cloud models share infrastructure between several organizations from a specific community with common concerns (e.g., security, compliance, jurisdiction). A community cloud may be managed internally or by a third party and hosted internally or externally. A common example of a community cloud is a government-funded education system that uses one of its campuses to function as the computing hub for the other campuses within the system.

D.5.4 Hybrid

Hybrid cloud is a composition of two or more cloud deployment models that remain distinct entities but are bound together. A hybrid cloud may allow one to extend either the capacity or the capability of a cloud service by aggregation, integration, or customization with another cloud service. An example of a hybrid cloud application is an organization may store sensitive client data in house on a private cloud application but interconnect that application to a billing application provided on a public cloud as a software service.

Hybrid clouds may offer a higher level of fault tolerance combined with locally immediate usability without dependency on Internet connectivity. However, hybrid cloud architecture typically requires both on-premises resources and off-site (remote) server-based cloud infrastructure.

D.6 Delivering Secure Services

Both physical security and IT professionals place great importance on cyber security. For example, network VSS consist of edge devices like network cameras and encoders that produce video content and metadata, control, analysis, media search and content management, storage, and display components. Physical and logical infrastructure provide connectivity between categories and also conform to industry standards. This ensures that a user or device cannot make a full network connection until they are properly authenticated.

If the IP video device is publicly accessible, the network security risks become more prevalent. Some of the risks can include compromised video integrity through manipulation of the video images or the breach of information systems to which the VSaaS is connected. Other risks include denial of service as the IP video camera will only support a finite number of users directly. There is also the risk of taking control of the device itself and redirecting the video stream elsewhere, leading to unauthorized access and possible destruction of stored video data within the camera. For this reason, many manufacturers have adopted the use of IEEE 802.1X, *Port-Based Network Access Control*, to better manage video streaming and accessibility of the recording and monitoring devices that exist on a corporate network. The ESS designer is cautioned, however, to model all systems that utilize authentication protocols to ensure the required performance level.

Current evolving capabilities that further extend the security framework of the network infrastructure components to the VSS include creating a trust model or high-assurance identity and access control framework that uses a security technique known as public key infrastructure (PKI) to implement cryptographic requirements for authenticating nonperson entities (NPEs) such as cameras or other DMC sources. Through PKI, video is encrypted during transmission over fixed and wireless networks as well as stored in mobile, network attached, or cloud-hosted storage repositories.

Authenticating NPEs in accordance with certificate and credentialing management standards is under development and will permit these devices to attain high trust levels and deliver DMC to users on public or private networks.

The validation of trusted network devices also makes bandwidth management easier and is a logical companion to network management systems.

D.7 Trends

Big data are data sets so large and complex that they are difficult to process by traditional applications. The capture, management, and analysis of data go beyond typical structured data, which can be queried by relational database management systems. Big data have come from advances in mobile devices and other sources of DMC-like network cameras. Users are collecting and keeping much more data than they did a decade ago.

Big data are characterized by volume, variety, and velocity:

- Volume is the amount of data.
- Variety refers to the wide-ranging types of data.
- Velocity refers to the speed of data processing or the required retrieval of archived information.

With big data volume varying from megabytes to exabytes, depending on the variety, the ESS

designer can furnish educated estimates of storage solution requirements.

However, data velocity is more challenging to model as security and safety professionals may have changing data retention policies and forensic investigation requirements. This alone would require the assurance of cloud computing scalability; however, even newer big data classifications have emerged:

- Validity—Are the security and safety data correlated as valid with similar sites?
- Veracity—Is the veracity of the data apparent, or are the analysis results meaningful for the security or safety function?
- Volatility—Is the data volatile, or are there rules, requirements, expiration, and repeated processing requirements?

This advanced analysis is often best provided as a service because security and safety data may unpredictably grow or shrink in size and require the scalability and agility of the cloud. Big data as a service offers users that produce large amounts of security and safety data the opportunity to make their data more meaningful to the users by using metadata and cloud-based solutions that can search effectively through this tagged data, avoiding the need to utilize on-site resources.

Appendix E System Training (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

An ESS system is a valuable part of the overall security solution. Many other systems depend on proper utilization and operation of the ESS system. Therefore, the users should know how to use the entire system properly.

Most ESS system software packages are currently designed around the different roles and job requirements of end users. For instance, some workstation software is written exclusively for the occasional operator who may have the responsibility to occasionally add a user and monitor the alarms that come into the system.

In some cases, software is written exclusively for the administrator who owns the system and is responsible for its operation and all of the integrated systems. A group of users is responsible for maintaining the system. Their work with the software is limited, but they need to be familiar with the hardware. Each group would receive the most value from training that is focused on their everyday tasks.

Manufacturers offer many choices for user training. Because each software application is unique, each training course should be customized to the user's unique needs. This customization should go beyond the content to include class location options. The classes may be held either on the installed system at the end user's location or on test or demonstration equipment at the manufacturer's location.

If the end user has 50 or more users for training, a train-the-trainer program may be more cost effective. This person would get the training, the certificate, and the handout materials from the manufacturer to conduct classes on location. An ESS designer should check with the manufacturer to learn if a train-the-trainer program is offered.

E.2 Sessions

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. Training should be required as part of the construction documents and included in the project cost.

E.3 Position or Task Training

The ESS system users may be divided by different roles or job requirements, such as:

- System administrators.
- System operators.
- Managers.
- IT staff.
- Maintenance personnel.

E.3.1 System Administrators

This training generally focuses on the personnel responsible for the system's initial setup and programming. This class teaches the system administrators how to use all the system functions.

These functions may include:

- System parameter programming.
- Operator permissions.
- Naming conventions for controllers and doors.
- Credential holder profile.
- Access level assignment.
- Identification badge design and production.
- Alarm implementation.
- Report retrieval.
- System backup.
- Database archiving.

E.3.2 System Operators

This training course generally focuses on the occasional users or the personnel responsible for day-to-day operations. This class teaches the system operator to monitor the various functions, including:

- Credential holder profile.
- Access level assignment.
- Identification badge design and production.
- Events—alarm notifications or credential transactions.
- Valid or invalid access monitoring.
- Alarm response.
- Alarm clearance.
- Reports.
- Manual door opening and closing.

E.3.3 Managers

This training course generally focuses on personnel who are overseers of the system administrators. The manager would need to know how to delete a user or change the operator or password.

This class also teaches:

- Login basics.
- System parameter programming.
- Operator permissions.
- Credential holder profile.
- Access level assignment.
- Reports.

E.3.4 Information Technology (IT) Staff

This training course generally focuses on IT department personnel who need to know how ESS systems connect to the LAN or wide area network. The bandwidth and other items, including data requirements, are discussed as well as:

- Network topologies.
- Communication to each control panel.
- Encryption strategies and capabilities.

E.3.5 Maintenance Personnel

This training course generally focuses on how the system works and covers:

- Hardware troubleshooting.
- System topology.
- Networking basics.
- Diagnostics.
- Simple programming.
- Device configurations.
- Software troubleshooting.

E.4 Training Schedules

Scheduling the training is almost as important as the training content. If the training is scheduled too far in advance, the attendees may forget the content because they would not have the opportunity to practice on the system and reinforce the knowledge gained during the class. Last-minute training also should be avoided.

The preferred point in the timeline to do system training is one to two weeks before the ESS system is commissioned and turned over to the customer. The training should be performed on a working system. The training equipment or the installed system can be used in the training.

There is an advantage to training on a live system. Many decisions pertaining to the names and descriptions of door/readers could be determined during training to ensure that they make sense to the customer. Simultaneously implemented programming and training reduces the number of hours needed for initial programming and may reduce the number of labor hours charged to the customer. This works best with smaller systems (e.g., 32 readers or less).

Too many control panels and readers may not allow a sufficient time to complete all of the programming during a training session.

If the training courses focus on role-based training, the order of the courses should be carefully considered. The administrator screens should be programmed before the operator screens to facilitate the programming flow. Cross training between the various roles is recommended.

This page intentionally left blank

Appendix F ESS Operations and Maintenance (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 Operation Best Practices

The following best practices should be addressed in system operation:

- Provide a document that describes and categorizes the systems installed and how they would impact the organization if they were to fail.
- Review in-house staff capabilities, and determine the level of support they could provide in the general operation and maintenance of the systems.
- Document installed devices, including device locations, maintenance schedule, and any operational conditions that may adversely affect or enhance the performance of the installed devices and systems.
- Document software and device firmware version.
- Document network configuration and device settings (e.g., Internet protocol [IP] address and login details) for access and troubleshooting.
- Document cable runs, splice boxes, and device termination points.
- For new installations, ensure that the information in the service arrangement matrix forms part of the bid package requirements and will be a part of the deliverables on the as-built drawings.
- Develop an operational testing schedule based on in-house criteria; testing can be daily, weekly, monthly, or annually. Testing should be an integral part of the organization's security and emergency management plan.
- Document and log system failures as well as abnormalities that can be used as a means of identifying trends that can be mitigated if properly diagnosed.
- Develop good documentation and recording policies that can be conducted with ease and simplicity.
- Develop a maintenance and repair policy that addresses spare parts and other critical devices within each subsystem with a clear understanding and agreement as to who carries the stocking cost of the spare parts required for a prompt response to a service request.
- If there are service contracts, determine the level of support that will be required of the security contractor (e.g., response time, equipment replacement) as well as permissible system downtime conditions and limits as outlined in the organization's security plan.
- If service is performed in-house, the responsibilities of management are to ensure that the service department is properly staffed and supplied with the spares needed to get the system running in the time period laid out in the security policy.
- Work with other groups (e.g., IT, electrical, facilities, HR department) to coordinate operation and maintenance efforts that are common to or affect the security system.
- Develop a set of key system parameters that set bench marks and operational standards that must be maintained for a system to be regarded as functioning and operational.
- Develop a set of key performance indicators (KPIs) that must be achieved to adequately maintain the security posture of the organization.

F.2 Maintenance Plan 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 crime statistics and other 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. If additional capabilities are required, consult with the security contractor on enhancements that can be done to the existing system with a minimal capital outlay.
- Develop educational material that can be distributed to the users of the systems that outlines the benefits of a functioning system but also highlights the potential risks that may result from a malfunctioning, poorly maintained, or improperly used system. This information should be presented in a way that relates to how, when, and where users interface with the systems as well as under what conditions this interfacing occurs.
- Manage the records of people who have left the organization or of those whose entry privileges have been changed or expired. Track, audit, and control individually issued items (e.g., access identification cards) that if lost or stolen could provide unauthorized access to the premises or compromise the integrity of the security system. This task requires close collaboration with the HR department to ensure that the cardholder database reflects the true identity and access privileges of only authorized employees.
- Ensure that the time stamp for the ESS system is perfectly synchronized with the video surveillance system so that facility entry and exit times are aligned with recorded video clips.
- Develop procedures to ensure that archive video is stored as required by either company policies or legal statute.

F.3 Service Contracts

F.3.1 Overview

Most newly installed ESS systems typically are guaranteed or warranted by the security contractor on the reliable operation of the system and components for at least one year from the date the system was accepted for use by the client. Therefore, it is important that this date is properly documented so that a service contract can be in place when the warranty period expires.

The security contractor chosen for maintaining the system per the service contract should be an experienced supplier certified by the manufacturer whose systems are installed through the facility or through the enterprise for organizations with networked-based systems dispersed across large geographic areas.

A security contractor selected for the ESS system should be staffed and equipped to provide the level of response required to deliver prompt and efficient service on short notice. Essential facilities requiring a minimum downtime of any portion of their security systems will require security contractors that offer 24/7 service.

Depending on the type of facility, an in-house maintenance and support team may be considered. The organization may establish an integrated ESS maintenance and support team as part of their facilities group. Because of constant changes in technology and pressure to reduce labor hours, a return on investment (ROI) should be calculated to justify such a path. An option pursued by some large organizations is to have their security contractor provide dedicated maintenance and support to their facility—their sole responsibility is to service and maintain the systems at the client's facility. The advantage of this arrangement is quick resolution to most service problems while maintenance can be done on a more flexible basis. The disadvantage of this arrangement is an increase in cost that may not be aligned with actual hours worked.

F.3.2 Recommendations

A service contract for the ESS system should clearly define the terms and conditions between the organization and the security contractor. Using written agreements that specify the scope of work 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 ESS 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 security contractor's business.
- Method of communicating with the security contractor, including calls occurring outside the security contractor's normal hours of operation.
- Categories of system or device failure matched to an emergency condition. The response time may then be calculated based on the level of the emergency condition that occurs (see Section F.3.3).
- Detailed list of all the systems and related devices to be serviced under the proposed contract, including:
  - 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 PTZ, IP or analog), housings, domes, recording devices, camera controllers, and display monitors.
  - Uninterruptible power supply 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.

To better manage the security contractor's response once a service call has been reported, the organization should formulate the following into its service contract:

- Define the work rules that exist at each facility to be serviced, including those related to parking, building access, means of communicating with local management regarding problems identified, and proposed course of action to restore system to operational condition.
- Develop a method in which management can authorize work to be performed that is not part of the normal service contract; the approval process should be streamlined to expedite authorization and minimize downtime of the system.
- Establish sign-in and sign-out procedures that clearly document the process that is followed in the completion of all service calls.
- List all safety rules that must be adhered to by service personnel while conducting their duties within the facility.
- List work area cleanup, storage of materials, and lockout and tagout procedures.
- Clearly define a list of spare parts that shall be maintained and immediately available for emergency installation in the event of a system or device failure.

List continues on next page

- Identify who is responsible for carrying and maintaining the list of spare parts deemed critical to maintain system operation; who carries this responsibility could impact the contract price and response time.
- Define the access level that will be granted to service personnel, especially in sensitive areas of the facility where an escort may be required for nonemployees.
- Define the procedures for the security contractor's workers seeking access to perform required or requested service. Failure to have a coherent policy could delay the response time if allowing access to service personnel is ambiguous or unclear.

F.3.3 Emergency Response Category

The content of the emergency response category matrix in Table F-1 should be viewed as a guide for organizations developing their own criteria for classification levels of failures.

Table F-1 Emergency Response Category Matrix

Emergency Level Condition	*Device/System Failure*	*Effects on Facility Security Posture*
Level 1	Server, recording system, site perimeter controllers and field panels, and fire alarm detectors and controllers.	Failure of these devices will severely degrade the facility's security operation. Prompt response is required.
Level 2	Access control device failure at vehicle entrance, main lobby, or entrance to sensitive areas; perimeter IDS sensor failure.	These types of failures will reduce the facility's security but can be enhanced by substituting labor hours.
Level 3	Loss of network connectivity at the security device.	Depending upon the system design, this could also be classified as a level 1 failure. Loss of network connectivity from an IP-based surveillance system could result in loss of control and video images. The ESS system and IDS continue to operate with their activities logged in the controller's internal memories by a schedule dump to the server once network connectivity is restored.
Level 4	Software-related issues, resulting in increased manual command and control of a system.	Result may be an increase in cost of labor hours and overall decrease in the efficiency of the security staff.

Appendix G 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 which may be of use to the reader.

Acoustical Society of America (ASA)

- ANSI/ASA S3.2-2009, *Method for Measuring the Intelligibility of Speech over Communication Systems*
- ANSI/ASA S3.41-1990 (R2008), A*udible Emergency Evacuation Signal*

American National Standards Institute (ANSI)

- ANSI S3.41, *Audible Emergency Evacuation Signal*

American Society of Mechanical Engineers (ASME)

- ASME A17.1-2007, *Safety Code for Elevators and Escalators*

ASIS International

- *Protection of Assets Manual*

BICSI

- *Information Technology Systems Installation Methods Manual, 6th edition*
- *Outside Plant Design Reference Manual, 5th edition*
- *Telecommunications Distribution Methods Manual, 13th edition*

Builders Hardware Manufacturers Association

- ANSI/BHMA A156.31-2001, *American National Standard for Electric Strikes and Frame Mounted Actuators*

Constructions Specifications Institute (CSI)

- *The Project Resource Manual: CSI Manual of Practice, 5th edition*

Electronic Components Industry Association (ECIA)

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

European Committee for Electrotechnical Standardization (CENELEC)

- EN 50174-3, *Information Technology—Generic Cabling Systems— Part 3: Industrial Premises*
- EN 50174-4, *Information Technology—Generic Cabling Systems— Part 4: Residential Premises*
- EN 50174-5, *Information Technology—Generic Cabling Systems— Part 5: Data Centres*

FM GLOBAL (FM)

- FM P7825a (2005), *Approval Guide Fire Protection*

Institute of Electrical and Electronics Engineers (IEEE)

- IEEE 802.1X, *Standard for Local and metropolitan area networks-Port-Based Network Access Control*
- IEEE 802.3bt, *Standard for Ethernet Amendment: Physical Layer and Management Parameters for DTE Power via MDI over 4-Pair*
- IEEE 1100 (The IEEE Emerald Book), *Recommended Practice for Powering and Grounding Electronic Equipment*
- ANSI/IEEE C2, *National Electrical Safety Code (NESC)*
- IEEE C62.41.1, *IEEE Guide on the Surges Environment in Low-Voltage (1000 V and Less) AC Power Circuits*
- IEEE C62.41.2, *IEEE Recommended Practice on Characterization of Surges in Low-Voltage (1000 V and Less) AC Power Circuits*

International Code Council

- *International Fire Code®*

International Electrotechnical Commission (IEC)

- IEC 60268-16, *Sound system equipment – Part 16: Objective rating of speech intelligibility by speech transmission index 3rd ed.*
- IEC 60849, *Sound systems for emergency purposes, 2nd ed.*
- IEC 61280-4-1 edition 2.0, *Fibre-optic communication subsystem test procedures – Part 4-1: Installed cable plant – Multimode attenuation measurement*

International Organization for Standardization (ISO)

- ISO 7240-16, *Fire detection and alarm systems – Part 16: Sound system control and indicating equipment*
- ISO/IEC 15693-1, *Identification cards – Contactless integrated circuit(s) cards – Vicinity Cards – Part 1: Physical characteristics*
- ISO/IEC TR 18046, *Information technology – Automatic identification and data capture techniques – Radio frequency identification device performance test methods*
- ISO/IEC TR 18047-3, *Information technology – Radio frequency identification device conformance test methods – Part 3: Test methods for air interface communications at 13,56 MHz*

National Fire Protection Association (NFPA)

- NFPA 1, *Uniform Fire Code*
- NFPA 3, *Recommended Practice on Commissioning and Integrated Testing of Fire Protection and Life Safety Systems*
- NFPA 72®, *National Fire Alarm Code*
- NFPA 80, *Standard for Fire Doors and Other Opening*
- NFPA 90A, *Standard for the Installation of Air Conditioning and Ventilating Systems*
- NFPA 92A, *Standard for Smoke-Control Systems Utilizing Barriers and Pressure Differences*
- NFPA 99, *Health Care Facilities Code*
- NFPA 101®, *Life Safety Code®*
- NFPA 170, *Fire Safety Symbols*
- NFPA 241, *Safeguarding Construction, Alteration, and Demolition Operations*
- NFPA 720, *Standard for the Installation of Carbon Monoxide (CO) Detection and Warning Equipment*
- NFPA 730, *Guide for Premises Security*
- NFPA 731, *Standard for the Installation of Electronic Premise Security Systems*

Security Industry Association (SIA)

- SIA AC-03, *Access Control Badging Guideline*
- SIA DC-02, *Digital Communications Technical Report – Generic Overview of Security Industry Communicator Formats*
- SIA DC-03, *DCS SIA Format Standard*
- ANSI/SIA DC-09, *SIA DCS - Internet Protocol Event Reporting*
- ANSI/SIA OSIPS-DVI, *Open, Systems Integration and Performance Standards – Digital Video Interface Data Model*
- SIA TVAC-01, *TVAC - CCTV to Access Control Standard*

Telecommunication Industry Association (TIA)

- TIA TSB-184-A, *Guidelines for Supporting Power Delivery Over Balanced Twisted-Pair Cabling*
- ANSI/TIA -598-D, *Optical Fiber Cable Color Coding*

Underwriters Laboratories Inc. (UL):

- UL 217, *Standard for Single- and Multiple-Station Smoke Alarm*
- UL 228, *Door Closers-Holders, With or Without Integral Smoke Detectors*
- UL 268, *Standard for Smoke Detectors for Fire Alarm Signaling Systems*
- UL 268A, *Smoke Detectors for Duct Application*
- UL 464, *Standard for Audible Signal Appliances*
- UL 521, *Heat Detectors for Fire Protective Signaling Systems*
- UL 639, *Standard for Safety for Intrusion-Detection Units*
- UL 827, *Standard for Central-Station Alarm Services*
- UL 864, *Control Units and Accessories for Fire Alarm Systems*
- UL 1034, *Burglary-Resistant Electric Locking Mechanisms*
- UL 1480, *Standard for Safety Speakers for Fire Alarm, Emergency, and Commercial and Professional Use*
- UL 1638, *Visual Signaling Appliances - Private Mode Emergency and General Utility Signaling*
- UL 1971, *Signaling Devices for the Hearing Impaired*
- UL 2017, *Standard for Safety for General-Purpose Signaling Devices and Systems*
- UL 2572, *Standard for Mass Notification Systems*
- UL File E349672, Project 11CA44391: *Validated test procedures for Category 5e/Class D and higher cabling for a Single Connector Modified Permanent Link for Direct Attach with and without a consolidation point*

U.S. National Archives and Records Administration (NARA)

- 47 CFR 15 Radio Frequency Devices
- 47 CFR 90 Private Land Mobile Radio Services

Other Standards and Documents

- *Americans with Disabilities Act*, United States Department of Justice
- *Handbook of Video Quality in Public Safety and Security*, United States Department of Homeland Security and Public Safety Communications Research
- *Federal Rules of Evidence*, Public Law 93-595, United States Congress
- *In-Car Video Camera Systems Performance Specifications: Digital Video Systems Module – Version 14, Digital Video Systems Minimum Performance Specifications Document*, International Association of Chiefs of Police
- NIJ CR-xxxx.00, *Law Enforcement Vehicular Digital Multimedia Evidence Recording Systems Certification Program Requirements*, National Institute of Justice, United States Department of Justice
- *Payment Card Industry Data Security Standard (PCI DSS)*, PCI Security Standards Council
- *Defining Video Quality Requirements: A Guide for Public Safety, Volume 1.0,* VQIPS (Video Quality in Public Safety Working Group), Department of Homeland Security's Office for Interoperability and Compatibility partnership with the Public Safety Communications Research program

This page intentionally left blank