Electronic Safety and Security Design Reference Manual

Third Edition









Bicsi®
advancing information technology systems

April 6, 2012

The ESS Credential—The Security Designer's Body of Knowledge in the Development of Effective Security Solutions

Electronic safety and security (ESS) technology is rapidly evolving from analog to digital. Fast-paced change, coupled with the need for design credentials created for industry professionals like you, has led the BICSI Board of Directors to establish the ESS design credential. Later this year, BICSI will offer a revised ESS industry design credential focused around competence, experience, and knowledge.

The BICSI board did not settle for creating this industry credential without close collaboration with other industry-related associations. We have established a friendship agreement with the Electronic Security Association (ESA) to cross-promote education, training, and credentialing in the electronic life safety and security industry. The ESA will assist BICSI and all information technology systems (ITS) industry professionals in providing training for installation craftspeople through the National Training School.

BICSI will provide e-learning and classroom instruction for the industry professional to pursue a career as an ESS design specialist. Through our extensive training network of related professionals, including Master Instructors, Authorized Training Facilities, and Authorized Design Training Programs, BICSI is the preeminent source of information and credentials for the ITS industry.

In today's business environment, the ESS professional is of particular importance to assist in the design of security, protection, and life safety based systems. In the future, the ESS credential holder will assist public, private, and government sector entities with complete and comprehensive system designs that are economical, flexible, and highly integrated.

This third edition of the *Electronic Safety and Security Design Reference Manual* (*ESSDRM*) captures the full scope of designing and documenting the various security systems that ESS designers are likely to encounter.

With every new update of the *ESSDRM*, BICSI has strived to capture the most up-to-date information available in the world of security safety and design. This edition features new information to enhance the command and control of the systems being designed, including updated devices, standards development, a systems correlation platform, and much more.

To capture and document all these changes required the support and participation of a broad cross section of security professionals with expertise in the various industry sectors. Documenting and reviewing the constantly changing body of material was a huge challenge, with the contributors ensuring that the body of material presented is in line with industry standards and best practices of the security design industry.

Many thanks go to our industry volunteers who provided their experience and talent for the benefit of you, the student and reader of BICSI's newest edition of the *ESSDRM*.

I trust you will find the *ESSDRM* to be of critical importance to your knowledge base. I hope you choose to pursue your credential as an ESS Designer, and I want to wish you all the best as you advance your knowledge of the ITS industry.

Thank you for trusting BICSI to help you along the way!



Maxwell A. Stevens
RTKL Associates, Inc.

Thank you for ordering the *Electronic Safety and Security Design Reference Manual*, 3rd edition, 2012. Please place the chapter tabs and appendix tabs in front of the title page for each chapter and appendix.

The section tabs should be inserted in front of the following pages:

Section Tab Placement

Chapter 10: Network Concepts

10-1 Section 1: Network Design Principles

10-31 Section 2: Network Security

We welcome all comments about this manual. If you have any questions about BICSI and its services, please contact our office at 800.242.7405 (USA/Canada toll free); +1 813.979.1991; fax +1 813.971.4311; e-mail bicsi@bicsi.org; website www.bicsi.org.

Electronic Safety and Security Design Reference

M A N U A L

3rd Edition

BICSI®

BICSI®, Tampa, FL 33637
© 2012 BICSI®
All rights reserved
Third edition published 2012
First printing July 2012
Printed in the United States of America

All rights reserved
ISBN (Manual) 1-928886-60-4
ISBN (Electronic) 1-928886-61-2

All brand names, trademarks, and registered trademarks are the property of their respective holders.

No part of this manual may be used, reproduced, or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without prior agreement and written permission from BICSI.

The contents of this manual are subject to revision without notice because of continued progress in electronic safety and security methodology and manufacturing within the information technology systems (ITS) industry.

THIS MANUAL IS SOLD AS IS, WITHOUT WARRANTY OF ANY KIND, RESPECTING THE CONTENTS OF THIS MANUAL, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES FOR THE MANUAL'S QUALITY, PERFORMANCE, MERCHANTABILITY, OR FITNESS FOR ANY PARTICULAR PURPOSE. BICSI SHALL NOT BE LIABLE TO THE PURCHASER OR ANY OTHER ENTITY WITH RESPECT TO ANY LIABILITY, LOSS, OR DAMAGE CAUSED DIRECTLY OR INDIRECTLY BY THIS MANUAL.

BICSI World Headquarters
8610 Hidden River Parkway
Tampa, FL 33637-1000 USA
Tel.: +1 813.979.1991 or
Tel.: 800.242.7405 (USA & Canada toll-free)
Fax: +1 813.971.4311
E-mail: bicsi@bicsi.org
Website: www.bicsi.org

Thank you for ordering the third edition of BICSI's *Electronic Safety and Security Design Reference Manual* (*ESSDRM*). The officers and management of BICSI are pleased to provide an up-to-date design reference manual that offers proven guidelines and methods accepted by the information technology systems (ITS) industry. Volunteers outside the United States and Canada have also provided valuable input to make the newest edition of the *ESSDRM* a valuable tool for an international audience.

As an ITS association, BICSI serves the industry by providing excellent opportunities to learn new technologies through the Registered Communications Distribution Designer (RCDD®) registration program, Registered Information Technology Professional (RITP™), Network Technology Systems (NTS), Outside Plant (OSP), Wireless Design (WD), Data Center Design Consultant (DCDC), Registered Telecommunications Project Manager (RTPM), and Electronic Safety and Security (ESS) designers, telecommunications distribution design and installation courses, and several educational conferences each year.

If you have questions about BICSI and its services, please contact our office at 800.242.7405 (USA and Canada toll-free) or +1 813.979.1991; fax: +1 813.971.4311. You also may contact BICSI via e-mail (bicsi@bicsi.org) or visit our website www.bicsi.org.

Jerry L. Bowman, RCDD, NTS, RTPM, CISSP, CPP; President
Michael A. Collins, RCDD, ITS Technician, CCDA, NCE; President-Elect
Christine Klauck, RCDD, NTS; Secretary
Brian Ensign, RCDD, NTS, OSP, CSI; Treasurer
Carol Everett Oliver, RCDD, ESS; U.S. Northeast Region Director
Mel E. Lesperance, RCDD; U.S. Southeast Region Director
Christy Miller, RCDD, RTPM; U.S. North-Central Region Director
Paul Marek, RCDD, CCNA; U.S. South-Central Region Director
Todd Strand, RCDD, NTS, OSP; U.S. Western Region Director
Peter Levoy, RCDD; Canadian Region Director
Brendan "Greg" Sherry, RCDD, NTS, WD; European Region Director
John D. Clark Jr., CAE; BICSI Executive Director & Chief Executive Officer

WARNING

It is the responsibility of the user of this manual to determine the use of the applicable safety and health practices associated with electronic safety and security (ESS) design and installation practices. BICSI shall not be liable to the purchaser or any other entity with respect to any liability, loss, or damage caused directly or indirectly by the application or use of this manual. No project is so important nor any completion deadline so critical to justify nonconformance to industry standards. This manual does not address safety issues associated with its use. It is the ESS designer's responsibility to use established and appropriate safety and health practices and to determine the applicability of all regulatory issues.

This technical design reference manual is not a single source document but a compendium of many sources of ITS industry-related practices, processes, and procedures.

The information contained in this technical design reference manual includes, but is not limited to, national and international codes, de jure and de facto standards, and industry-accepted best practices. All source information can be found in Appendix A: Codes, Standards, Regulations, and Organizations and the Bibliography and Resources of this manual.

International Credentials

BICSI's professional registration programs are internationally recognized.

- ESS Designer
  - The Electronic Safety and Security (ESS) Designer designation recognizes proficiency in ESS design.
- RCDD®
  - The title Registered Communications Distribution Designer (RCDD®) recognizes those who demonstrate expertise in the design, implementation, and integration of telecommunications and data communications technology systems and related infrastructure components.
- RITP™
  - The title Registered Information Technology Professional (RITP™) recognizes those who demonstrate expertise in the ITS industry but who do not wish to pursue a design credential. The RITP designation also allows individuals to apply formal education and industry-related designations to RITP credential requirements.
- RTPM
  - The title Registered Telecommunications Project Manager (RTPM) recognizes those who demonstrate expertise in all facets of telecommunications project management.
- DCDC
  - The title Data Center Design Consultant (DCDC) recognizes those who demonstrate expertise in all facets of data center design.
- NTS Designer
  - The Network Technology Systems (NTS) Designer designation recognizes proficiency in NTS and internetworking design.
- WD Designer
  - The Wireless Designer (WD) designation recognizes proficiency in wireless design.
- OSP Designer
  - The Outside Plant (OSP) Designer designation recognizes proficiency in OSP design.
- BICSI ITS Installer 1
- BICSI ITS Installer 2, Copper
- BICSI ITS Installer 2, Optical Fiber
- BICSI ITS Technician
  - BICSI ITS Installers and Technicians are proficient in the latest ITS industry standards and codes requirements and in various topics, including the pulling, terminating, testing, and troubleshooting of copper and optical fiber cable using BICSI global best practices as a guide.

 © 2012 BICSI®

Acknowledgments

BICSI's Technical Information and Methods (TI&M) Committee serves to coordinate the information within all of BICSI's technical manuals. BICSI officers, membership, and Technical Publications and Design staff wish to thank the TI&M Committee and its many volunteer contributors who helped in the development of the third edition of BICSI's *Electronic Safety and Security Design Reference Manual* (*ESSDRM*).

The following dedicated subject matter expert team leaders (SMETLs) and subject matter experts (SMEs) provided the key expertise required for the development of this manual's technical content:

TI&M Chair:		**David P. Labuskes, RCDD, NTS, OSP, CTS, CPHIMS, *RTKL Associates, Inc.***
TI&M *ESSDRM* 3rd edition SMETL:		**Maxwell A. Stevens, *RTKL Associates, Inc*.**
Chapter 1 Introduction	**Chapter SMETL:**	**Edward F. Coye, RCDD, NTS, OSP, WD, DCDC, *Tyco AMP***
	SME Contributors:	Robert Y. Faber Jr., RCDD, NTS, *MonoSystems* David P. Labuskes, RCDD, NTS, OSP, CTS, CPHIMS, *RTKL Associates, Inc.*
Chapter 2 Principles of Security	**Chapter SMETL:**	**James K. Goddard, RITP, *GRW Engineers, Inc*.**
	SME Contributors:	Beatriz M. Bezos, RCDD, NTS, OSP, WD, ESS, *Ross & Baruzzini* Philip W. Janeway, RCDD, *TWTelecom* Charles V. Urso, RCDD, *Loftus Engineers*

Acknowledgments, continued

Chapter 3 Electronic Safety and Security Design Process	**Chapter SMETL:**	**Eric R. Ebert, RCDD, OSP, *STV Incorporated***
	SME Contributors:	Edward F. Coye, RCDD, NTS, OSP, WD, DCDC, *Tyco AMP* Robert Y. Faber Jr., RCDD, NTS, *MonoSystems* Anthony Frassetta, RCDD, *A|E Works* Rick Harmon, RCDD, OSP, RTPM, *exp* David P. Labuskes, RCDD, NTS, OSP, CTS, CPHIMS, *RTKL Associates, Inc.* F. Patrick Mahoney, RCDD, *Cannon Design* Maxwell A. Stevens, *RTKL Associates, Inc.*
Chapter 4 Access Control Systems	**Chapter SMETL:**	**F. Patrick Mahoney, RCDD, *Cannon Design***
	SME Contributors:	Edward F. Coye, RCDD, NTS, OSP, WD, DCDC, *Tyco AMP* James A. Darnell, RCDD, NTS, OSP, *Schmidt Associates, Inc.* Robert B. Hertling, RCDD, OSP, *Parsons Transportation Group* David Pedreira, AOC, CSI, CDT, *ASSA ABLOY Door Security Solutions* Maxwell A. Stevens, *RTKL Associates, Inc*. Ben Williams, CSI, *ASSA ABLOY Door Security Solutions*
Chapter 5 Video Surveillance Systems	**Chapter SMETL:**	**Maxwell A. Stevens, *RTKL Associates, Inc*.**
	SME Contributors:	Robert B. Hertling, RCDD, OSP, *Parsons Transportation Group* F. Patrick Mahoney, RCDD, *Cannon Design* Timothy V. Peters, RCDD, WD, *Tech/Knowledge, Inc*. Gregory M. Sparrow, RCDD, NTS, ESS, PMP, CTS, *Signet Electronic Systems, Inc.*

 © 2012 BICSI®

Acknowledgments, continued

Chapter 6 Intrusion Detection Systems	**Chapter SMETL:**	**Maxwell A. Stevens, *RTKL Associates, Inc.***
	SME Contributors:	Eric R. Ebert, RCDD, OSP, *STV Incorporated* Robert B. Hertling, RCDD, OSP, *Parsons Transportation Group* Gregory M. Sparrow, RCDD, NTS, ESS, PMP, CTS, *Signet Electronic Systems, Inc.*
Chapter 7 Fire Detection and Alarm Systems	**Chapter SMETL:**	**Charles V. Urso, RCDD, *Loftus Engineers***
	SME Contributors:	David R. Fohs, NICET Level IV FPET-FA, *Parsons Transportation Group* Michael W. Havens, RCDD, *HDR Architecture, Inc.* Robert B. Hertling, RCDD, OSP, *Parsons Transportation Group* Philip W. Janeway, RCDD, *TWTelecom* Gregory M. Sparrow, RCDD, NTS, ESS, PMP, CTS, *Signet Electronic Systems, Inc.*
Chapter 8 Notification, Communication, and Display Devices	**Chapter SMETL:**	**Maxwell A. Stevens, *RTKL Associates, Inc.***
	SME Contributors:	Eric R. Ebert, RCDD, OSP, *STV Incorporated* William P. Foy, RCDD, NTS, OSP, WD, ESS, *Panduit*
Chapter 9 Special Systems	**Chapter SMETL:**	**Gregory M. Sparrow, RCDD, NTS, ESS, PMP, CTS, *Signet Electronic Systems, Inc.***
	SME Contributors:	William P. Foy, RCDD, NTS, OSP, WD, ESS, *Panduit* Philip W. Janeway, RCDD, *TWTelecom* Maxwell A. Stevens, *RTKL Associates, Inc.*
Chapter 10 Network Concepts	**Chapter SMETL:**	**Timothy V. Peters, RCDD, WD, *Tech/Knowledge, Inc.***
	SME Contributors:	Philip W. Janeway, RCDD, *TWTelecom* Pam Neil, *Tech/Knowledge, Inc.* Alexander Pournelle, *Tech/Knowledge, Inc.* Daniel Spisak, CCNA, *Tech/Knowledge, Inc.*

Acknowledgments, continued

Chapter 11 Systems Integration	**Chapter SMETL:**	**James A. Darnell, RCDD, NTS, OSP,** ***Schmidt Associates, Inc.***
	SME Contributors:	James K. Goddard, RITP, *GRW Engineers, Inc.* Philip W. Janeway, RCDD, *TWTelecom* F. Patrick Mahoney, RCDD, *Cannon Design* Timothy V. Peters, RCDD, WD, *Tech/Knowledge, Inc.*
Chapter 12 System Operation and Commissioning	**Chapter SMETL:**	**Ronald E. Mann, RCDD,** ***Astorino***
	SME Contributors:	Michael W. Havens, RCDD, *HDR Architecture, Inc.* Robert B. Hertling, RCDD, OSP, *Parsons Transportation Group* Charles V. Urso, RCDD, *Loftus Engineers*
Appendix A: Codes, Standards, Regulations, and Organizations	**Chapter SMETL:**	**Robert B. Hertling, RCDD, OSP,** ***Parsons Transportation Group***
	SME Contributors:	Beatriz M. Bezos, RCDD, NTS, OSP, WD, ESS, *Ross & Baruzzini* Robert Y. Faber Jr., RCDD, NTS, *MonoSystems* Anthony Frassetta, RCDD, *A|E Works* Philip W. Janeway, RCDD, *TWTelecom* Robert Jensen, RCDD, *Fluke Networks* Peter Olders, RCDD, NTS, OSP, ITS Technician, *Terra Communications, Inc.* Jeff Silveira, RITP, AStd, *BICSI*
A**ppendix B:** Legal Aspects of Electronic Safety and Security Design	**Chapter SMETL:**	**Meg Gibson-Henlin, Attorney at Law,** ***Henlin Gibson Henlin***
	SME Contributors:	David P. Labuskes, RCDD, NTS, OSP, CTS, CPHIMS, *RTKL Associates, Inc.* Maxwell A. Stevens, *RTKL Associates, Inc.*

 © 2012 BICSI®

Acknowledgments, continued

Glossary	**SMETL:**	**Robert Y. Faber Jr., RCDD, NTS, *MonoSystems***
	SME Contributors:	*ESSDRM* 3rd edition Revision Team
Bibliography and Resources	**SMETL:**	**Robert B. Hertling, RCDD, OSP, *Parsons Transportation Group***
	SME Contributors:	*ESSDRM* 3rd edition Revision Team
Index	**SMETL:**	**Jeff Silveira, RITP, AStd, *BICSI***
Overall Chapter and Appendix Consistency		**Edward F. Coye, RCDD, NTS, OSP, WD, DCDC, *Tyco AMP***

Participants, *ESSDRM* 3rd edition Editorial Review, Tampa, FL, November 3-5, 2011:

Edward F. Coye, RCDD, NTS, OSP, WD, DCDC; **James A. Darnell**, RCDD, NTS, OSP; **Eric R. Ebert**, RCDD, OSP; **William P. Foy**, RCDD, NTS, OSP, WD, ESS; **Robert B. Hertling**, RCDD, OSP; **Philip W. Janeway**, RCDD; **David P. Labuskes**, RCDD, NTS, OSP, CTS, CPHIMS; **F. Patrick Mahoney**, RCDD; **Timothy V. Peters**, RCDD, WD; **Gregory M. Sparrow**, RCDD, NTS, ESS, PMP, CTS; **Maxwell A. Stevens**; and **Charles V. Urso**, RCDD.

BICSI Staff Attending:

Nicole Bryson; John Ditzel; Jeff Giarrizzo, Clarke W. Hammersley; Karen Jacob; David W. Lester, RCDD, NTS, ESS, RTPM, DCDC, ITS Technician; Lois Rosa; and Jeff Silveira, RITP, AStd.

Acknowledgments, continued

The following BICSI Professional Development staff members produced this manual at BICSI World Headquarters, Tampa, FL:

Vice President of Professional Development:	Mark Coppa
Managing Editor–Technical Publications and Design, *ESSDRM* 3rd edition Project Manager:	Clarke W. Hammersley
***ESSDRM* 3rd edition Lead Technical Editor:**	Karen Jacob
***ESSDRM* 3rd edition Technical Co-Editors:**	Jeffrey Giarrizzo Amy Woodland (under contract)
***ESSDRM* 3rd edition Technical Publications Designers:**	Nicole Bryson John Ditzel
Editorial Review Logistics:	Lois Rosa

 © 2012 BICSI®

BICSI Policy for Numeric Representation of Units of Measurement

BICSI technical manuals primarily follow the modern metric system, known as the International System of Units (SI). The SI is intended as a basis for worldwide standardization of measurement units. Generally, units of measurement in this manual are expressed in SI terms, followed by an equivalent imperial (U.S. customary) unit of measurement in parentheses (see exceptions listed below):

- In general, SI units of measurement are converted to an imperial unit of measurement and placed in parentheses. Exception: When the reference material from which the value is pulled is provided in imperial units only, the imperial unit is the benchmark.
- In general, soft (approximate) conversions are used in this manual. Soft conversions are considered reasonable and practicable; they are not precise equivalents. In some instances, equivalents (hard conversions) may be used when it is a:
  - Manufacturer requirement for a product.
  - Standard or code requirement.
  - Safety factor.
- For metric conversion practices, refer to SI 10-02 American Society for Testing and Materials (ASTM)/Institute of Electrical and Electronics Engineers® (IEEE®) SI 10, American National Standard for Use of the International System of Units (SI): The Modern Metric System.
- Trade size is approximated for both metric and nonmetric purposes. Example: 100 mm (4 trade size).
- American wire gauge (AWG) and plywood are not assigned dual designation SI units. Dimensions shown in association with AWGs represent the equivalent solid conductor diameter. When used in association with flexible wires, AWG is used to represent stranded constructions whose cross-sectional area (circular mils) is approximately equivalent to the solid wire dimensions provided.
- In some instances (e.g., optical fiber media specifications), the physical dimensions and operating wavelengths are designated.
- When Celsius temperatures are used, an equivalent Fahrenheit temperature is placed in parentheses.

About BICSI... Advancing Information Technology Systems

BICSI Vision Statement

BICSI® is the worldwide preeminent source of information, education, and knowledge assessment for the constantly evolving information technology systems industry.

BICSI Mission Statement

BICSI's mission is to:

- Lead the information technology systems industry with excellence in publications, education, and knowledge assessment.
- Advance our members' ability to deliver the highest quality products and services.
- Provide our members with opportunities for continual improvement and enhanced professional stature.

Supporting the Information Technology Systems (ITS) Industry

BICSI is a professional association supporting the information technology systems (ITS) industry with information, education, and knowledge assessment for individuals and companies. BICSI serves more than 23,000 ITS professionals, including designers, installers, technicians and telecommunications project managers. These individuals provide the fundamental infrastructure for telecommunications, audiovisual (AV), life safety, electronic safety and security (ESS), data center design, and automation systems. Through courses, conferences, publications, and professional registration programs, BICSI staff and volunteers assist ITS professionals in delivering critical products and services and offer opportunities for continual improvement and enhanced professional stature.

Headquartered in Tampa, Florida, USA, BICSI membership spans nearly 100 countries. For more information, contact BICSI at 800.242.7405 (USA and Canada toll-free) or +1 813.979.1991. You may also e-mail bicsi@bicsi.org or visit www.bicsi.org.

 © 2012 BICSI®

Become a BICSI Member!

BICSI membership is your key to a successful career in the ITS industry. Member benefits extend into the technical, legislative, and even the financial realms of this competitive industry. Membership offers ample opportunities for professional networking and career development and advancement. Membership is open to individuals and corporations serving the ITS and building industries. Join BICSI, and combine your expertise with your colleagues' in the network of ITS professionals.

Corporate Connection Program

The Corporate Connection Program gives BICSI's corporate members what they are looking for in one simple package. With six levels of membership to choose from, we are sure there is something that fits your corporate needs. Whether it's training, conference, or company recognition, the Corporate Connection membership has something for your company needs. Want more information? Call our membership representatives at +1 813.979.1991 or e-mail us at customerservice@bicsi.org.

Member Benefits

Gain the Competitive Edge!

Combine all the benefits of BICSI membership into one complete package, and you will understand why BICSI members hold a competitive advantage. BICSI keeps you ahead of your competition through a continuous flow of new information in the fast-changing field of low-voltage distribution systems. By prominently displaying your BICSI membership, you make known your professional ability to industry contacts.

Fast Access to Information

BICSI's website (www.bicsi.org) is a quick way to find a wide variety of detailed BICSI information. While on the website, find answers to industry questions and communicate with members and colleagues through BICSI's online forums. Search for BICSI members, installers, specialists, and RCDDs. Corporate Connection members also have the option of providing a brief company description and a link to their website.

Member Discounts

BICSI members receive substantial discounts on quality education—manuals, design courses, and conferences. BICSI members also receive discounts on BICSI ITS standards, Cabling Standards Update Newsletter, industry-related reports, Continental Automated Buildings Association (CABA) conferences, and Society of Cable Telecommunications Engineers Inc. (SCTE) products and conferences. Members can also enroll in many InfoComm International® AV courses at BICSI member prices.

In addition, BICSI offers health, dental, vision, disability, term life, accidental death and dismemberment, and errors and omissions insurance rates for yourself and your company.

Member Benefits, continued

Training

BICSI presents leading-edge technical training in all phases of ITS distribution design and installation. These vendor-neutral courses are offered at hundreds of locations across the country and around the world, including nearly 100 BICSI Authorized Training Facilities (ATFs) and several Authorized Design Training Providers (ADTPs).

In addition, BICSI can bring first-class training to your location. All BICSI courses are available for on-site training. BICSI members gain knowledge and continuing education credits (CECs) by attending BICSI courses, conferences, and classes.

BICSI CONNECT

BICSI CONNECT, BICSI's interactive learning network, offers a flexible way to earn CECs and advance your ITS knowledge. BICSI CONNECT is available 24/7, 365 days a year from the convenience of any personal computer, accommodating your scheduling needs, while saving you travel and hotel expenses. Visit www.bicsiconnect.org to view all of the current learning opportunities.

Educational Conferences

Each year, BICSI hosts design conferences in North America as well as regularly scheduled conferences held in other BICSI Districts and Regions worldwide. Conferences include presentations by leaders in the ITS industry and opportunities to network with your peers.

Technical Publications

Become a member and you will receive substantial discounts on BICSI's highly acclaimed manuals—long considered the definitive reference source of the industry. BICSI's manuals serve as valuable reference and study tools for BICSI courses and exams. Also available in electronic downloadable versions, BICSI manuals are based on global best practices that follow and, in many cases, exceed the requirements of recognized international codes, standards, and regulations. Our most popular publications include the *Telecommunications Distribution Methods Manual (TDMM), Network Design Reference Manual (NDRM), Electronic Safety and Security Design Reference Manual (ESSDRM), Information Technology Systems Installation Methods Manual (ITSIMM), Wireless Design Reference Manual (WDRM), AV Design Reference Manual (AVDRM* [a joint publication with InfoComm International®]), and *BICSI Information Transport Systems (ITS) Dictionary*. BICSI publishes many workbooks to complement selected manuals.

Standards

Become a member and you will receive substantial discounts on BICSI's standards publications, including ANSI/BICSI 001-2009, *Information Transport Systems Design Standard for K-12 Educational Institutions*; ANSI/BICSI 002-2011, *Data Center Design and Implementation Best Practices*; ANSI/NECA/BICSI 568-2006, *Standard for Installing Commercial Building Telecommunications Cabling*; and NECA/BICSI 607-2011, *Standard for Telecommunications Bonding and Grounding Planning and Installation Methods for Commercial Buildings.*

Member Benefits, continued

Legislative and Standards Involvement

In the United States, the BICSI Governmental Relations Committee constantly monitors legislative, regulatory, and judicial activities and will advise you of any actions that affect BICSI and its membership. BICSI's representatives take active roles in standards-setting panels and agencies worldwide.

BICSI Community UPLINK

In an effort to reduce inbox clutter, yet still provide members with important information, BICSI has consolidated most of its e-mails into regularly scheduled, monthly e-mails called *BICSI Community UPLINK*. This e-communication features news about upcoming conferences, workshops, and region meetings; calls for presentations; training and exam schedules; announcements from the Board of Directors; new publications; and other newsworthy BICSI information.

Recruiting and Job Search Engine

BICSI's ITS-jobs.com offers the ITS industry an effective tool to bring employers and job seekers together. ITS-jobs.com has an expanded number of resumes and jobs posted and offers an important service for BICSI members and the entire ITS industry.

The web-based resume posting, recruiting, and job search engine is truly an interactive tool. Using ITS-jobs.com, job seekers can post, edit, and update resumes. Areas of expertise can be identified so that employers can more easily find qualified candidates. Automatic notifications are sent when job postings match job seeker criteria.

If you are an employer seeking ITS talent, the extensive search capabilities of ITS-jobs.com help filter experience and background to search for the most qualified candidates.
You also will have access to statistics such as number of views and number of applications for a job posting.

There is no cost to post and manage resumes and apply for jobs. For posting available jobs, employers pay a fee. A discounted rate applies to employers who are BICSI members.

Complete information can be found at www.ITS-jobs.com.

Member Benefits, continued

Newsletters and Website

BICSI helps keep you in touch with industry news and association activities through BICSI News Magazine, BICSI Community UPLINK, ATF Insider, and targeted communications. BICSI's website (www.bicsi.org) provides immediate information about BICSI activities around the world. The site features searchable databases where members and visitors can register for courses, conferences, and exams and participate in online forum discussion topics.

BICSI members also can view a listing of more than 15,000 BICSI credential holders, including RCDDs, specialty designations, and Registered Installers and Technicians. Promote your company online as a BICSI Corporate Connection Member and include a direct link to your website. Purchase manuals and receive "members-only" access to valuable documents.

Join BICSI Today!

BICSI membership is open to individuals and corporations serving the ITS and building industries. Join BICSI, and combine your expertise with your colleagues in the network of ITS professionals. Complete BICSI information is available upon request. For a membership application or other information, contact:

BICSI World Headquarters
8610 Hidden River Parkway
Tampa, FL 33637-1000 USA
Tel.: 800.242.7405 (USA/Canada toll-free) Tel.: +1 813.979.1991
Fax: +1 813.971.4311
E-mail: bicsi@bicsi.org
Website: www.bicsi.org

We welcome your comments about the *ESSDRM*. To do so, simply complete the Reader's Comment Form on the last page of this Preface and return it to BICSI. Our goal is to make BICSI publications the most important design and reference tools in your office.

 © 2012 BICSI®

Comments? More Information?

For information on how to use this manual, see the following page.

To submit comments about the BICSI *Electronic Safety and Security Design Reference Manual* (*ESSDRM*) or for further information about BICSI, please complete the Readers Comment Form in this section or contact:

BICSI World Headquarters
8610 Hidden River Parkway
Tampa, FL 33637-1000 USA
Tel.: 800.242.7405 (USA/Canada toll-free) Tel.: +1 813.979.1991
Fax: +1 813.971.4311
E-mail: bicsi@bicsi.org
Website: www.bicsi.org

HOW TO USE THIS MANUAL

Chapter number and name are indicated at the outside top of each page.

Chapters are divided into sections.

Section Heading

Topic Heading

Each chapter section is divided into multiple subheadings.

Part Heading

Part headings are used to discuss major areas of a topic.

Bullet important terms and phrases.

– Bullets are often followed by more detailed information.

Figures, examples, and tables are numbered sequentially in a given chapter. Each is followed by a brief descriptive title.

Figure 1.1
Title

Page numbers are shown at the bottom of the page. The chapter number precedes the page number.

© 2012 BICSI®

© 2012 BICSI®

Reader's Comment Form

***Electronic Safety and Security Design Reference Manual (ESSDRM),* 3rd edition**

You may use this form to communicate your comments about this publication, its organization, or the subject matter. Your comments will be sent to BICSI's Technical Information and Methods (TI&M) Committee for review and action, if any is deemed appropriate.

Comments (please include specific chapter and page reference; attach a marked-up page when a figure change is needed):

Please complete the following information:

last name	first name	middle initial	date
company name			
mailing address			
city	state/province	zip/postal code	country
daytime phone	fax	e-mail	

Thank you for your comments.

Send to: Attn: *ESSDRM* User Response
BICSI
8610 Hidden River Parkway
Tampa, FL 33637-1000 USA

or fax to: +1 813.971.4311

Office Use Only

Response from Technical Information and Methods Committee:

☐ Class A ☐ Class B ☐ Class C

TI&M Committee chair signature	date
TI&M SME chair signature	date

Table of Contents

Chapter 1: Introduction

Introduction to Safety and Security 1-1
Electronic Safety and Security (ESS) Design Fundamentals 1-4
Current and Future Trends in Safety and Security 1-6
Manual Overview 1-8

Chapter 2: Principles of Security

Principles of Security 2-1
Security Development Theory 2-2
Security Design Basics 2-3
Security Design and Implementation Practitioners 2-9

Chapter 3: Electronic Safety and Security (ESS) Design Process

Electronic Safety and Security (ESS) Design Process 3-1
Architecture and Engineering (A&E) Design Process 3-2
Schematic Design (SD) 3-5
Design Development (DD) 3-19
Construction Document (CD) 3-26
Bidding Phase 3-32
Construction Phase 3-41
Postconstruction Phase 3-46

Chapter 4: Access Control Systems (ACS)

Access Control Systems (ACS) 4-1
Areas of Application 4-4
System Structure 4-7
Design Considerations 4-59
Communications 4-66
System Programming 4-70
System Verification Testing and Startup 4-74
System Training 4-76

Chapter 5: Video Surveillance Systems (VSS)

Video Surveillance Systems (VSS) 5-1
Video Surveillance Systems (VSS) by Function 5-3
Video Surveillance Systems (VSS) Components 5-7
Image Capture/Video Sources 5-11
Transmission 5-43
Processing 5-56
Recording 5-60
Monitoring Devices 5-67
Support Infrastructure 5-85
Video Surveillance Systems (VSS) Interoperability Methods and Practices 5-88
Common Terminology 5-91

Chapter 6: Intrusion Detection Systems (IDS)

Intrusion Detection Systems (IDS) 6-1
Principles of Operation 6-2
Communication Methods 6-5
Electronic Security Components 6-7
Intrusion System Cabling 6-25

Chapter 7: Fire Detection and Alarm Systems

Fire Detection and Alarm Systems 7-1
Classes of Fire Alarm Systems 7-3
Public Fire Alarm Reporting System 7-8
Initiation Devices 7-10
Air-Sampling (Aspirating) Fire Detection Systems 7-18
Other Fire Detection System Devices 7-31
Fire Suppression Systems and Supervision Devices 7-32
Notification Appliances 7-35
Control Units 7-52
Trouble Conditions 7-56
Digital Alarm Communicator System (DACS) 7-61
Transmitters 7-62
Receivers 7-66
Internet Protocol (IP) Alarm Communicator System 7-67

 © 2012 BICSI®

Chapter 8: Notification, Communication, and Display Devices

Notification, Communication, and Display Devices 8-1
Audio Communication Systems 8-1
Voice Communication Systems 8-3
Public Address (PA) Systems 8-6
Video Display Devices 8-11

Chapter 9: Special Systems

Special Systems 9-1
Nurse Call 9-1
Radio Frequency Identification (RFID)-Based Systems 9-10

Chapter 10: Network Concepts

SECTION 1: NETWORK DESIGN PRINCIPLES

Network Design Principles 10-1
Information Technology (IT) and Electronic Safety and Security (ESS) 10-2
Internet Protocol (IP) Network Architecture 10-10
Internet Protocol (IP)-Based Access Control Systems (ACS) 10-15
Internet Protocol (IP)-Based Video Surveillance Systems (VSS) 10-17
Internet Protocol (IP)-Based Voice Communication Systems 10-19
Miscellaneous Systems Utilizing Internet Protocol (IP) 10-24

SECTION 2: NETWORK SECURITY

Network Security 10-31
Risks 10-33
Control Measures 10-36

Chapter 11: Systems Integration

Systems Integration 11-1
Fundamentals of Integration 11-7
Electronic Safety and Security (ESS) Components 11-9
Understanding the Risks Involved with Integration 11-24

Chapter 12: System Operation and Commissioning

System Operation and Commissioning 12-1
Operation 12-2
Maintenance Plan 12-5
Commissioning 12-12

Appendix A: Codes, Standards, Regulations, and Organizations

Introduction A-1
International Codes and Standards A-6
Regional Codes and Standards A-27
National Codes and Standards A-38
Enforcement of United States (U.S.) Building Codes, Standards, and Regulations . . . A-62
Regulations and Standards for Wireless Transmission A-66
Wireless Standards Development Organizations A-67
United States (U.S.) Approval of Electrical Products and Equipment A-70
Canadian Approval of Electrical Products and Equipment A-72

Appendix B: Legal Aspects of Electronic Safety and Security (ESS) Design

Legal Aspects of Electronic Safety and Security (ESS) Design B-1

Glossary

Glossary Terms Gls-1
Acronyms and Abbreviations Gls-37

Bibliography and Resources

Index

 © 2012 BICSI®

Figures

Chapter 2: Principles of Security

Figure 2.1 Security balance 2-2
Figure 2.2 Vulnerability model 2-4
Figure 2.3 Elements of a security program 2-7
Figure 2.4 Layering. 2-8

Chapter 3: Electronic Safety and Security (ESS) Design Process

Figure 3.1 Design process 3-4
Figure 3.2 Design bid build contract 3-36
Figure 3.3 Design build contract. 3-37

Chapter 4: Access Control Systems (ACS)

Figure 4.1 Request to exit devices 4-17
Figure 4.2 Electrified exit hardware 4-18
Figure 4.3 Door contacts 4-19
Figure 4.4 Calculation chart 4-24
Figure 4.5 Types of relay configurations 4-29
Figure 4.6 Electric strikes 4-33
Figure 4.7 Magnetic locks 4-35
Figure 4.8 Electric locksets 4-36
Figure 4.9 Electric latch and bolt 4-37
Figure 4.10 Control trim 4-38
Figure 4.11 Delayed egress devices 4-39
Figure 4.12 Door closer hardware 4-41
Figure 4.13 Biometric characteristics 4-52
Figure 4.14 Biometrics in physical access control application 4-54
Figure 4.15 Biometrics in user identification application 4-55
Figure 4.16 Biometrics in logical access control application 4-55
Figure 4.17 Example of access control system floor plan. 4-63

Chapter 5: Video Surveillance Systems (VSS)

Figure 5.1 Analog camera components 5-12
Figure 5.2 Internet protocol video camera components. 5-14
Figure 5.3 Internet protocol camera with analytics 5-15
Figure 5.4 Charge-coupled device imagers and lens compatibility 5-28
Figure 5.5 300 Millimeter lens at f/8 5-33
Figure 5.6 300 Millimeter lens at f/2.8 5-33
Figure 5.7 300 Millimeter lens at f/2.8 5-33
Figure 5.8 Comparison of total reflectance between asphalt and concrete 5-35
Figure 5.9 National Television System Committee waveform 5-43

Figure 5.10 Analog system without matrix switch 5-70
Figure 5.11 Analog system with matrix switch 5-71
Figure 5.12 Internet protocol video system embedded recording 5-72
Figure 5.13 Network video system for point of sale applications. 5-73
Figure 5.14 Hybrid Internet protocol video system with recording server 5-74
Figure 5.15 Remote network video monitoring system using software as a service. . . . 5-75

Chapter 6: Intrusion Detection Systems (IDS)

Figure 6.1 Logical intrusion detection systems diagram. 6-2
Figure 6.2 Liquid crystal display keypad 6-10
Figure 6.3 Passive infrared detector 6-11
Figure 6.4 Two styles of acoustic glass break detectors. 6-12
Figure 6.5 Window shock sensor 6-13
Figure 6.6 Surface-mounted magnetic switches 6-14
Figure 6.7 Examples of recessed magnetic switches 6-15
Figure 6.8 Roller ball switch. 6-15
Figure 6.9 Plunger switch 6-16
Figure 6.10 Floor-mounted overhead door switch. 6-16
Figure 6.11 Single beam photoelectric detector 6-18
Figure 6.12 Long-range dual beam photoelectric detector 6-18
Figure 6.13 Radar sensor controlling a pan, tilt, and zoom camera. 6-20
Figure 6.14 Indoor speaker or siren 6-21
Figure 6.15 Outdoor speaker or siren 6-21
Figure 6.16 Types of line supervision 6-26
Figure 6.17 States of a magnetic switch 6-27
Figure 6.18 Resistor color code chart 6-28

Chapter 7: Fire Detection and Alarm Systems

Figure 7.1 Larger central station retransmit chain 7-6
Figure 7.2 Typical ionization smoke detector 7-12
Figure 7.3 Photoelectric smoke detector using principle of light obscuration 7-14
Figure 7.4 Typical photoelectric smoke detector using principle of light scattering . . . 7-14
Figure 7.5 Typical photoelectric beam-type detector 7-16
Figure 7.6 Typical duct smoke-type detector 7-17
Figure 7.7 Air-sampling system 7-21
Figure 7.8 Typical fixed temperature heat detector 7-22
Figure 7.9 Typical rate-of-rise heat detector 7-24
Figure 7.10 Principle of operation of typical combination rate-of-rise and fixed temperature heat detector 7-25
Figure 7.11 Typical infrared flame detector 7-27
Figure 7.12 Typical detector coverage areas 7-30
Figure 7.13 Typical fire alarm pull station 7-31

 © 2012 BICSI®

Figure 7.14 Typical water flow detector 7-32
Figure 7.15 Typical valve tamper switch 7-33
Figure 7.16 Typical pressure switch 7-34
Figure 7.17 Typical fire alarm bell 7-36
Figure 7.18 Typical fire alarm chime 7-37
Figure 7.19 Typical fire alarm chime with integrated strobe 7-37
Figure 7.20 Typical fire alarm horn 7-38
Figure 7.21 Typical fire alarm horn with integrated strobe 7-38
Figure 7.22 Typical fire alarm speaker 7-40
Figure 7.23 Typical fire alarm speaker with integrated strobe 7-40
Figure 7.24 Typical fire alarm strobe 7-41
Figure 7.25 Typical visible notification appliance coverage pattern 7-45
Figure 7.26 Visible notification appliance placement 7-46

Chapter 9: Special Systems

Figure 9.1 Typical nurse call staff emergency station 9-3
Figure 9.2 Typical nurse call bedside station 9-4
Figure 9.3 Typical nurse call code call station 9-5
Figure 9.4 Typical nurse call staff station 9-6
Figure 9.5 Nurse call system traditional one-line diagram 9-9
Figure 9.6 Typical radio frequency identification tag 9-10

Chapter 10: Network Concepts

Figure 10.1 Open Systems Interconnection Reference Model 10-11
Figure 10.2 Message transfer described using the Open Systems Interconnection Reference Model 10-13
Figure 10.3 End-to-end Internet protocol paging system diagram 10-21
Figure 10.4 Hybrid Internet protocol/traditional paging system diagram using an Internet protocol backbone 10-22
Figure 10.5 Hybrid Internet protocol/traditional fire alarm system diagram 10-26
Figure 10.6 Hybrid Internet protocol/traditional intrusion detection systems diagram 10-28
Figure 10.7 Hybrid Internet protocol/traditional nurse call system diagram 10-30
Figure 10.8 Stand-alone network 10-37
Figure 10.9 Enterprise network 10-38
Figure 10.10 Example of security zones 10-40

Chapter 11: Systems Integration

Figure 11.1 Typical access control configuration 11-10
Figure 11.2 Sample physical security information management system 11-13
Figure 11.3 Typical network building automation system 11-16

Appendix A: Codes, Standards, Regulations, and Organizations

Figure A.1 Conformité européenne (CE) mark A-72

Tables

Chapter 3: Electronic Safety and Security (ESS) Design Process

Table 3.1 Drawing set systems 3-21
Table 3.2 *SectionFormat*™ outline 3-28

Chapter 4: Access Control Systems (ACS)

Table 4.1 Circular mils of standard American wire gauge conductors 4-27
Table 4.2 Voltage drop per 30 meter (m [100 feet (ft)]) run of paired wire (61 m [200 ft] total length of wire) 4-28
Table 4.3 Comparing smart card technologies 4-48
Table 4.4 Personal identification biometric systems 4-53
Table 4.5 Sizing for biometric applications 4-56
Table 4.6 Biometric performance parameters 4-57
Table 4.7 Access level matrix 4-62

Chapter 5: Video Surveillance Systems (VSS)

Table 5.1 Internet protocol and analog video comparison 5-9
Table 5.2 Image formats and sizes 5-20
Table 5.3 Types of lenses 5-29
Table 5.4 Stop and brightness chart 5-31
Table 5.5 Color temperature 5-36
Table 5.6 Light sources and their behavior 5-37
Table 5.7 Color rendition 5-38
Table 5.8 International Organization for Standardization resolution chart 5-39
Table 5.9 Surveillance video function/resolution/maximum field of view 5-41
Table 5.10 Typical coaxial cable signal losses 5-47
Table 5.11 Frame size estimates 5-65

Chapter 6: Intrusion Detection Systems (IDS)

Table 6.1 Detection sensor technology and application 6-3

Chapter 7: Fire Detection and Alarm Systems

Table 7.1 Temperature classification for heat-sensing fire detectors 7-23
Table 7.2 Typical ambient sound levels by location 7-43
Table 7.3 Room spacing for wall-mounted visible appliances 7-47
Table 7.4 Room spacing for ceiling-mounted visible appliances 7-48

 © 2012 BICSI®

Chapter 8: Notification, Communication, and Display Devices

Table 8.1 Audio signal distance limitations 8-8

Chapter 10: Network Concepts

Table 10.1 Challenges to Internet protocol migration 10-24

Chapter 11: Systems Integration

Table 11.1 Multiple systems 11-12

Chapter 12: System Operation and Commissioning

Table 12.1 Service arrangement matrix 12-2
Table 12.2 Access control operation matrix 12-6
Table 12.3 Surveillance operation matrix 12-7
Table 12.4 Access control key performance example data (notional) 12-8
Table 12.5 Emergency response category matrix (notional) 12-10

Appendix A: Codes, Standards, Regulations, and Organizations

Table A.1 Relationship between series EN 50174 and other design standards A-28
Table A.2 Sections of the *Canadian Electrical Code* A-42
Table A.3 Federal Communications Commission documents A-47
Table A.4 *NESC*® parts, sections, and rules applicable to telecommunications distribution requirements A-49
Table A.5 *NEC*® 2011 chapters, articles, and sections that impact telecommunications installation A-53
Table A.6 Federal safety health standards A-64
Table A.7 Federal Communications Commission regulations A-67

Examples

Chapter 5: Video Surveillance Systems (VSS)

Example 5.1 Optical fiber performance calculations worksheet 5-51

Chapter 1
Introduction

Chapter 1 provides an overview of the fundamental aspects of the industries that influence electronic safety and security (ESS) design.

Table of Contents

Introduction to Safety and Security 1-1
Industry Changes 1-2
Electronic Safety and Security (ESS) Bodies of Knowledge 1-3
Electronic Safety and Security (ESS) Design Fundamentals 1-4
Access Control 1-4
Surveillance 1-4
Intrusion Detection 1-4
Fire Detection and Alarm 1-5
Special Systems 1-5
Network Security 1-5
Integrated Systems 1-5
Types of Projects 1-5
Current and Future Trends in Safety and Security 1-6
Information Technology (IT) 1-6
Physical Security 1-6
Integration of Access Control Systems (ACS) and Building Automation Systems (BAS) 1-7
Video Surveillance 1-7
Technology Advancements and Convergence 1-7
Manual Overview 1-8
Chapter 2: Principles of Security 1-8
Chapter 3: Electronic Safety and Security (ESS) Design Process 1-8
Chapter 4: Access Control Systems (ACS) 1-8
Chapter 5: Video Surveillance Systems (VSS) 1-9
Chapter 6: Intrusion Detection Systems (IDS) 1-9
Chapter 7: Fire Detection and Alarm Systems 1-9
Chapter 8: Notification, Communication, and Display Devices 1-9
Chapter 9: Special Systems 1-9
Chapter 10: Network Concepts 1-10
Section 1: Network Design Principles 1-10
Section 2: Network Security 1-10
Chapter 11: Systems Integration 1-10
Chapter 12: System Operation and Commissioning 1-10
Appendix A: Codes, Standards, Regulations, and Organizations 1-11
Appendix B: Legal Aspects of Electronic Safety and Security (ESS) Design 1-11

Introduction to Safety and Security

The *Electronic Safety and Security Design Reference Manual* (*ESSDRM*) is designed to educate and inform professionals engaged in the electronic safety and security (ESS) arena. Safety is protection against hazards, while security is protection against threats. To be safe is to be protected, while to be secure is to be free from danger. Protection leads to a condition of being free from danger or threat, which ultimately reduces risks.

The *ESSDRM* discusses trends and expertise in security areas that apply to information technology systems (ITS) and the integration of ESS systems.

IMPORTANT: The *ESSDRM* is not intended to be a stand-alone reference manual; therefore, the construction of a comprehensive ESS design requires reference to additional bodies of knowledge.

This manual presents a guideline for the design and deployment of ESS systems and should never be used in place of a legal opinion. An ESS designer should be familiar with the laws governing surveillance, legislation that is pending, and the requirements of the authority having jurisdiction (AHJ). The ESS designer should seek multiple legal opinions and use these opinions and established standards, guidelines, and best practices to deploy an ESS system as part of the overall security master plan.

The security industry has standards, practices, and organizations dedicated to defining and refining those practices. In addition to the *ESSDRM*, BICSI® is developing an industry standard for the design and implementation of structured cabling for ESS systems. This reference manual provides information from both the security and ITS industries so that professionals in both industries will have a common understanding of each other's roles in designing and implementing ESS systems.

Industry Changes

Prior to 1996, security systems were viewed as an option to most architectural projects. With the specialized cabling and equipment required for installation, not many changes were made to the products offered within the industry for a number of years. That changed when the first Internet protocol (IP) camera was introduced to the industry in 1996.

The opportunity to use standards-based telecommunications cabling and cabling infrastructure was tempered with other complex issues. IP cameras tended to have extremely high bandwidths. Users also had to consider whether to maintain or abandon the analog systems they had previously implemented.

As late as 2002, there was some speculation that hybrid systems would remain very popular over the use of pure IP systems. In spite of this speculation, the IP camera market expanded dramatically. ESS equipment suppliers, system integrators, and users began to consider the integration and implementation of entire safety and security systems on an IP platform.

This discipline has grown from the early human guarding of objects to sophisticated surveillance cameras and building automation systems (BAS). Each began as a stand-alone system, but the rise of networks and ITS has lead to an increased need to converge multiple systems. As technology develops at a rapid pace, its influence in the relatively stable world of security is ongoing and ever changing.

Advancements in common infrastructure have enabled manufacturers to create systems based on similar network protocols, allowing different systems to communicate with one another. The simple beginnings, exemplified by the employment of guards and patrols, have progressed to complex advancements in surveillance that have enabled the addition of intelligence to electronic security systems and BAS.

The cost benefits of cabling infrastructure convergence can be seen with lower cabling costs; easy modifications for moves, adds, or changes (MACs); unified integration with other information technology (IT) environments; elimination of specialized equipment; and space savings by using ITS servers and storage devices instead of video cassette recorder (VCR) tapes and video recorders.

 © 2012 BICSI®

Electronic Safety and Security (ESS) Bodies of Knowledge

The ESS designer should have knowledge of:

- ITS fundamentals.
- Principles of security.
- Design process.
- Preliminary security design.
- Architecture and engineering (A&E) design.
- IP design.
- Security systems.
- Access control systems (ACS).
- Surveillance systems.
- Intrusion detection.
- Fire alarms.
- Special systems.
- Network security.
- Systems integration.
- Project management.
- Systems operation and commissioning.

Chapters in this manual are devoted to areas and practices that influence the design of a security system. These chapters address:

- Security consulting.
- Design practices.
- Codes, standards, regulations, and organizations.
- Legal issues.
- The design process of the Construction Specifications Institute (CSI) and the American Institute of Architects (AIA).

With the expansion of security and special systems, nontraditional bodies of knowledge that can now be included in the responsibilities of the ESS designer include the following systems:

- Voice and notification.
- Nurse call.
- Mustering.
- Radio frequency identification (RFID) inventory management.

Electronic Safety and Security (ESS) Design Fundamentals

The practice of safety and security design involves the ability to use and integrate various practices, methodologies, and devices, resulting in improved safety and security. Many elements of design are unique to the protection of life and property, and others are multidisciplinary.

The ESS designer must have a thorough understanding of the fundamentals described in detail throughout this manual 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. Physical and ESS systems must work as a comprehensive package. The ESS designer must understand how they influence each other to be successful.

Access Control

Access control is the process by which access to an asset or location can be limited to those individuals expressly authorized for its use. 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.

Surveillance

Video surveillance is a widely used technology within ESS systems, and it involves the use of cameras for watching or controlling assets. Video surveillance is the process of image:

- Capturing.
- Transmitting.
- Processing.
- Viewing.
- Recording.

This technology requires knowledge of cameras and their placement, image transmission, and recording principles.

Intrusion Detection

Intrusion detection is often viewed as part of the ACS 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 must 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 people in secure zones. Intrusion detection systems (IDS) can generate simple local or paging alarms, or they can be integrated with other systems to provide more active responses (e.g., turning on cameras or lighting).

 © 2012 BICSI®

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.

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.

Network Security

As more systems migrate to the network, the issues associated with protecting those systems must be addressed. Isolation can provide protection, but it comes 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.

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 applications, including facilities, campuses, vehicles, and personal tracking.

Types of Projects

An ESS project may be:

- An original design.
- A retrofit of an existing plan.
- An upgrade or replacement of an existing system.

To successfully complete a project, the ESS designer must be able to interact with building owners, tenants, architects, engineers, and security professionals. Additionally, the ESS designer may need to consult end users and other stakeholders.

Current and Future Trends in Safety and Security

Several areas in ESS design are affected by rapid advancement in technology, including:

- IT.
- Physical security.
- Integration of ACS and BAS.
- Video surveillance.
- Technology advancements and convergence.

Information Technology (IT)

Most current systems have migrated to the use of the IP network for communication 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 must understand the system communication methods, the required infrastructure particular to the specific system installed, and the effect network outages will have on system functionality.

The ESS designer must 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 must 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.

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.

 © 2012 BICSI®

Integration of Access Control Systems (ACS) and Building Automation Systems (BAS)

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. The 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 BAS, 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 ACS integrates with BAS and subsystems in the surrounding areas is becoming a major factor in the design of ACS.

Video Surveillance

Video 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.

Many factors will affect the selection, including court admissibility, network impact, and available space within buildings to house equipment.

Technology Advancements and Convergence

Technology's growing impact on security has led to the convergence of many systems. Convergence can encompass a range of capabilities, from limited monitoring to full command and control functions across a common IP network.

Some of the most common types of convergence are the interconnection of:

- Multiple systems within a single site.
- Single systems across multiple sites.
- Multiple systems across multiple sites.

This shift in implementation is driving a change in both the security industry and communications industry. Professionals in both industries have to learn more concerning each industry. Today's successful security professionals must understand the cabling infrastructure required for an installation, while cabling infrastructure professionals are asked to perform more safety and security related tasks.

Manual Overview

This third edition of the *ESSDRM* comprises 12 chapters and two appendixes that contain information intended to assist both security specialists and IT professionals in understanding the systems and the convergence that occurs between the industries. The following is a brief description of what the reader can expect to find in each chapter of this reference manual.

Chapter 2: Principles of Security

Chapter 2 discusses security planning and applications that pertain to the integration of a system of deterrence and detection by electronic means, including the:

- Basics of security theory.
- Fundamentals of security design.
- Roles of practitioners involved in electronic security systems.
- Skills and experience required for each role.

Chapter 3: Electronic Safety and Security (ESS) Design Process

Chapter 3 introduces the ESS design process by discussing the various types of contractual relationships and the following design process phases:

- Schematic design
- Design development
- Construction documentation
- Bidding
- Construction administration
- Postconstruction

Chapter 3 also provides guidance to the ESS designer to adequately address the information from the client as prepared by a consultant, including:

- Threat assessment.
- Client interview.
- Facility location analysis.

Additionally, the roles of team members and the interaction between those individuals during the various design process phases are explored.

Chapter 4: Access Control Systems (ACS)

Chapter 4 explores the purpose and application of ACS. The various types of systems are discussed, including a review of the hardware and software requirements. RFID and IP integration are included in this chapter.

 © 2012 BICSI®

Chapter 5: Video Surveillance Systems (VSS)

Chapter 5 provides an overview of video surveillance fundamentals. Designing with a perspective-oriented approach is discussed. The progression from analog also is explained.

Chapter 6: Intrusion Detection Systems (IDS)

Electronic intrusion detection is designed to both ensure the detection of and allow a timely response or deterrent to security breaches that may adversely affect people and property. Chapter 6 explores the basics of design and provides examples of the application of various types of sensors to provide intrusion detection.

Chapter 7: Fire Detection and Alarm Systems

Chapter 7 provides an overview of the complex subject of fire detection and alarm systems, including:

- Classes of fire alarm and detection systems.
- Components that initiate a fire alarm condition.
- Detectors and systems currently available.
- Fire suppression systems and their related initiation devices.
- Notification appliances.

Chapter 8: Notification, Communication, and Display Devices

Notification and display devices provide a means of communicating a message through the use of audio or display devices or a combination of both. Chapter 8 discusses:

- Audio communication.
- Emergency telephones.
- Public address and paging.
- Display devices.

Chapter 9: Special Systems

Chapter 9 explains the design and application of various specialty systems. It provides an ESS designer with the fundamental tools necessary to properly design some of the more basic systems as well as a level of knowledge necessary to work in cooperation with the specific system providers. Some of the systems discussed include:

- Nurse call.
- RFID.
- At-risk human perimeter systems.
- Asset management systems.

Chapter 10: Network Concepts

Chapter 10 is divided into two sections:

- Network design principles
- Network security

Section 1: Network Design Principles

The first section provides an introduction to the design principles for IP-based ESS systems. It includes a brief overview of the IP network-based security world, followed by a general introduction to network architecture and the considerations necessary for the planning, design, and implementation of state-of-the-art systems.

Section 2: Network Security

The second section focuses on a broad overview of threats and countermeasures for network security as it relates to IP-based ESS system design. Risks and control measures are explained and discussed.

Chapter 11: Systems Integration

Chapter 11 discusses the concepts, systems, and processes related to the integration of ESS, including:

- ESS systems.
- Command and control.
- Data networks.
- Building automation.
- Fire-life-safety.
- Energy/lighting management.

Chapter 12: System Operation and Commissioning

Chapter 12 provides ESS designers, security contractors, and end users with a framework to develop standardized policies and procedures.

 © 2012 BICSI®

Appendix A: Codes, Standards, Regulations, and Organizations

Appendix A provides an overview of the codes, standards, and regulations that the ESS designer must work with, including:

- Telecommunications.
- Building and construction.
- Electrical.
- Fire protection.
- Life safety.
- Security.

Appendix B: Legal Aspects of Electronic Safety and Security (ESS) Design

Appendix B examines some of the legal issues relevant to the ESS designer regarding liability and risk.



Chapter 2
Principles of Security

Chapter 2 discusses security planning and applications that pertain to the integration of a system of deterrence and detection by electronic means, including the basics of security theory, fundamentals of security design, roles of practitioners involved in electronic security systems, and skills and experience required for each role.

Table of Contents

Principles of Security 2-1
Introduction 2-1
Security Development Theory. 2-2
Overview 2-2
Security Design Basics 2-3
Security Assessment Process 2-3
Asset Identification 2-3
Threat and Risk Identification 2-3
Categories of Threats 2-5
Balanced Approach to Design 2-6
Layering 2-8
Security Design and Implementation Practitioners 2-9
Overview 2-9
Security Consultant 2-9
Role 2-9
Profile 2-9
Security Designer 2-10
Role 2-10
Profile 2-10
Security Installer 2-11
Role 2-11
Profile 2-11
Systems Integrator 2-11
Role 2-11
Profile 2-11

Figures

Figure 2.1 Security balance 2-2
Figure 2.2 Vulnerability model 2-4
Figure 2.3 Elements of a security program 2-7
Figure 2.4 Layering. 2-8

Principles of Security

Introduction

An asset is anything tangible or intangible that has value. The safety and security of a valuable asset can be enhanced by the use of proper countermeasures. A combination of the principles outlined in this manual should be employed to provide the necessary security to ensure safety. This chapter considers the security planning and applications that relate to the integration of a system of deterrence and detection by electronic means.

Economics are a fundamental determinant of any system design. A balance between the value of the asset to be protected and the cost of protection is a key factor in security system design. The more valuable the asset, the more elaborate the security system design. Safety and security should not impede the practical use of the asset.

As technology constantly changes, the design and installation of electronic safety and security (ESS) systems continue to evolve. Both security system components and the property to be protected continue to become more sophisticated. The practitioners of security systems (e.g., consultants, designers, installers, integrators) must constantly change to keep pace with the evolution of their trade. The challenges of change are not only with technological advancements but also with changes in culture and society. Shifts in the value of property, both tangible and intangible, are considerable. As more of our assets become electronic in nature, the lines between electronic security and information security (InfoSec) will blur.

The purpose of this chapter is to:

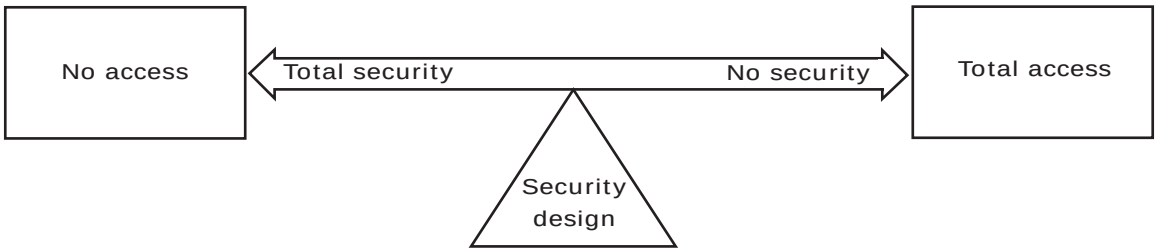
- Outline the basics of security theory.
- Provide an understanding of the fundamentals of security design.
- Identify the various roles of practitioners involved in the development and implementation of ESS systems.
- Outline the skills and experience required for each role.

Security Development Theory

Overview

Security is the level of protection provided against danger, damage, loss, and crime. Theoretically, absolute security for an individual would require total isolation from a normal environment and other people; absolute security for a tangible object or asset would require that it be completely isolated from access. The complete isolation of a person or asset is not practicable and is rarely possible. Accessibility is an integral part of asset value, and centralizing information in one location ensures that updates are available to users. Providing safety and security is a balancing act between access and isolation. Figure 2.1 demonstrates this balance.

Figure 2.1
Security balance



Security is not an absolute. Even with total isolation, there is no guarantee of safety. As addressed later in this chapter, the practice of security consulting requires:

- Assessing known and potential threats.
- Estimating the likelihood that threats will occur.
- Recommending a pragmatic system of prevention.

This is sometimes referred to as the risk formula, which is outlined as:

$$\text{Risk} = \frac{\text{Threat} \times \text{Vulnerability} \times \text{Impact}}{\text{Control measures}}$$

Several examples of risk are as follows:

- Example 1—Threat of blizzard conditions in southern Florida:
  - Vulnerability is low
  - Impact is low
  - Control measures would be little to nonexistent (cost could be low)
- Example 2—Threat of theft in properties located in high crime areas:
  - Vulnerability is high
  - Impact is high
  - Control measures would be more extensive (cost could be high)

 © 2012 BICSI®

Security Design Basics

Security Assessment Process

It is the consultant's role to thoroughly assess the asset to be protected, its environment, and any potential risks that exist or could develop. The consultant must analyze architectural and operational security. The impact of protection must be compared with the impact of loss. The designer and integrator must consider existing systems and ensure compatibility with any new systems. The designer also must detail the conditions that the installer is likely to encounter.

Asset Identification

Examples of assets are:

- People—Tenants, customers, employees, contractors, guests, and under some legal concepts, even trespassers.
- Property—Real and personal property of monetary or perceived value.
- Operations—Patents, processes, reputation, and goodwill.
- Information—Proprietary data, trade secrets, client information, and business plans.

Threat and Risk Identification

A threat or risk can be described as follows:

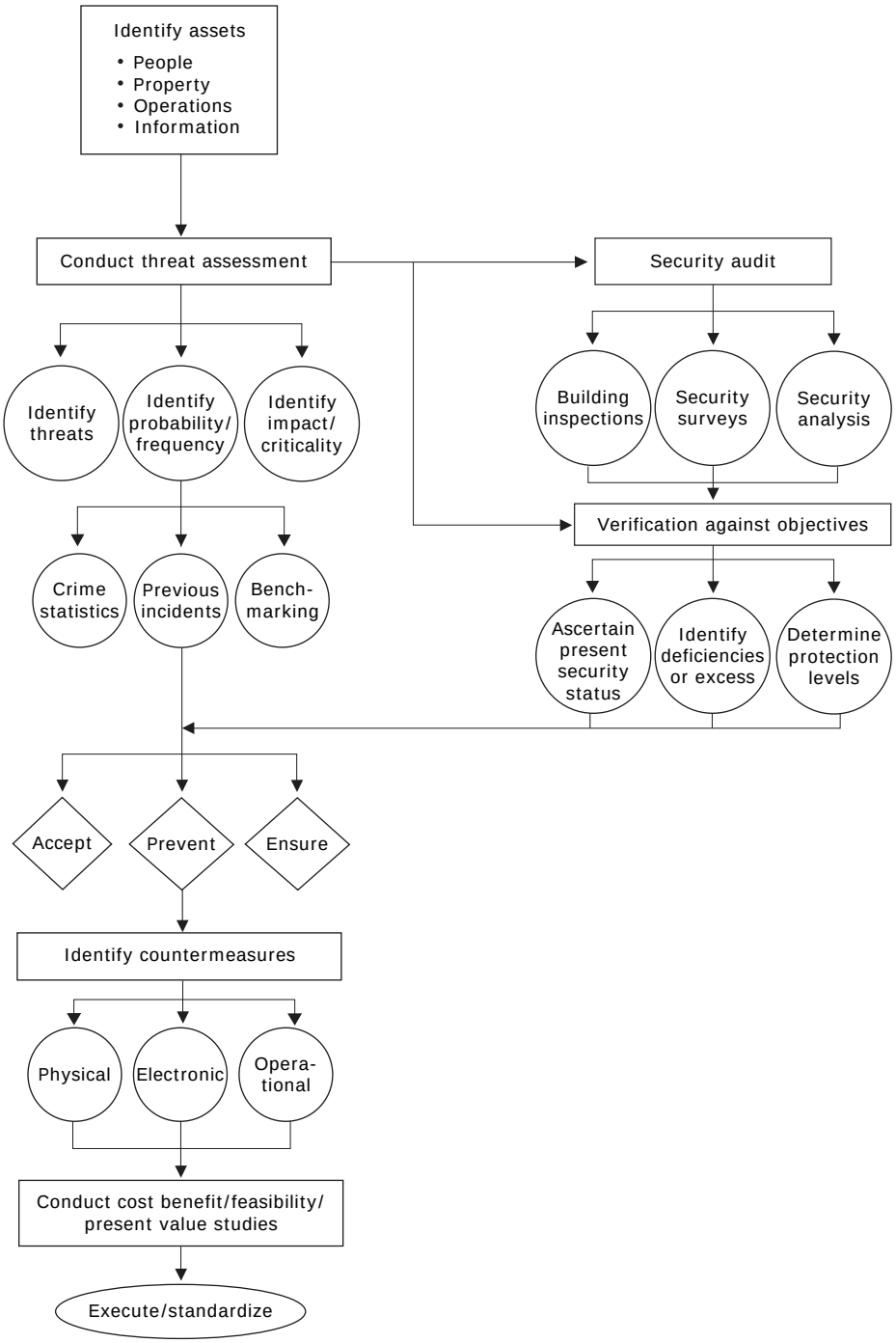
- Threat is an indication of an event or the intent to do harm or damage.
- Risk is a vulnerability to, or potential for, loss from a threat or event.

The task of identifying threat and risk is expressed in numerous vulnerability models that are available across many industries. This equally applies to the security industry. The model shown in Figure 2.2 represents the key components of vulnerability assessments, audits, and surveys.

Although this figure does not show the considerable detail required, it should be noted that the ultimate goals are to quantify and qualify all aspects of this flow diagram and minimize subjectivity.

Threat and Risk Identification, continued

Figure 2.2
Vulnerability model



 © 2012 BICSI®

Categories of Threats

Knowing and identifying the types of potential threats are critical to the security design. It is commonly thought that the potential for damage or loss can be subdivided into several categories.

The generally accepted categories of threats are:

- Temperature—Includes sunlight, fire, freezing, and excessive heat.
- Chemicals and gases—Usually applies to chemical warfare gases, commercial vapors, humidity, dry air, suspended particles, smoke, smog, cleaning fluid, fuel vapors, products of combustion, fuel leaks, acid, and paper particles from printers.
- Liquids—Include floods, plumbing failures, precipitation, and spilled drinks.
- Biological—May include viruses, bacteria, people, animals, and insects. Examples are illness of key workers, molds, contamination from skin oils and hair, and contamination and damage from animal or insect infestation.
- Projectiles—May include tangible objects in motion and powered objects. Examples are meteorites, falling objects, cars, trucks, bullets, rockets, explosions, and wind.
- Movement—Typically involves collapse, shearing, shaking, vibration, liquefaction, flows, waves, separation, and landslides. Examples are dropping or shaking fragile equipment, earthquakes, lava flows, sea waves, and adhesive failures.
- Energy anomalies—Include electrical surges or failure, magnetism, static electricity, aging circuitry, sound, light, radio, microwave, and electromagnetic waves. Examples include electrical utility failures, proximity to magnets and electromagnets, carpet static, decomposition of electrical circuits, cosmic radiation, and explosions.
- Radiological—Includes ionizing radiation, nuclear blasts, and electromagnetic pulses. Examples include exposure to radioactive material and X rays.
- Information related—Includes jamming of signals, social engineering, impersonation, exploits, and denial of service.

Regardless of how the threats to data, property, or well-being are classified, identifying the source of a potential risk remains key to mitigating the risk.

Balanced Approach to Design

It is critical to understand that a security program consists of four independent components or mitigation techniques:

- 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 (CPTED) 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 a specialized area under InfoSec.

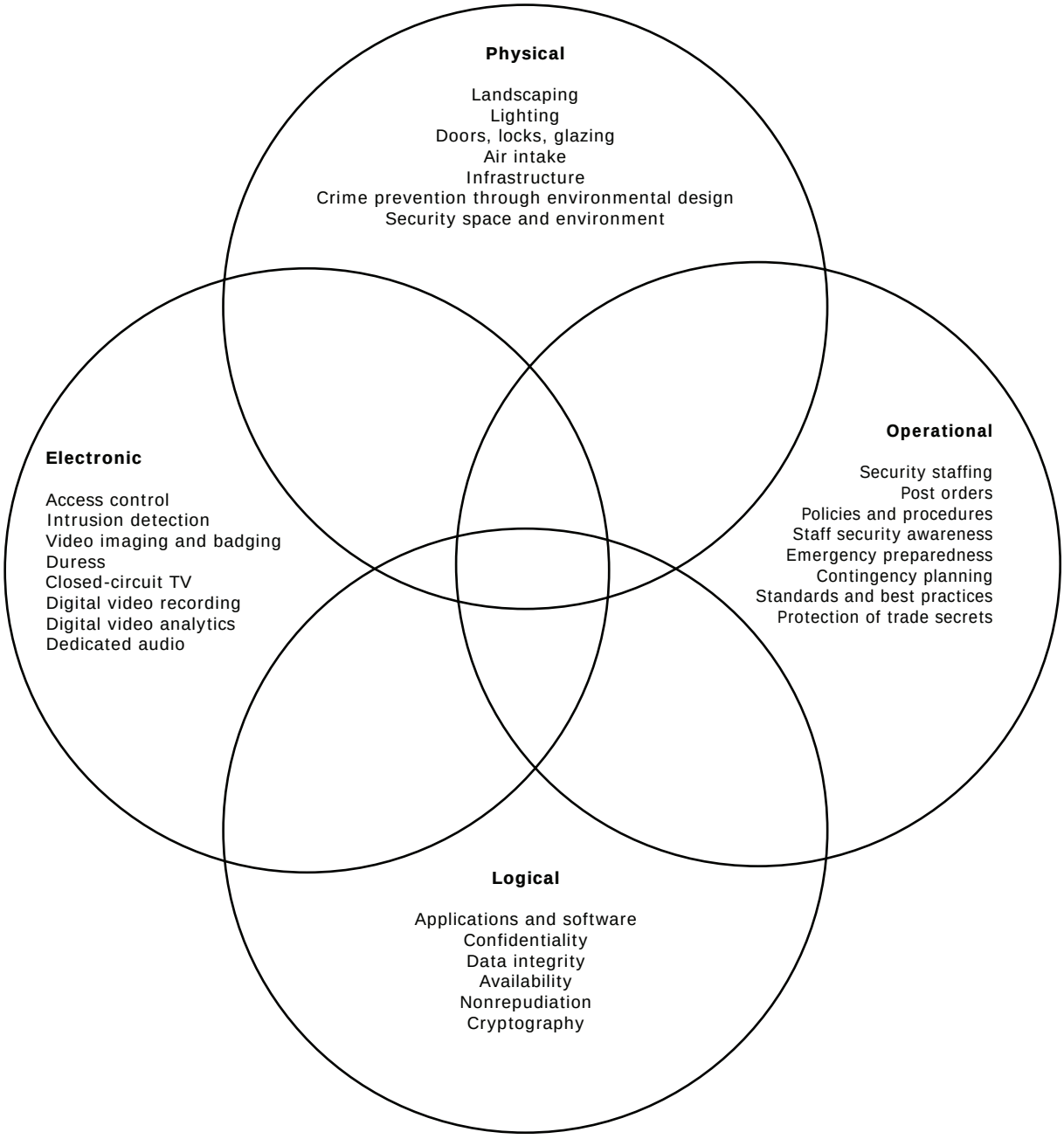
 © 2012 BICSI®

Balanced Approach to Design, continued

Through a balance of these four elements, higher levels of security can be achieved while reducing overall capital and operational costs. These components can work independently or in conjunction with one another.

The four elements of any security program, along with examples of applications, are shown in Figure 2.3.

Figure 2.3
Elements of a security program

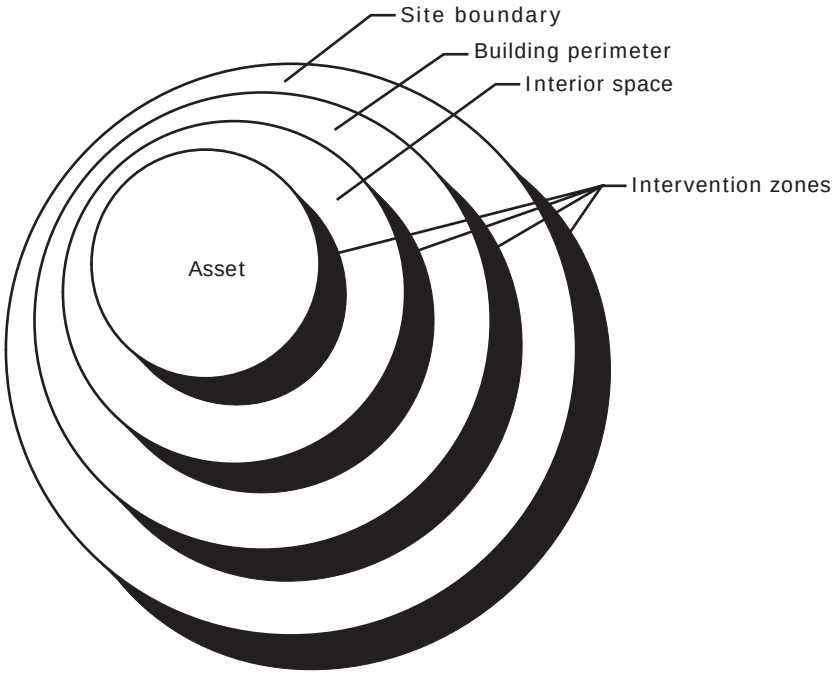


Layering

As seen in Figure 2.4, a fundamental concept when designing a security program is the use of layering. The general consensus within the security industry's best practices is that security countermeasures are simply a means to deter, delay, and detect violations (e.g., there are no impenetrable sites or zero fault tolerant technologies). As such, the theory of concentric circles illustrates that utilizing multiple points of detection provides the greatest opportunity for evaluation and response.

This can be achieved by implementing multiple perimeters beginning at the farthest most site boundary, moving inward to the building perimeter, and finally tightening around the most critical assets. Another solution that meets this requirement is the use of multiple technologies or features to mitigate a single vulnerability.

Figure 2.4
Layering



 © 2012 BICSI®

Security Design and Implementation Practitioners

Overview

It is important to define the roles or steps involved in the design and implementation of an ESS system. The four primary security roles are:

- Consultant.
- Designer.
- Installer.
- Integrator.

Each role is representative of a progressive step in the development and implementation of an ESS system design. All of these roles can be performed by a single individual or a series of different individuals. However, if one individual assumes multiple roles, the distinct functions of each step are still important and should be carefully developed.

Security Consultant

Role

The security consultant is the first role in the development of an ESS system. The consultant must start by considering the asset to be protected. The value and environment of the asset must be determined. The value can provide an indication of the extent of the amount of protection required. The environment defines any challenges to protection.

The consultant identifies and documents threats and risks. A proposal is then prepared that details the appropriate security measures needed to protect a specific valuable asset in a specific environment. The consultant requires the ability to gather data about an area, structure, business, or individual and to develop a protection plan. The consultant is responsible for providing the designer with a comprehensive analysis of the site and making appropriate recommendations for the safety and security of the asset.

Profile

Security consultants come from a variety of backgrounds (e.g., military, law enforcement, forensic, private security). As the need for specialized security consultants rises, more colleges and universities are providing security curriculums. This need has led to the growth of private training firms that specialize in generalized and specific training for security consultants.

Several professional credentials are available (e.g., Certified Protection Professional [CPP™], Certified Information Systems Security Professional [CISSP™]) .

Security Consultant, continued

The security consultant must have competency in:

- Emergency planning.
- Investigation.
- Personnel security.
- Physical security.
- Protection of sensitive information.
- Security management.
- Loss prevention.
- Legal aspects of security.

Security Designer

Role

The security designer is the second step or design role. The designer must evaluate the consultant's documentation and recommendations to formulate an ESS system design.

The designer's experience and knowledge of available systems will lead to a design that is consistent with the asset value and environment and will result in the selection of appropriate physical, electronic, and operational countermeasures.

The designer may be involved in many different levels of the building design and construction. A designer's work may become part of the construction documents or independent scope of work (SoW), or it may be input directly to a field installer and integrator as part of a design or build project.

NOTE: Refer to Chapter 3: Electronic Safety and Security Design Process for more detailed information on an SoW.

The designer and consultant roles may overlap and are often shared by a single professional. Both must understand the motivations and methods of the intruder or perpetrator and the defined risk.

Profile

Profiling a security designer can be difficult. Because of the technical knowledge required, many designers begin their career as an installer or integrator. Hardware and software advances in the electronic security field are constant. Staying current with product knowledge and function is vital to the success of any designer. Without the latest techniques and equipment, a designer cannot offer the most efficient and reliable systems available to the consumer.

Examples of professional security designer credentials are the BICSI® ESS Designer™ and ASIS International Professional (PSP®).

 © 2012 BICSI®

Security Installer

Role

The security installer's role is to deliver the system that meets the requirements of the design.

Profile

The security installer must understand the design and intent of the system. The installer must train to an approved and certified standard to obtain the experience necessary to become a craftsperson. The training may include licensing that is required by the authority having jurisdiction and certification that is required by the manufacturer.

Systems Integrator

Role

An integrator is a practitioner who can assemble many different components to work together as an operational system. Integrated systems can increase value and functionality.

Examples of systems integration include:

- Lighting system activation upon security code entry.
- Heating, ventilating, and air conditioning activation or deactivation, depending on the building occupancy.
- Egress control based on inputs from a fire alarm control panel.

Profile

An integrator must not only thoroughly understand the security system but also have a working knowledge of other systems to be integrated. For two or more systems to share the same database, they must have some form of compatible communication.



Chapter 3
Electronic Safety and Security Design Process

Chapter 3 discusses the architecture and engineering design process and incorporates electronic safety and security (ESS) design considerations into the process.

Table of Contents

Electronic Safety and Security (ESS) Design Process. 3-1
Introduction 3-1
Architecture and Engineering (A&E) Design Process 3-2
Overview 3-2
Team 3-2
Types of Projects. 3-3
Working Environment 3-3
Design Process 3-4
Schematic Design (SD) 3-5
Overview 3-5
Project Functional Requirements 3-5
Preliminary Design Documents 3-6
Threat Assessment. 3-6
Site Survey and Assessment 3-8
Client Interview 3-9
Design Elements 3-12
Design Team Coordination. 3-12
Scope of Work 3-13
Title 3-13
General Statement 3-13
Objective (Narrative) 3-13
Specific Tasks 3-14
Reporting Requirements 3-16
Qualification Requirements 3-16
Place and Period of Performance 3-16
Construction Management. 3-16
Restrictions 3-17
Security Clearances 3-17
Contracting Representative 3-17
Attachments 3-17
Assumptions 3-17
Preliminary Cost Estimate 3-18
Documentation 3-18

Design Development (DD) 3-19
Overview 3-19
Drawings 3-20
Design Coordination 3-23
Design Development (DD) Deliverables 3-24
Design Verification 3-24
Cost Projection 3-25
Final Acceptance 3-25

Construction Document (CD) 3-26
Overview 3-26
Final Specifications 3-27
Electronic Safety and Security (ESS) Final Design 3-31
Preparation for Bid 3-31

Bidding Phase 3-32
Bidding Process 3-32
Substitution Requests 3-32
Review of Responses and Recommendations 3-33
Negotiation with Vendors 3-34
Roles of the Design and Construction Team Members 3-35
Client 3-35
Architect, Engineer, Consultant, and Electronic Safety and Security (ESS) Designer 3-35
Construction Manager (CM) 3-35
General Contractor (GC), Contractor, and Subcontractor 3-35
Bid versus Request for Proposal (RFP) 3-35
Low Bid versus Negotiated Bid 3-35
Types of Contracts 3-36
Design Bid Build 3-36
Design Build 3-37
Integrated Project Delivery (IPD) 3-38
Meetings 3-39
Pre-Bid Meeting 3-39
Bid Opening 3-39
Pre-Award Meeting 3-39
Bid Documents 3-39

 © 2012 BICSI®

Construction Phase 3-41
Overview 3-41
Construction Administration (CA) 3-41
Construction Submittals 3-41
Review Design Implementation 3-42
Request for Information (RFI) Process 3-42
Roles of the Design and Construction Team 3-43
Client 3-43
Architect, Engineer, Consultant, and Electronic Safety and Security (ESS) Designer 3-43
Construction Manager (CM) 3-43
General Contractor (GC) and Subcontractor 3-43
General Contractor (GC) versus Construction Manager (CM) 3-43
Forms 3-44
Submittals 3-44
Meetings 3-45
Job Start Meeting 3-45
Facility Review 3-45
Weekly Project Meetings 3-45
Site Safety Meetings 3-45

Postconstruction Phase 3-46
Overview 3-46
Roles of the Design and Construction Team 3-46
Client 3-46
Architect 3-46
Engineer, Consultant, and Electronic Safety and Security (ESS) Designer 3-46
Construction Manager (CM) 3-47
Contractors and Subcontractors 3-47
Computer-Aided Facility Management (CAFM) 3-47
Drawings 3-47
Manuals of Operation 3-47
Databases 3-47
Web (Internet and Intranet) 3-48

Figures

Figure 3.1 Design process 3-4
Figure 3.2 Design bid build contract 3-36
Figure 3.3 Design build contract 3-37

Tables

Table 3.1 Drawing set systems 3-21
Table 3.2 *SectionFormat*™ outline 3-28

 © 2012 BICSI®

Electronic Safety and Security (ESS) Design Process

Introduction

The project design process starts with general ideas and a conceptual design of what is going to be accomplished. These ideas are refined as the design proceeds through several design steps or stages that continue to define and refine the ideas to specific project requirements. This process may be simple or elaborate depending on the complexity of the project.

This chapter explores the architecture and engineering (A&E) design process and incorporates electronic safety and security (ESS) design considerations into the following stages of design and construction:

- Schematic design (SD)
- Design development (DD)
- Construction document (CD)
- Bidding phase
- Construction phase
- Postconstruction phase

Architecture and Engineering (A&E) Design Process

Overview

This section of the chapter is intended to describe the A&E design process by outlining the various types of contractual relationships and the roles and interactions of team members during the various design processes.

The design of ESS systems must follow a sound methodical process. This chapter provides information and an overview of the design process accepted throughout the industry.

In addition to this manual, the ESS designer should refer to other publications and sources such as:

- BICSI's *Telecommunications Distribution Methods Manual*.
- The Construction Specifications Institute's (CSI's):
  - *The Project Resource Manual—CSI Manual of Practice* (*PRM*).
  - *Master Format*™.
- ASIS International's (ASIS) *Protection of Assets Manual*.
- The United States (U.S.) National CAD Standard® (NCS).
- The U.S. General Services Administration building information modeling (BIM) library.

Team

The ESS designer is part of a design team. A successful project can be attained only if all the members work together with a clear focus on the project goals. A design team must agree on the basic project goals before determining a strategy. Other team members may not understand security goals and may inadvertently compromise the overall security of the building or its occupants.

Each team member has individual responsibilities and expertise that can be utilized to encourage the overall safety and security of the building's occupants. One example of this cross-disciplinary contribution is a landscape architect adjusting the landscaping plan to optimize camera views. The ESS designer also might be able to incorporate a different card reader or camera that better matches the exterior design aesthetic. Any team that works together in such a manner is more likely to accomplish the project's goals.

 © 2012 BICSI®

Types of Projects

The traditional types of projects that the ESS designer may encounter include:

- New construction—There is no existing infrastructure or existing spaces to work with. This project type offers the best opportunity to introduce new systems, technology, and design initiatives.
- Existing construction—Infrastructure and spaces exist, but they can be challenging when trying to deploy new systems and technology into existing spaces.
- Remodel—Significant changes to the infrastructure and spaces are to occur that may present an opportunity to coordinate the deployment of new electronic security systems and technology.

Working Environment

A project team can range from small to large. The team can be a stand-alone consultant or a large multilevel architect/engineer/contractor (AEC), construction manager (CM), and client team. The project environment will determine how the ESS designer works with others and the associated responsibilities, scope, and risks. The ESS designer must establish the authority structure and its responsibilities in either a contract or a scope of work (SoW).

These details will define the ESS designer's influence and legal risk not only in the successful completion of the project but, more importantly, in the ongoing satisfactory and secure operation of the project's entity.

NOTE: Refer to Appendix B: Legal Aspects of Electronic Safety and Security Design for additional information.

It is important to remember that designed systems will impact the client's business processes long after the project is completed.

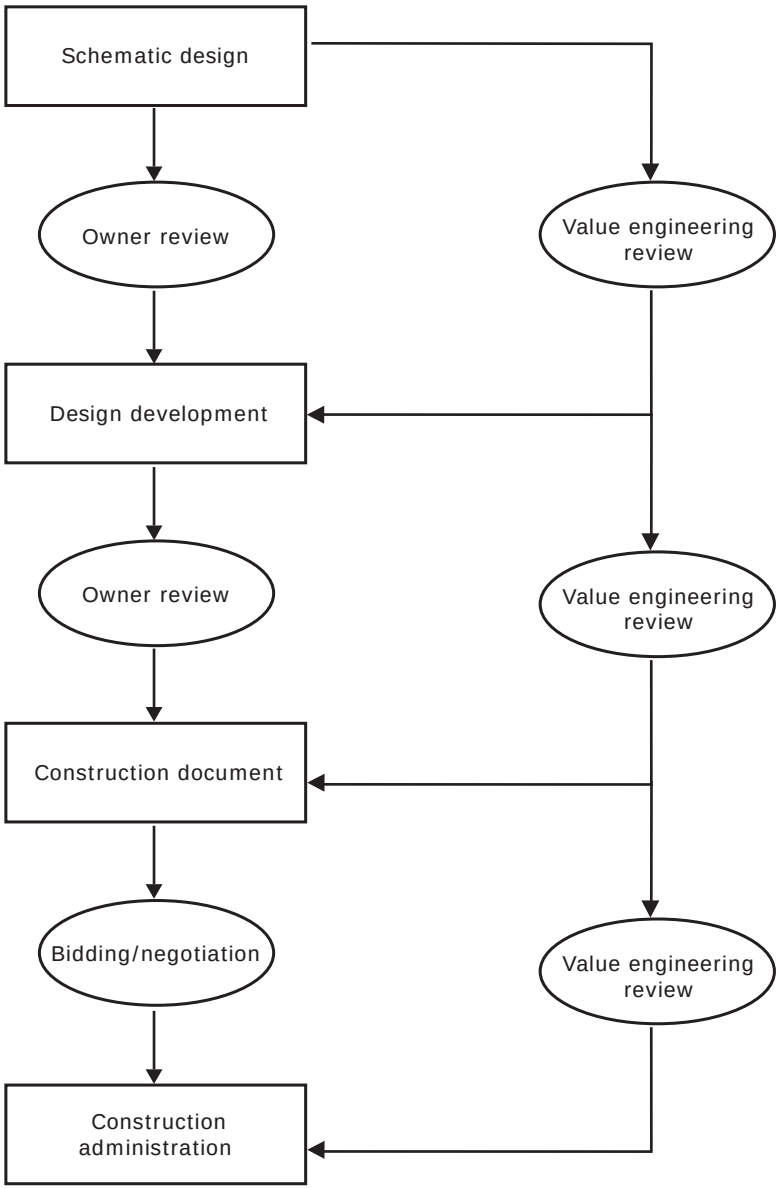
An ESS designer may have sole design responsibility for an ESS project without the expertise of an architect, engineer, or other professional. Regardless of the working environment, the ESS designer must know and execute, where applicable, the design process of the larger team, that of the AEC, CM, and client. Therefore, the remainder of this section will focus on the larger team.

Design Process

A project passes from the client's conception to utilization over a period of time and by means of different activities. The methodology used to successfully accomplish the project could be selected from various accepted procedures. However, the construction industry has utilized various forms of the SD, DD, and CD processes described in this chapter (see Figure 3.1).

NOTE: Any of these phases may be combined or further segmented dependent upon the schedule and scale of a particular project.

Figure 3.1
Design process



 © 2012 BICSI®

Schematic Design (SD)

Overview

The SD is the conceptual and budgetary portion of the process. In this phase, the project lead interfaces with the client to review, analyze, and evaluate the concept of the project. This involves examining the basis for the project, the business processes to be accomplished in the space, the amount of space required, and the resource requirements, all within a sustainable financial constraint.

The project architect often will determine the space programming for the client's consideration by means of:

- Sketches.
- Rough and generalized floor plans.
- Elevation or vertical surface concepts with sections or details.
- Written and pictorial descriptions of solutions for the client's needs and budget.

The project architect typically will involve the entire team for a coordinated holistic design approach. It is important that the ESS designer becomes involved by at least this stage. Since functional and budgetary aspects of a project are significantly impacted by ESS systems, this discipline should be integrated into the SD process.

Project Functional Requirements

The following define some project issues:

- Site surveys—Risk assessment and site surveys may need to be done to better understand the client's operations and assist the ESS designer in determining the overall design. As described in the next section on Preliminary Design Documents, these surveys may have been completed prior to beginning the design.
- Workflow—The ESS designer must understand the workflow and schedule of the architect's SD and the client's requirements as interpreted by the design team. The architect may have made preliminary workflow paths and equipment space requirements within the facility. The spaces identified for ESS equipment need to be confirmed by the designer.
- Security—The ESS designer may provide information that would support and reflect the architect's space planning design. The security issues raised should include not only those with respect to outside individuals and objects but also those of visitors and staff. The review process also includes an evaluation of traffic flow and security issues related to the architectural design.
- Requirements—The ESS designer should discuss the required codes and standards with respect to what spaces and processes must be monitored or controlled with the design team. Documentation records, such as a summary of conferences, must be maintained on all items discussed.
- Feature sets—The ESS designer will observe particular system features either desired or rejected. It is important to define and limit these items and understand the basis for them. The ESS designer often will have to understand an expression and interpret it to an actual deliverable feature set.
- Design philosophy—The ESS designer should have a documented basis of design (BOD), which may include sketches and other supporting information.

Preliminary Design Documents

Preliminary design documents are prepared by a professional consultant or organization for the ESS designer to use as a benchmark for designing the overall ESS solution.

Prior to beginning the design, the following information is gathered from the stakeholders to determine the design criteria:

- Threat and vulnerability assessment
- Site survey and assessment
- Client interview that outlines concept of operation and standard operating procedure of the proposed system

This information is presented to the client or its representative and is used by the ESS designer as a guideline for the overall design process.

Preliminary design documents must be prepared to conceptually describe the manner in which the ESS system will achieve the following processes:

- Deter
- Detect
- Delay
- Decide
- Act

Threat Assessment

This chapter is not intended to provide adequate training, instruction, or knowledge on how to perform a security threat assessment. However, the building owner, operator, security manager, human resources department, insurance carrier, and ESS designer must understand the threat of potential risks to the project and determine a reasonable and appropriate security plan to manage those risks. Armed with this knowledge, the ESS designer should design the security system to minimize those risks identified to the facility.

To effectively secure any personal or intellectual property, building, facility, campus, or other physical location, a qualified security consultant or practitioner must perform a complete threat or risk assessment. The assessment report should be a comprehensive evaluation of the site that includes an assessment of the access to the facility, site, and interior lighting; landscape design; utilities accessing the facility; and assets that if destroyed or compromised could severely impact the operation of the business in question.

There are three basic elements to a threat assessment:

- Identifying potential threats
- Analyzing risks associated with the threats
- Determining which risks and occurrences are permissible and which require prevention

 © 2012 BICSI®

Preliminary Design Documents, continued

A security threat assessment takes into account many factors that together compose the overall security requirements for the facility. This threat assessment preparation does not constitute the design of an access control or other security system, but it is an overall assessment and recommendation for countermeasures that are necessary to protect life and property and mitigate risks.

A threat assessment includes:

- Understanding the organization's mission and security objectives, including the:
  - Nature of the business that will be conducted at the facility.
  - Object of protection.
  - Need for egress control.
  - Type of roadway access to the site (public and private).
  - Type of facility ownership (public, private, or combined).
  - Customers served by the facility.
  - Facility's functional departmentalization.
  - Hours of operation.
  - Facility users.
  - High-value assets.
  - Protection of assets inside and outside the facility.
  - Protection of intellectual property.
  - Risk of criminality and terrorism.
- Determining the organization's and the facility's vulnerabilities, including the:
  - Events that most likely would occur.
  - Comparison between common and worst-case scenarios.
  - Customer demographics.
  - Location of buildings.
  - History of security and crime issues.
- Assessing the physical facility, including the:
  - Site landscape design.
  - Traffic and parking design.
  - Exterior and interior lighting.
  - Stairwell design.
  - Entrance design.
  - Exit design.

Preliminary Design Documents, continued

Threat assessments should be prepared by trained and certified security consultants or practitioners. The ESS designer should prepare a design based upon the review of the security threat assessments and suggest available technologies to meet the specified design criteria. If a threat assessment has not been performed for the facility, it is recommended that the ESS designer be an active participant in the process to allow the ESS designer to better understand the security consultant's areas of concerns and rationale on the mitigation strategies recommended.

Site Survey and Assessment

One of the more important aspects of the design process is a thorough understanding of the environment for which the ESS is being designed. The site survey or assessment provides the ESS designer with critical, firsthand data upon which to base the design.

A well-documented survey is an important step in developing a good system design and well-planned installation. The survey should be meticulous and complete, gathering as much relevant information as possible that will impact the design.

When conducting a survey, the following should be thoroughly addressed:

- Equipment location—Clearly identify the location of all sensors, control panels, cameras, detectors, annunciators, monitors, strobes, and sirens. Forms of this documentation include sketches and recorded notes.
- Policies—Prior to performing any site survey, the ESS designer should confirm with the client any policies or procedures that may impact the method of documentation and areas accessed such as safety training required to access the client's site.
- Photographs—When possible and authorized, take photographs or video recordings of areas in the facility that may offer some difficulty in system design (e.g., perimeter areas) where various detection device solutions may have to be considered.
- Lighting—The lighting at certain sensor locations should be documented if system functionality at low-light levels is required. During the design process, consideration should be given to the level of lighting available for cameras placed outdoors. The absence of light will impact the kind of cameras specified and the subsequent images recorded.
- Trees and shrubs—The effectiveness of cameras and other detection devices (e.g., microwave, infrared) can be severely impacted by the presence of trees and tall shrubs. Trees not only will prevent cameras from providing clear images but also can create false alarms on sensors that reduce the reliability of the system.
- Existing systems—Identify the location of all existing systems along with any equipment that may be defective or inoperable. If rack mounted, include the location in the rack, manufacturer, make, model number, and current software revision. If the design requires the integration of new and existing systems, ensure that all systems can be seamlessly integrated. This may require, among other considerations, the design of a special interface, additional power supplies, and additional cabling.

 © 2012 BICSI®

Preliminary Design Documents, continued

- Critical assets—Identify the exact location of all critical assets of the client. This includes all assets that would be essential for the operation of their business (e.g., telecommunications rooms [TR], research labs, computer operation center, cash transaction areas). Assets may be provided with increased level of security, including:
  - Doors that are always locked and require an authorized card, code, or personal identification number (PIN) to enter.
  - Cameras that start recording once a door is opened.
  - Doors that sound an alarm once they are opened.
  - Doors that sound an alarm once they are opened beyond a certain time limit.
  - Doors that require an audit trail of all entry and exit through them.
  - Areas that should be protected during specific times with limited access to only designated personnel.
  - Areas that require special levels of entry (e.g., two different card reads before a door can be opened).
  - Stationary assets that may require special sensors for protection.

Client Interview

An interview with the client or its appointed representative should be conducted prior to the design of any ESS system. During this interview, the following points should be discussed to understand the needs of the client and its organization:

- Categories of security concern—Address burglary/intrusion, fire, personal safety, surveillance, access control, environmental, or other concerns.
- Existing systems—Inquire about existing systems with regard to their use, familiarity, likes, and dislikes. This will be used as the basis for future design.
- Type of facility—Inquire about the type of facility. Certain facilities are governed by strict security guidelines that may have an impact on their operation (e.g., hospitals, government facilities). If specific regulations and standards apply to these facilities, they must be reviewed and used as the basis for design.
- Specific customer requirements—Discuss all special requirements that may be requested by the client. This could include the needs of physically challenged employees or special security requirements for a particular area.
- Location of facility—The location of the facility sometimes will dictate the system design with regard to equipment use and placement. A facility located in a remote, desolate location will require a different level of security than one located in the center of a city in close proximity to major roadways and busy intersections.

Preliminary Design Documents, continued

- Corporate cultures—Security systems can clash with corporate cultures; therefore, it is important that during the client interview the culture of the organization is discussed and clearly understood by the ESS designer. A system design that does not address the culture of an organization may fail regardless of its functional capability.
- Command, control, and administration—Where and how the systems will be controlled and administered will determine the communication pathway to be designed. The design for a facility that will control and administer its system from the same site will require little or no remote signal transmission while a client that needs to control and administer several facilities from multiple locations might require a dedicated network pathway or transmission on an existing network to meet the level of control and security required.

Additionally, the interview with the client should include the following:

- Discuss applicable codes, standards, and regulations.
- Provide guidance from the ESS designer into both the process and the ESS systems enabling or controlling the process. A good procedure is to do a "day in the life of" exercise. This will reveal the client's desired workflow, the equipment and space impact on that flow, and how the ESS systems could control, monitor, and indicate status of the processes.
- Verify previously received information, and expand the knowledge and wisdom attained. Sometimes information is filtered, and an important detail is not developed, which could impact the ESS design. One of the first verifications is to list the authority having jurisdiction (AHJ) for each discipline that may impact a business. The client knows best these compliance issue agencies or standards.
- Consider entities that can have life safety influences on a facility. In addition to a local building inspector and the fire inspector controlling the design's feature set and ultimately allowing or disallowing the utilization of the space, a number of other entities can have life safety influences on a facility. For example, in hospitals, state and national standards and agencies are continual, daily influencers (e.g., Office of Statewide Health Planning and Development [OSHPD] in California, The Joint Commission, state boards of health that must approve an opening, Healthcare Insurance Portability and Accountability Act [HIPAA], homeland defense standards that establish or restrict equipment location and utilization).
- Exercise existing and desired security model. If the entity is an existing operation, it is advisable to study the processes that have been in use. If the operations are based on company policies and procedures, be sure to obtain a copy for the project file. If the project is for a new facility, one must exercise the required, desired, and visualized processes and anticipate a design that will fulfill and comply.

 © 2012 BICSI®

Preliminary Design Documents, continued

- Validate existing and desired feature sets at the user level. If allowed, this interaction and observation of the client's operations and staff will produce a wealth of information and attitudes, which will be helpful and cautionary in carrying out a design. Also, conduct interviews with the security personnel. There will be times when a design must be changed because of a small detail from the actual or prospective users.
- Review existing methods, materials, and procedures. There are at least five goals to attain when interviewing and observing the client and staff in their facility:
  - Suitable—What features and functions are working or could work? What are their strengths and weaknesses? What needs do these features meet? Why do they meet the needs?
  - Desired—What features and functions would enhance the work space and the client's care or attitude? What efficiencies could occur? Why would this be an improvement?
  - Requested—What features and functions should remain or not be changed? Why is it important that these elements remain? What changes are necessary and why? How would these requested features and functions interact with other functions in the immediate space and the operation as a whole? What positive experiences has staff had with similar features?
  - Rejected—What features and functions should be deleted or changed? What possible features should not be introduced and why? What negative experiences has staff had with similar features? What negative operational or compliance issues have been involved with these features? What negative impact have these features had on adjacent or organization-wide operations?
  - Compliant—How do they comply with policies, procedures, and known standards? What features and functions have been experienced as noncompliant or marginally so?
- Discuss initial concepts. Conduct guided discussions of the options and opportunities with both the AEC and the client's staff. This also provides an opportunity to consider what features, functions, and basic operational principles are advised and acceptable. Make sure that individuals understand that to arrive at a proper and complete design that is consistent with the budget, different design decisions may be made other than those discussed.
- Always follow up with a summary of conference reports to confirm the design direction.

The ESS designer must design systems to meet the owner's business practices as well as all local codes and ordinances.

Preliminary Design Documents, continued

Design Elements

The review of the project's functional requirements and the client interview form the basis, rationale, and feature sets of the SD for the security systems. It should include not only the systems, functions, and outcomes but also the goals to be attained for the client's business processes. It also should indicate compliance areas and items of concern.

The SD should address:

- Discussion topics.
- Standards.
- Regulatory compliance.
- Best practices.
- Client-provided design criteria.

The SD should be submitted to the AEC and client team.

The ESS designer should review current security technologies, technology literature, and manufacturers' current offerings to stay current with the industry. Construction of a facility can have long lead times (design, approvals, fabrication, and acceptance), possibly resulting in the systems designed utilizing today's technology being obsolete by the time the client utilizes the systems. Any system design should consider a migration path to emerging technologies and feature sets.

The SD should identify the general installation methods and materials for the basic system configuration. This will form the basis for documenting the design in the CDs as well as being a part of the presentation to the AEC and client team. This should include a one-line drawing of the system (an interconnected assembly of symbols that illustrates the system components in a functional way), floor plans showing general physical placements of equipment, and special considerations that any member of the AEC team would need for coordination.

A listing of system features should be included in a narrative that accompanies any drawings. This narrative will describe the business process and technology deliverables for the client's operations.

Design Team Coordination

The ESS designer, as a member of the design team, must invest time in the design process to review the work of other disciplines.

During the SD phase, this coordination may include:

- Reviewing the work of the architect and other disciplines, usually not coordinated, and considered to be an SD.
- Reviewing and commenting on available work products to ensure their suitability and workflow with the design intent of the ESS system.
- Participating in the coordination meetings with the intent of reducing the total DD time and efforts by identifying deficiencies that will require redesign earlier in the process.

 © 2012 BICSI®

Scope of Work

An SoW is a document developed by either a client or a client/designer collaborative team for defining the project requirements. A well-defined SoW is important for a successful project.

The critical elements of an SoW include:

- Title.
- General statement.
- Objective.
- Specific tasks.
- Reporting requirements.
- Qualification requirements.
- Place and period of performance.
- Construction management.
- Restrictions.
- Security clearance requirements.
- Contracting representative.
- Attachments.
- Assumptions.

This section outlines the major elements of a well-defined SoW.

Title

The title can be important if an organization has multiple solicitations each year. Some procurement agencies choose to assign a number to each solicitation with the year embedded in the number to help with identification (e.g., 0012012).

General Statement

The general statement is a brief description of the overall project. An example of a general statement is, “Provide video surveillance cameras at building 02.”

General statements may lengthen and become more comprehensive as the size and scope of the project increases.

Objective (Narrative)

The objective is a description of the overall project. For example, “Cameras shall be provided on the roof of building 02 at the entrance and exits of the Elm Street parking garage.”

Scope of Work, continued

Specific Tasks

Identify each specific task that should be completed under an SoW. Examples of important details that should be included in the specific tasks section of the SoW are discussed below.

Type of Camera

The ESS designer should specify the type of cameras furnished:

- Analog pan, tilt, and zoom (PTZ)
- Internet protocol (IP) mini-dome
- Infrared
- Thermal imaging

Type of Mount

The specific type of mount to be installed should be included:

- Parapet
- Pole
- Wall
- Corner

Pathway

The ESS designer should identify the pathway carrying the cables. Some considerations for ESS pathways include:

- Type and size of conduit required.
- Conduit pathway to align with device placements.
- Separate conduits for power and control/video signals.

Type of Cables

The ESS designer should identify the type and quantity of cables that need to be installed:

- Coaxial cable
- Twisted-pair cable
- Optical fiber cable

Associated Hardware and Material Required

Associated hardware includes cabling hardware and connecting hardware. Details for associated hardware should be listed in the material lists. Any special requirements for these items may be included in the descriptions.

 © 2012 BICSI®

Scope of Work, continued

Bonding and Grounding (Earthing) Requirements

The ESS designer should identify any lightning and surge protection requirements. Identify points of bonding to ground.

Permit Requirements

The ESS designer should identify any permits that need to be obtained. Depending on the jurisdiction, some permits can take a substantial amount of time to process.

Insurance Requirements

Identify any specific insurance requirements:

- Name the owner and ESS consultant as additional insured on the contractor's general liability policy.
- Minimum umbrella policy coverage.
- Workers compensation insurance.
- The contractor indemnifies the owner for hazardous materials brought to the site by the contractor and handled negligently.

Code and Standard Requirements

The ESS designer should identify the codes and standards to which the project must conform (e.g., UL 2044, *Standard for Commercial Closed-Circuit Television Equipment*).

Testing Requirements

The ESS designer should identify and document the type of testing that will be required to meet the design requirements.

Documentation Requirements

The ESS designer should identify the deliverables that are required before and after project completion, including the:

- Safety plan (before project start).
- List of materials (before project start).
- Drawings (postproject).
- View from each camera at various lighting conditions (postproject).
- Test procedures for all installed ESS devices and systems (postproject).
- Hard and soft copies of test results (postproject).
- Documentation for system warranty requirements (postproject).

Include a statement that if the submittal schedule is not provided promptly after the contract is awarded, the contractor forfeits the right to additional money or time based on the time required for the ESS designer's review of the submittals.

Scope of Work, continued

Reporting Requirements

The ESS designer should identify what deliverables are due to the client during the course of the project. Some examples include:

- Progress reports.
- Project schedule.
- Audits.
- Safety reports.

Qualification Requirements

The ESS designer should identify any licenses, registrations, or certifications that a bidder must have as a minimum requirement for bidding on the project.

Examples of licenses or certifications include:

- Master electrician license.
- Security contractor license.
- BICSI Registered Communications Distribution Designer (RCDD®).
- ESS Designer.
- BICSI Information Technology Systems (ITS) Technician credential.

The owner has the right of approval over the selection of a superintendent.

Place and Period of Performance

The place of performance indicates the locations where the installation will be performed. This also is indicated on the construction drawings. The security contractor must comply with any owner safety programs in the place of performance.

The period of performance indicates both the first day and the final day of the contract. Additionally, the hours of operation during which the work can be completed by the security contractor are identified. This also should be included in the project management documents.

Construction Management

The ESS designer should determine whether an on-site CM is required for the project. The ESS designer should indicate whether there are any special or minimum requirements for the CM (e.g., 10 years of experience, managing projects over $5 million, RCDD, ESS).

 © 2012 BICSI®

Scope of Work, continued

Restrictions

The ESS designer should identify any special restrictions that might be relevant to the job, including:

- Schedules.
- Environmental restrictions.
- Prevailing wages (Davis-Bacon Act).
- Governmental restrictions.

Security Clearances

Some government and commercial work may require a variety of security clearances. The ESS designer should identify the scope of the security for the project and delineate in the project plan how the requirements will be handled.

Contracting Representative

The ESS designer should identify who will be the client's authorized representative to make contractual decisions for the project. The name, office or agency, address, telephone and fax number, and e-mail address of the client's representative should be included.

Attachments

The ESS designer should list any attachments that are included in the SoW, including the:

- Schedule.
- Wage determinations.
- Construction drawings.

Assumptions

The ESS designer should identify any project-specific assumptions that are required, including the following:

- All asbestos will be abated before installation can begin.
- Secure, environmentally controlled space will be provided to store materials.

Preliminary Cost Estimate

During the SD of the security systems, the ESS designer may prepare a preliminary cost estimate of the systems. This is crucial since it includes the potential costs of the security systems in the budgets related to the total project.

A preliminary cost estimate will require:

- Identification of the systems included in the design.
- An investigation of the coverage areas of the systems.
- A general enumeration of the quantity and quality of the devices needed.

Actual locations of devices at this stage of design may be difficult. However, some determination of the magnitude and range of devices to be deployed and the effect of the devices on centralized equipment is needed. The ESS designer may estimate principal field device quantities by marking the potential device locations, routes, and pathways on the architect's drawings. This will assist in estimating the number of each type of device, structured cabling requirements, and labor impact.

The preliminary cost estimate should include the estimated central equipment and field devices as well as any scalability issues related to the centralized equipment that may affect costs. The estimate should be based on project information and data known at this time during the design along with the experience of the ESS designer with similar systems and projects.

The preliminary cost estimate should:

- Be reasonable.
- Be slightly conservative.
- Include a contingency.
- Have assumptions identified upon which the cost estimate is based.

The ESS designer should provide a level of confidence in the cost estimates. The preliminary cost estimate should avoid costs per square foot or square meter since ESS systems do not scale well for utilizing an area-based estimating of costs. As most systems are sized incrementally, a change in the architect's design could have a dramatic impact on both the design and costs for implementation.

Documentation

The ESS designer should produce a set of drawings and written documents for use in the architect's SD submission. This may include:

- Typical device floor plan drawings—The drawings should include the initial markup of the architect's backgrounds (e.g., floor plans, any applicable riser or sectional drawings). Although the drawings are preliminary, the locations indicate the interaction of the ESS systems with the business processes, staff, and client environment. The drawings also should indicate secure and nonsecure areas to better understand traffic flow.
- Narrative system description—The ESS designer should prepare a generalized performance description of the ESS systems that can serve as the basis for the specifications or request for proposals (RFPs).

 © 2012 BICSI®

Design Development (DD)

Overview

The DD stage of a project design follows the review of the SD with the AEC, CM, and client team. This often will involve significant interaction with every responsible person and user group in the client's organization. There is a potential for changes to occur as the result of input from all participating parties.

Information received from the client and other members of the design team will modify the ESS systems to align with the desired operational and business processes.

The DD phase is a technical phase of the design process and occurs when many of the issues of how the ESS systems must operate and interface with other systems are defined, redefined, and concluded.

Documents created during the DD phase may include:

- Detailed documentation of the design process (e.g., refined project development guide [PDG]).
- Drawings.
- Outline specifications.
- Proposed schedule.
- Draft bid/procurement documents.

The DD phase is where critical decisions are made by the team to develop a complete list of design criteria.

Drawings

Project drawings or construction drawings of the ESS systems will become part of the contract documents. The ESS designer shall utilize the client's design standards, if available. If no client standards are available, there is an industry standard for numbering the drawings that utilizes the NCS. The NCS incorporates the following publications:

- National Institute of Building Sciences (NIBS) Plotting Guidelines
- American Institute of Architects (AIA) CAD Layer Guidelines
- CSI's Uniform Drawing System (UDS™)

The architect usually assigns the drawing set's numbering system. The usual method is to group it by AET discipline (A for architectural, E for electrical, T for telecommunications) as described in the NCS. It is also industry standard to provide a letter suffix to the sheets (e.g., EP for electrical power, TA for audiovisual, TY for security).

The drawings are further enumerated by drawing types (e.g., plans, elevations, sections, details). The *PRM* describes some organization systems (see Table 3.1). The placement of the ESS drawings in the complete set should be discussed with the architect.

NOTE: Tables 3.1 and 3.2 are reprinted with permission from McGraw-Hill. Both tables were taken from CSI's *PRM 5th edition*, copyright 2004, published by McGraw-Hill.

 © 2012 BICSI®

Drawings, continued

Table 3.1
Drawing set systems

Uniformat™	National CAD Standard
A Substructure	G General
A10 Foundations	H Hazardous materials
A20 Basement construction	V Survey/mapping
	B Geotechnical
B Shell	W Civil works
B10 Superstructure	C Civil
B20 Exterior enclosure	L Landscape
B30 Roofing	S Structural
	A Architectural
C Interiors	I Interiors
C10 Interior construction	Q Equipment
C20 Stairs	F Fire protection
C30 Interior finishes	P Plumbing
	D Process
D Services	M Mechanical
D10 Conveying	E Electrical
D20 Plumbing	T Telecommunications
D30 HVAC	R Resource
D40 Fire protection	X Other disciplines
D50 Electrical	Z Contractor/shop drawings
	O Operations
E Equipment and furnishings	
E10 Equipment	
E20 Furnishings	
F Special construction and demolition	
F10 Special construction	
F20 Selective demolition	
G Building site work	
G10 Site preparation	
G20 Site improvements	
G30 Site civil/mechanical utilities	
G40 Site electrical utilities	
G90 Other site construction	
Z General	
Z10 General requirements	
Z20 Contingencies	

CAD = Computer-aided design
HVAC = Heating, ventilating, and air conditioning

Drawings, continued

At the DD level, preliminary drawings of the ESS systems should be developed and completed. This includes construction details as well as notes, schedules, or matrices of device deployment and interaction.

The ESS designer will need to draw device symbols at precise locations to provide the required services or functions. The drawings should utilize a layering feature of a computer-aided design (CAD) system for different systems. A format for layer names is also listed in the NCS.

After device locations are drawn on the architectural backgrounds (the architect's CAD drawings that display the details of a space), the ESS designer should count the device for use in refining the cost estimate. Infrastructure components (e.g., structured cabling, mountings, pathways) also should be included in the drawings.

The DD drawings for the ESS systems should identify:

- Cable routes.
- Capacities.
- Methods.
- Infrastructure requirements.

A typical package might consist of sheets depicting device placement, basic one-line drawings showing device connectivity, details of device mountings, pathway requirements, and a legend sheet with abbreviations and definitions.

NOTE: The above descriptions provide detailed information regarding the process by which the ESS designer will develop drawings using popular CAD software packages. The ESS designer should be aware of newer technology that is called BIM. This software technology utilizes a database-centric virtual model for the representation of design decisions and has a broad impact on the processes followed by an ESS designer to communicate the design information of an ESS. The descriptions of phase and content remain unchanged regardless of the software platform utilized within a project.

 © 2012 BICSI®

Drawings, continued

The ESS designer should prepare specifications or RFPs with detailed requirements in compliance with the CSI MasterFormat or other standard as described by the project team. The specifications are documents that state detailed requirements as to products, methods, and outcomes.

Specifications have three parts:

- Part 1 is general and lists the authority and responsibility, summary and description of the project, and all referenced documents and codes.
- Part 2 is products. ESS designers write the section based on performance and avoid propietary equipment.
- Part 3 is execution and describes the installation quality, testing and commissioning, training, and warranty.

The ESS designer also may prepare an executive summary of the DD for the client's consideration and approval. This document will assist the client in understanding how the details of the design have been addressed.

The ESS designer may coordinate with some manufacturers, vendors, or contractors to ensure that the design will function as desired. It is important that the ESS system requirements are realistic and constructible and will not result in unexpected additional costs.

Design Coordination

In developing the ESS design, the ESS designer must coordinate with all the team members affected by the ESS system and with the client. This includes drawing and equipment schedule coordination. Since there is usually a limited amount of space for infrastructure in a facility, the coordination of the AEC team is important. This includes not only the devices and their functional or physical locations but also the pathways and infrastructure.

The ESS designer should coordinate with other trades regarding items such as ductwork, electrical pathways, sprinkler heads, and lights. The standards of all applicable organizations must be adhered to strictly. Incorporation in the project of such standards must be effectively communicated to the AEC team members.

Coordination of the path of egress with door hardware is essential.

The ESS designer also must ensure that the DD documents comply with the agreement with the AEC or client. The DD documents are considered a deliverable of services, and as such, the submission of DD document files to the architect should include a transmittal letter and request acceptance of the documents.

Design Development (DD) Deliverables

The ESS designer should present the following to the client:

- Updated system narrative or PDG
- Design drawings (e.g., floor plans, details, partial plans)

The ESS DD documents should contain additional information that will explain the features, functions, and business process security issues for the education of the AEC and the client.

The ESS designer should discuss the business operational processes and compliance and reveal any issues, assumptions, decision metric, and budget impacts. These steps will help ensure the validity of the design as well as the importance of the ESS designer's work product and its completeness. This educational effort also should help to maintain the integrity of the design.

The educational documents should be formally acknowledged to indicate both an understanding and acceptance of the design by the AEC and client team. Additional tasks or changes may be requested and may require a change in the ESS designer's SoW or contract.

Design Verification

The ESS designer should ensure that the design is not only biddable and constructible but that it is also achievable by getting acceptance from likely manufacturers. This is one of the prime differences between documents produced as a specification and an RFP. An RFP may include an SoW and a description stating what is needed and desired.

A contractor or vendor responding to the RFP will offer a system identifying, in detail, where the system meets, exceeds, or fails to comply with the expressed needs. However, in a specification, one must write an SoW that is attainable by a manufacturer. The manufacturer may be required to write or modify software or produce modifications to an existing product.

A design that is not achievable may result in a no bid by all contractors or vendors, thereby putting the project at risk. The ESS designer should ensure that there are no potential cost overruns or unforeseen issues driven by scalability or feature set details.

 © 2012 BICSI®

Cost Projection

At the DD level, a complete cost projection may be submitted with the documents. The level of detail submitted will assist all team members in evaluating and discussing the entire project budget.

The schedule of values included in the budget will be used by the architect and client to guide the construction of the facility design. The AEC, CM, or client may submit a preliminary DD to an outside estimating service to determine a realistic projected cost for the project design.

The ESS designer may be required to apply value engineering (VE) to the ESS design because of budget concerns. VE is reengineering to change the design of a project to align better with the client's budget. The previously presented deliverables should form a basis for the AEC and client teams in the evaluation of proposed changes that may have a negative impact on the design. The integrity of the ESS systems must be maintained during the VE process.

When the VE process is followed, it is important to recognize the interaction of three elements of a design: cost, schedule and quality. It is difficult to achieve ideal levels in all three of these elements. The ESS designer should work closely with the owner and other members of the design team to reach the optimum balance among them.

Final Acceptance

The ESS designer will integrate any requested or required changes to the drawings and specifications or RFPs and prepare the documents for publication.

The appropriate quantities and forms of DD documents should be printed and transmitted to the architect or client with a letter of transmittal. The formal submission and acceptance are important to record for both the alignment of the project milestones and the ESS designer's contract.

A DD submission should incorporate all of the needs of the client in coordination with the architectural backgrounds. Care should be taken to be as accurate as possible. In design build projects, a DD is sometimes used for bid purposes or procurement of long lead items.

Construction Document (CD)

Overview

CDs are a complete set of project documents produced by the entire AEC team. CDs include at least the following elements:

- Specifications
- Contract drawings

Completed CDs form the entire project description, defining not only the quality and process, but also the legal context for the contractors.

The reduction of errors and omissions within the CDs will significantly benefit the construction activities. The ESS designer should produce a complete, accurate set of CDs that clearly convey the design intent and scope of the project.

The development of CDs is accomplished through the refinement of the DD documents, incorporation of all the comments and requirements, and coordination with other members of the design team to reach the final set of CDs.

As the ESS designer works to complete the design, the following items should be considered for addition to the CDs:

- Installation details
- Material schedules
- Configuration and programming information
- Quality requirements

It is not uncommon for the client's financial controller to request an updated cost projection with the objective of confirming the project is within budget. In the event the project's anticipated costs of construction are beyond the financial means of the client, VE options may be requested for consideration.

Available choices for consideration may include:

- Reducing the scope.
- Phasing the project over a period of time.
- Reducing the quality of products or workmanship required.

The ESS designer needs to attend all VE meetings where the ESS design will be discussed to ensure that the integrity of the design is not compromised by VE decisions. Minutes from VE meetings discussing other construction areas need to be reviewed by the ESS designer to ensure that any decisions will not externally affect the design.

 © 2012 BICSI®

Final Specifications

The ESS designer must finalize the specifications along with completing the contract drawings. Utilizing CSI's *MasterFormat* divisions, the ESS designer should write detailed specifications that describe the complete system requirements. The majority of the ESS designer's work will involve Division 28—Electronic Safety and Security.

Possible sections include the following:

- 280000 (Electronic Safety and Security)
  - 280600 (Schedules for Electronic Safety and Security)
  - 280800 (Commissioning of Electronic Safety and Security)
- 281000 (Electronic Access Control and Intrusion Detection)
  - 281300 (Access Control)
  - 281600 (Intrusion Detection)
- 282000 (Electronic Surveillance)
  - 282300 (Video Surveillance)
- 283000 (Electronic Detection and Alarm)
  - 283100 (Fire Detection and Alarm)
- 284000 (Electronic Monitoring and Control)
  - 284600 (Electronic Detention Monitoring and Control Systems)

The specifications should be organized in accordance with CSI's three-part *SectionFormat*™ outline (see Table 3.2) and formatted in a logical hierarchy for the presentation of information. The *SectionFormat* includes the following categories:

- Part 1—General
- Part 2—Products
- Part 3—Execution

Final Specifications, continued

Table 3.2
SectionFormat™ outline

Part 1 General	Part 2 Products	Part 3 Execution
Summary Section includes: Products supplied but not installed under this section, products installed but not supplied under this section, allowances, unit prices, measurement procedures, payment procedures, alternates	Manufacturers	Installers
References	Existing products	Examination Site verification of conditions
Definitions	Materials	Preparation Protection, surface, preparation
System description Design requirements, performance requirements	Manufactured units	Erection
Submittals Product data, shop drawings, samples, quality assurance/ control submittals (design data, test reports, certificates, manufacturers' instructions, manufacturers' field reports), closeout submittals	Equipment	Installation
Quality assurance Qualifications, regulatory requirements, certifications, field samples, mock-ups, preinstallation meetings	Components	Application

 © 2012 BICSI®

Final Specifications, continued

Table 3.2, continued
SectionFormat™ outline

Part 1 General	Part 2 Products	Part 3 Execution
Delivery, storage, and handling Packing, shipping, handling, and unloading, acceptance at site, storage and protection	Accessories	Construction Special techniques, interface with other work, sequences of operation, site tolerances
Project site conditions Project/site environmental requirements, existing conditions	Mixes	Repair/restoration
Sequencing	Fabrication Shop assembly, fabrication tolerances	Reinstallation
Scheduling	Finishes Shop printing, shop finishing	Field quality control Site tests, inspection, manufacturers' field services
Warranty Special warranty	Source quality control Tests, inspection, verification of performance	Adjusting
System startup		Cleaning
Owner's instructions		Demonstration
Commissioning		Protection
Maintenance Extra materials, maintenance service		Schedules

Final Specifications, continued

As the final CD is an integrated set of information for all disciplines, the ESS designer shall review other related divisions within the specifications manual.

Possible CSI divisions where the ESS systems' specifications could have interface include the following:

- Division 00—Procurement and Contracting Requirements
- Division 01—General Requirements
- Division 08—Openings
- Division 21—Fire Suppression
- Division 23—Heating, Ventilating, and Air Conditioning
- Division 25—Integrated Automation
- Division 26—Electrical
- Division 27—Communications
- Division 28—Electronic Safety and Security

The ESS designer is responsible for ensuring that the information is presented in the correct location within the specification manual, regardless of the division.

It is not uncommon for the ESS designer to have information that should be included in other divisions. This information may include pertinent content areas that are not covered within the ESS system's specification sections.

The architect and other members of the design team may lack the expertise or access to the information to be included. These items must be written by the ESS designer and inserted into the appropriate sections. The ESS designer should negotiate with the architect or specification writer to include them in the appropriate section.

The ESS designer should make written suggestions to the architect for inclusion in the contract bid documents. An omission of these items in the procurement requirements or contracting requirements final bid forms should generate questions during the bidding cycle.

 © 2012 BICSI®

Electronic Safety and Security (ESS) Final Design

The ESS designer should ensure completeness of the documents. A complete bottom-up review of all drawings and specifications should be accomplished prior to completion. It is advisable that peers review the documents to ensure that details and assumptions are explicit.

The ESS designer should coordinate with other specialties and consultants. As a project nears publication of the CDs, each member of the AEC must ensure that the design elements within their portion of the package coordinate and have few conflicts with other team members. The ESS designer should properly affix seals, statements, and AHJ required items to the documents. If AHJs have requirements for professional engineer (PE) seals, compliance statements, or other items to be affixed to the drawings, it is critical that they be properly and timely inscribed.

If the ESS designer must submit the work product to another entity for these items, adequate time must be included prior to publication deadlines for proper review and action, including the ESS designer's corrective action. Some AHJs have required a single engineer of record to stamp all documents, even those produced by an ESS designer who is a registered PE.

Preparation for Bid

The ESS designer should prepare the following bidding documents for use by the AEC or CM or for inclusion in the CD package or RFP:

- Provide a schedule of values or spreadsheet for use by the architect in formatting the required response items.
- Clearly state the options, alternates, and add or deduct items that are described in the ESS designer's sections for inclusion in the architect's bid forms.
- The fee for the set of bidding documents and bid and performance bonds are normally included by the architect. However, if the ESS designer is preparing the CDs or RFPs, these items should be included by the ESS designer to protect the client's project.
- Prepare a transmittal letter to the AEC, CM, or client describing the required pre-bid meeting, preapproval of systems, bid submissions, and formats.

These items are an important part of assuring that the complex requirements of the ESS are adequately and fairly communicated to possible responders. Expressing these requirements to the AEC, CM, or client attempts not only to reserve the process in their scheduling but also to state the importance of such requirements. If the requirements are stated only within the context of the CD, they could be overlooked.

Bidding Phase

Bidding Process

The ESS designer should observe the contractual requirements regarding dates for questions from potential bidders and answers to the questions. The ESS designer must maintain the requirements (deadlines and format) stated in the documents for contractors and vendors asking for information or clarifications. Commitment to deadlines is important in maintaining a fair and accurate process.

The ESS designer should answer questions completely to increase the validity of the responses. The ESS designer should not ignore submitted questions or the questioner's intent. If there is a failure to communicate, the ESS designer should revise the content.

The ESS designer should ensure that every vendor and bidder receives all communications and provides an affirmative response on the bid form and bidder's liability:

- It is critical that adequate records be maintained on plan holders to ensure that all questions and answers are transmitted to each.
- When using e-mail, be sure to turn on the return receipt requested and retain the returned documentation.
- The answers should be published to all plan holders and pre-bid meeting attendees as an addendum to the bid documents.
- The explicit statement of responsibility and liability to the content of the questions and answers as well as any other addendums issued must be on the bid forms. Responders must state that they have received the bid documents and that their responses reflect all addendums published in an actual listing.

Substitution Requests

The ESS designer should ensure that the stated process is maintained. Adequate time must be available and utilized to thoroughly examine the submittals of contractors and vendors.

The ESS designer should evaluate substitutions according to client's needs and design conformance while being open to valid options. While the ESS designer may have published the design with specific products or feature sets in mind, the ESS designer is ethically bound to thoroughly investigate submissions based on the specifications.

Several statements are utilized to express the design's openness to products. When "equal to" or "better than" is used, the ESS designer must review not only the actual product compliance with the design but also its effect upon system integration and other systems that may require interface or interaction.

The ESS designer should publish all information for every vendor and bidder. When products or manufacturers are allowed for use in a contractor's or vendor's response, such approvals must be published in an addendum for all plan holders and potential bidders.

 © 2012 BICSI®

Review of Responses and Recommendations

The review should include the following:

- Evaluate compliance with the design and specifications. Dependent upon the specifications and bid documents, this can be a short or extensive process and report and indicate:
  - Approvals—If the contractor's or vendor's products and methods are fully compliant with specifications and drawings, the ESS designer should document this and recommend approval or conditions for the issuance of a contract.
  - Required changes—If the contractor's or vendor's products or methods are not fully compliant or there are issues, the ESS designer should document that in detail and recommend required changes prior to the issuance of a contract. The submittal also can be approved as noted.
  - Rejections—If the contractor's or vendor's products or methods are not compliant or there are issues that will result in failure of the design or no integration with other systems, the ESS designer should document this in detail and recommend rejection of the contractor, vendor, or system, thereby barring the issuance of a contract.
- Evaluate bid items, unit pricing, schedule of values, and scalability issues. If the ESS contractor's or vendor's bid items, unit pricing, and schedule of values are available, the ESS designer must examine the documents for compliance with the CD and rationalize the schedule of values. It is important to investigate the impact of scalability issues prior to making final recommendations.
- Present results and recommendations for action by the AEC, CM, or client. The ESS designer's evaluation results and recommendations should be presented in a readily understood format and organized similar to the CD. The recommendations not only must be understandable by non-ESS decision makers but also should be clearly justified and defensible.

Negotiation with Vendors

Dependent upon the nature of the project and the team, the ESS designer may represent the client in negotiating with one or more of the contractors or vendors toward obtaining the most compliant system at the best price.

The negotiation process should include the following:

- Negotiate based on bid evaluations and options. Because of the complexity of ESS, there may be several paths to the best system for the best vendor, cost, and time structure. The various items should be weighted to assist in the evaluation when there are many complex determinants.
- Negotiate VE and system options. Contractors and vendors usually will have discovered less expensive ways of complying with the design intent. These options, as well as the CD-presented bid options, provide opportunities for reducing the cost of the project. The results and recommendations arising from VE or the selection of system options should be clearly described along with both the present and future implications on utilization and costs. The presentation should be available to all stakeholders.
- Negotiate alternates and project changes by the AEC, CM, and client. Prior to the final production of contract agreements and amendments, there may be changes within the project that will impact the ESS. If so, these must be described to and negotiated with the ESS contractor or vendor. It should not be assumed that change impacts would be linear in nature.
- Prepare contract documents for the selected bidder or vendor. If the project is such that the ESS contractor or vendor is to execute the prime contract, the final documents will be extensive. The documents should comply with AIA and CSI references stated in the CD. If the ESS contractor or vendor is a subcontractor, explicit statements should be included in the general contracts that will adequately describe the changes agreed to in the CD and the contractor's or vendor's response.

 © 2012 BICSI®

Roles of the Design and Construction Team Members

Client

The client typically supplies the bidding and contracting requirements to be included in the project manual. The client often coordinates advertising or sending invitations to prospective bidders.

Architect, Engineer, Consultant, and Electronic Safety and Security (ESS) Designer

The design team produces any addenda required to clarify the contract documents. The design team also may participate during the evaluation or negotiation of the bids and help the client determine the successful bidder by considering alternates and substitutions.

Construction Manager (CM)

Depending on the nature of the project, the CM may lead or participate during the bidding process and the evaluation of the bids to help the client determine the successful bidder.

General Contractor (GC), Contractor, and Subcontractor

The general contractor (GC) and other contractors prepare and submit their bids to the client. Subcontractors prepare and submit their pricing to the GC or other contractors.

Bid versus Request for Proposal (RFP)

When a contractor responds to a bid, the requirements are usually clearly defined with drawings and specifications. An RFP is often written more loosely and leaves much of the solution in the hands of the responding contractors.

Low Bid versus Negotiated Bid

Publicly funded projects and some private projects require that the lowest qualified and responsive bidder be awarded the work. Additionally, in some countries (e.g., United States), bidding laws often may require the mechanical, plumbing, and electrical portions of the work to be bid and contracted separately from the general construction contract. This is called a multiple prime bid.

Most privately funded projects are awarded to a contractor based on a negotiated bid amount. After the bids are received, the client selects a contractor and begins negotiations. A contract is then executed.

Types of Contracts

Three types of contracts are described below:

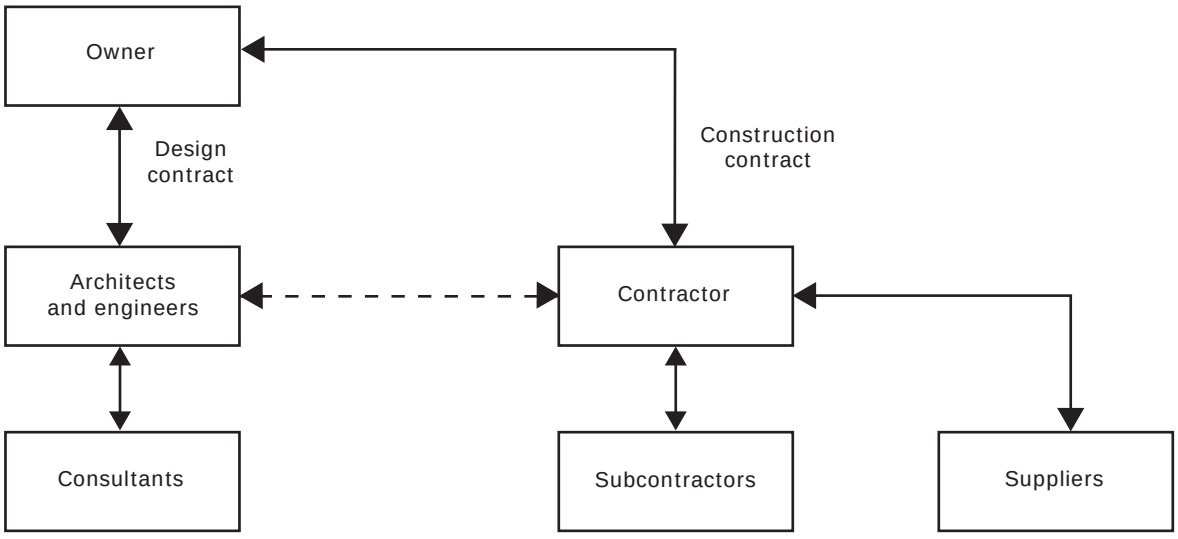
- Stipulated sum—A contractor submits a fixed price for the SoW required. Most low-bid contracts are stipulated sum contracts; however, a stipulated sum contract also can be the result of negotiations between the client and the contractor.
- Cost plus fee—A contractor is reimbursed for actual costs plus a fee. To establish the absolute maximum price of the project for the client, the contractor or CM may be required to state a guaranteed maximum price (GMP). With this form of contract, there can be a shared savings clause or incentives for early completion. This form of contract often leads to VE that can generate savings during the construction phase of the building. However, these savings can return as onetime or recurring expenses during the operation, maintenance, or repair of the building.
- Unit price—The unit price is used when the actual SoW cannot be determined at the time of the bid. The key to obtaining effective bids is to provide a realistic estimate of the quantities for a given type of activity.

Design Bid Build

A design bid build contract is a project delivery method in which the client contracts with separate entities for the design and construction of the project (see Figure 3.2).

Typically, a design team will have a contract to design the project and produce a set of bid documents. The client will declare the selection criteria for contract award to the successful bidder. Contractors are invited to submit their bids for review and disposition. The client selects a contractor from the bidding contractors.

Figure 3.2
Design bid build contract



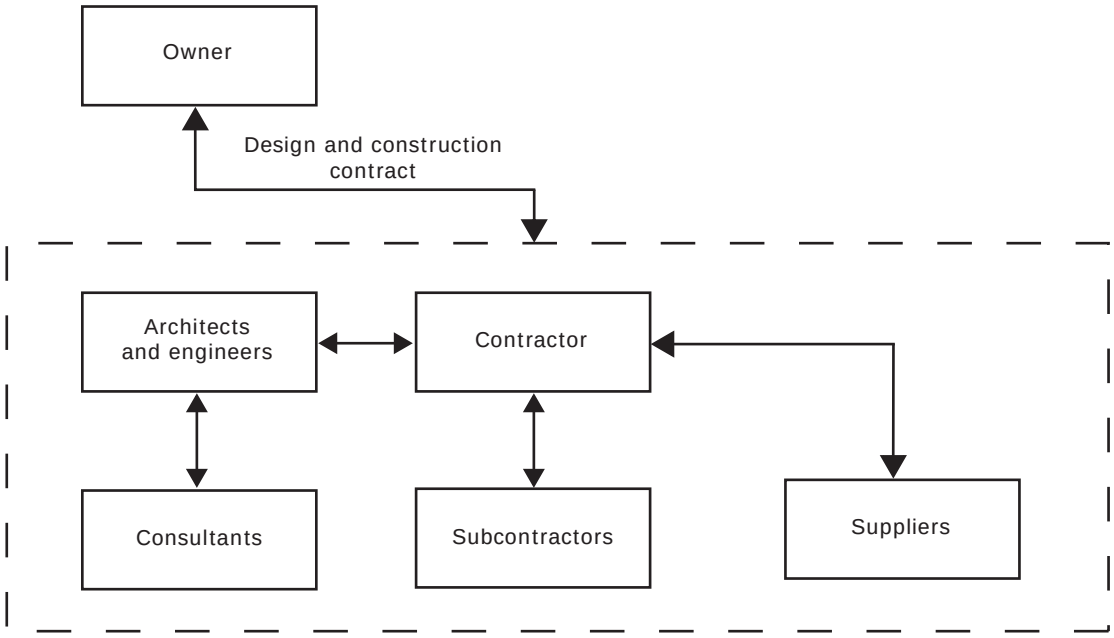
 © 2012 BICSI®

Types of Contracts, continued

Design Build

A design build contract is a project delivery method in which one entity is employed by a client to both design and build a project. This entity is referred to as the prime contractor. The structure of the team will vary by project and depends upon the desires of the prime contract holder as well as the needs of the client (see Figure 3.3).

Figure 3.3
Design build contract



Integrated Project Delivery (IPD)

Integrated project delivery (IPD) is a collaborative alliance of people, systems, business structures, and practices into a process that harnesses the talents and insights of all participants to optimize project results, increase value to the owner, reduce waste, and maximize efficiency through all phases of design, fabrication, and construction.

Difficulties in contemporary construction include buildings that are behind schedule and over budget as well as possible contentious relations among the owner, GC, and architect.

The focus in IPD is the final value created for the owner: the finished building. Rather than participants focusing exclusively on their part of construction without considering the implications on the whole process, the IPD method brings all participants together early with collaborative incentives to maximize value for the owner. This collaborative approach allows informed decision making early in the project where the most value can be created.

There are sequential phases to the integrated project delivery method:

- Conceptualization (e.g., expanded programming)
- Criteria design (e.g., expanded SD)
- Detailed design (e.g., expanded DD)
- Implementation documents (e.g., CDs)
- Agency review/permitting
- Buyout
- Construction
- Closeout
- Facilities management

 © 2012 BICSI®

Meetings

Pre-Bid Meeting

Typically, this meeting is facilitated by the lead ESS designer and is attended by all interested bidders and client representatives. The pre-bid meeting is used to review the contract documents, bidding procedures, project schedule, and site conditions and to answer questions from the bidders.

NOTE: This meeting may be mandatory for a contractor's bid to be considered responsive.

Bid Opening

The bid opening may be a public or private meeting at which the bid responses are opened and the results tallied.

Pre-Award Meeting

The pre-award meeting can be used to interview the lowest qualified contractor before awarding a contract to confirm that the contractor understands the CDs and project expectations.

Bid Documents

The consultant or contractor must be familiar with all elements in the bid documents. This awareness minimizes the possibility of creating discrepancies between front-end documents and other division specifications.

The following is a partial listing of the front-end sections of the project manual:

- Bid solicitation:
  - Brief overview of the scope
  - Where bidding documents can be reviewed or obtained
  - Bid security requirements
  - Bid due date, time, and location
- Instructions to bidders:
  - Type of bid
  - How to prepare the bid
  - Bid security
  - Bonds and certificates
  - Permits
  - Wage rate schedule
  - Subcontractor listings
  - Pre-bid meeting requirements
  - Information related to the opening of the bids
  - Schedule of alternates and unit prices

Bid Documents, continued

- Information available to bidders:
  - Existing conditions
  - Hazardous materials
  - Description of the site and buildings
- Bid response forms:
  - Project identification
  - To whom the bid is directed
  - Who submitted the bid
  - Acknowledgments
  - Length of time that bids are valid
  - Acknowledgment of addenda
  - Pricing
  - Start and completion dates
  - Signature and date of the bid
- Contract forms
- General conditions and supplementary conditions
- Specifications:
  - Procurement and contract requirements
  - Common requirements
  - Site construction
  - Common construction
  - Facility construction
  - Equipment
  - Facility services construction
  - Infrastructure construction
  - Process construction
- Drawings:
  - Device locations
  - Installation details
  - Block diagrams
  - Connectivity diagrams
  - Riser diagrams
  - Equipment and device schedules

 © 2012 BICSI®

Construction Phase

Overview

Once the agreements are executed between the client and the contractors, the planning and scheduling begins. Contractor mobilization and materials purchasing occur at the beginning of this phase of the project. Submittals, shop drawings, modifications, and record documents are produced. At the end of this phase, punch lists (e.g., documents that summarize corrections a contractor must make prior to work being accepted as complete) and substantial completion surveys and documents are prepared.

Construction Administration (CA)

Construction Submittals

The ability of the ESS designer to ensure that the project is completed in compliance with the design is largely dependent upon the quality of the construction submittals. This can and should be enforced via contractual requirements.

Construction submittals consist of shop drawings, cutsheets, and installation details that demonstrate the vendor's or contractor's detailed plans to deploy the systems as described in the CD. The submittal drawings will always show more detail than the CD. These drawings may also contain information on the coordination of the vendor's or contractor's products with other systems.

The cutsheets or catalog sheets contain the product data and should provide the manufacturer's details and sufficient information to ensure compliance with the CD, including interoperability with other systems as described in the CD.

The submittals should contain installation details, including interdependencies with other work. These installation details provide valuable information in determining or creating the following:

- Compliance with the design and contract
- VE if the project is over budget or scaled back
- Schedule of values as required by the contract or the client's needs
- Redesign fee

Construction Administration (CA), continued

Review Design Implementation

Review the design implementation for the following:

- Coordination—The ESS designer should be involved in the early coordination and implementation planning of a project. Proper coordination will reveal the probable conflicts of systems or specialties. Such issues not addressed early among all affected parties will become costly, impacting both the budget and timing. Failure to properly coordinate can result in risks to the project.
- Changes—Changes are inevitable. If the changes are due to inadequate design, the project and ESS designer are at risk in budget, timing, and costs. Change order (CO) requests have been a profit center of some vendors and contractors. When a CO request is received by the AEC, project manager (PM), and GC team, it must be quickly and completely addressed and documented. Design teams have been judged by the number of COs processed. If a CO cost increase or decrease is issued, it must be agreed to by all affected parties and documented. Work may be delayed, redone, or litigated because of inadequate CO processing.
- Progress payments—The ESS designer may be part of documenting and approving progress payments to the vendor or contractor. A detailed schedule of values is useful in determining the amount to be paid for a quantifiable amount of work. It is important that a vendor or contractor is neither underpaid nor overpaid as work is placed into service.
- Percentage of completion—When possible, perform a weekly analysis of the progress of work. This is usually expressed in percent complete. The CD and schedule of value documents should adequately and fairly express progress points.

Request for Information (RFI) Process

During the course of construction, questions from the contractor will arise. The request for information (RFI) process is used to answer those questions. The process will help to confirm a specification or detail on the drawings and provide documented clarification to continue work. It also should help to facilitate communication between the design and construction teams and help the project to be completed on time with approved documentation.

The RFI should be:

- Responded to in a timely fashion so as not to delay the project. The typical response time for an RFI should be one to five working days, but it may vary because of the urgency of the issue, the amount of work required for design, or other circumstances (e.g., AHJ approval).
- Clear and complete in the answers. Include references to drawing numbers and specification sections. Responses also should provide graphic depictions and drawings of the resolution when necessary.

RFI responses should not replace verbal communication between the parties on a project. When it appears that a resolution or suggested resolution of the RFI may adversely impact the schedule or the cost of the work, that fact must be included as part of the RFI communication process.

Unless otherwise noted, the contractor will assume that a response to an RFI constitutes a release for construction.

 © 2012 BICSI®

Roles of the Design and Construction Team

Client

During the construction phase, the client is obligated to make payments to the contractor under the terms of the contract. The client can stop work, complete work the contractor fails to complete, clean the site (if not cleaned by the contractor), and partially occupy the building. The client may also be authorized to terminate the contract without cause.

Architect, Engineer, Consultant, and Electronic Safety and Security (ESS) Designer

The design team's role during construction usually includes inspection and observation of the work with the client's representative, which ensures the work complies with the contract documents. The design team reviews submittals, interprets the contract documents, and modifies the contract documents as required. The design team also may prepare change orders.

Construction Manager (CM)

The CM coordinates construction activities and events and typically is in charge of the construction site with respect to access, safety, and items such as storage of materials. If the contractor has a guaranteed maximum price contract with the client, the CM also may be subcontracting out portions of the project and managing the overall budget. The CM also may issue or manage the change order.

General Contractor (GC) and Subcontractor

The GC's primary role during the construction phase is to complete the work. Some of the contractor's specific responsibilities include:

- Obtaining required permits and licenses.
- Arranging for required tests and inspections.
- Maintaining record documents.
- Preparing submittals.
- Maintaining a clean and safe work environment.
- Overseeing commissioning plan.
- Correcting any work rejected by the client.

General Contractor (GC) versus Construction Manager (CM)

The size and time frame of the project often determine whether a client will hire a CM to manage the construction activities. If a CM is not hired, then the client, GC, or both may assume the coordination activities.

Forms

Numerous forms and documents are used to administer a construction project. In the United States, organizations such as the CSI, AIA, Engineers Joint Contract Documents Committee (EJCDC), and Design-Build Institute of America (DBIA) have developed comprehensive and tightly coordinated documents. Because of this close coordination, many of the forms are standard requirements.

The following is a list of commonly required forms:

- Notice to proceed—Informs the contractor to begin work on a particular date.
- Meeting minutes—Keeps track of the issues raised in meetings, and forms the agenda for subsequent meetings.
- Request for interpretation—Used to obtain a formal response to the contract documents.
- Field order—Used to facilitate minor changes to the requirements that do not require a change order. However, a contractor may submit a change order request in response to a field order.
- Proposal request—Used to solicit a quotation from the contractor for a proposed change to the project scope.
- Change order request—Can be submitted by the contractor in response to a field order or as an uninitiated request for a change in scope.
- Change order—A formal document that defines the required changes in the project scope and identifies associated changes to the time frame, the dollar amounts, or both.
- Punch list—A document that summarizes corrections that a contractor must make prior to the work being accepted as complete.

Submittals

Submittals are required throughout the construction phase of the project. A submittal is essentially any information that a contractor must submit to the design team for review and approval.

Items that the contractor likely will need to submit include:

- Certificates of insurance.
- Surety bonds.
- Lists of subcontractors and products.
- Schedules of activities.
- Commissioning plan.
- Shop drawings.
- Product data.
- Samples.
- Test reports.
- Manuals.
- Project photographs.
- Record/as-built drawings.
- Contractor training certifications and credentials.

 © 2012 BICSI®

Meetings

Job Start Meeting

Before starting the work, the contractor may need to attend a job start meeting to:

- Introduce contractor personnel to other parties involved with this project and other projects being undertaken at the same time.
- Review all requests for facilities by the contractor and subcontractors.
- Review the client's requirements and concerns.
- Permit the ESS designer's contractor to review and interpret the project documents.

Facility Review

The contractor will likely need to conduct a walk-through of all work areas with the client. The contractor will be required to describe specific work methods and proposed schedules. This allows the client or client's representative to identify areas of concern, desired installation, and time lines as well as review important procedural and safety precautions.

Weekly Project Meetings

Throughout the duration of the project, the contractor typically will need to attend a weekly project meeting to review the status of current and planned activities, review the schedule, and conduct other business associated with the project.

Site Safety Meetings

It is a common practice for subcontractors to conduct weekly site safety meetings or, at a minimum, have representation at the GC's weekly on-site safety meeting.

Postconstruction Phase

Overview

Some projects may include a requirement for commissioning. The scope of commissioning can be extensive and is not fully addressed in this overview section. For more complete information regarding commission of the ESS refer to Chapter 12: System Operation and Commissioning.

At a minimum, a commissioning plan should include cutover and first-use activities that begin as soon as construction is complete or nearing completion. Training the client's personnel on the use and adjustments of the installed equipment and warranty inspections occurs during this postconstruction phase.

The operation and maintenance of various systems in the new facility often begin prior to the completion of the construction phase. The as-built version of the drawings that are used to construct the building and prepared from the record copy drawings can be integrated or incorporated into the computer-aided facility management (CAFM) system.

Final payments are usually made, and retainage amounts released well after occupancy once the client is satisfied that the project is fully completed.

Roles of the Design and Construction Team

Client

At this point in the project, the client is accepting responsibility for the operation of the building.

The client's staff is:

- Learning how the newly constructed systems operate.
- Finalizing move-in and first-use activities.

Architect

The architect is involved with final acceptance and contract closeout activities. Final punch lists and reviews of the new facility are being prepared. Record copy drawings are being used to update the as-built documents.

Engineer, Consultant, and Electronic Safety and Security (ESS) Designer

The engineers, consultants, and ESS designers are actively involved with the final punch list reviews, system startup, and testing. System as-built documentation is being prepared from the record copy drawings.

 © 2012 BICSI®

Roles of the Design and Construction Team, continued

Construction Manager (CM)

The CM is involved with final acceptance and contract closeout activities. Final punch lists and reviews of the new facility are being prepared. Final accounting activities are being addressed. At this phase, the CM is accommodating the client's staff on the work site and coordinating the removal of construction equipment, tools, and work trailers.

Contractors and Subcontractors

The contractors are finishing the construction activities and resolving issues identified on the punch lists. Carpet contractors, furniture vendors, painters, site restoration and signage workers, ITS contractors, movers, and other contractors are completing the final installations and activations.

Computer-Aided Facility Management (CAFM)

Drawings

As-built drawings, if needed by the client as a requirement of the design team, should be delivered at the time of occupancy. The drawings should be provided in both electronic and hard-copy formats using the client's master layering scheme.

Most clients realize the benefit of having CDs in an electronic format with the information normalized to the client's layering standards. This allows the information to be easily integrated into the master documentation.

Manuals of Operation

Operation manuals and technical documentation should be provided at the time of occupancy. Manuals are often preferred in electronic format (e.g., compact disc) because they are easier to search and can be integrated and updated with information from the manufacturer's website.

Databases

Complex ITS infrastructures and systems are good candidates for documentation via a database. Many organizations use a range from simple spreadsheets to complex databases to track many facets of a facility. The database requirements should be clearly evaluated and understood at the early stages of the design.

Failure to plan without understanding the facility management requirements can lead to costly manipulation of the information created during a construction project, allowing the manipulated data to be integrated into an existing facility management or ITS management system.

Computer-Aided Facility Management (CAFM), continued

Web (Internet and Intranet)

Web technology via the Internet or an intranet has created new ways to manage modern buildings. Product information and updates, facility drawings, and databases can be accessed easily from a standard browser.

The impact of web technology on how buildings are built, maintained, and managed cannot be underestimated and is limited only by the imagination of the system developer and building managers.

 © 2012 BICSI®



Chapter 4
Access Control Systems

Chapter 4 explores the purpose and application of access control systems (ACS). The various types of systems are discussed with an in-depth review of the hardware and software requirements. Radio frequency identification (RFID) and Internet protocol (IP) integration are included.

Table of Contents

Access Control Systems (ACS) 4-1
Introduction 4-1
Purpose of Access Control 4-1
Authority Having Jurisdiction (AHJ) 4-2
Door Hardware 4-2
Door Closers 4-3
Revolving Doors and Turnstiles 4-3
Areas of Application 4-4
Overview 4-4
Single Structure Sites 4-5
Multiple Structure Sites 4-5
System Structure 4-7
Overview 4-7
Central Equipment Processing (Level 1) 4-8
Server 4-8
Event Recording 4-8
Backup Requirements System 4-9
Computer Hardware 4-9
Software 4-9
Backup Power 4-10
Environmental Conditions 4-10
Space Requirements 4-11
Workstations 4-11
Controllers for Intelligent Field Processing (Level 2) 4-13
Access Controller 4-13
Controller Configurations 4-14
Peripheral Devices (Level 3) 4-15
Request to Exit (REX) 4-15
Door Contacts 4-19
Electrified Door Hardware 4-21
Power Distribution 4-23
Relays 4-29
Metal Oxide Varistor (MOV) 4-30
Fire-Rated Hardware and Doors 4-30
Lock Types, Functions, Grades, and Styles 4-31
Electric Strikes 4-32
Magnetic Locks 4-34

Electric Locksets/Electric Latch 4-36
Electric Bolts 4-37
Control Trim 4-38
Delayed Egress Devices 4-39
Power Transfer Devices 4-40
Door Closers 4-41
Readers 4-45
Credentials (Level 4) 4-46
Radio Frequency Identification (RFID) 4-46
Access Control Cards, Credentials, and Biometrics 4-46
Card Formats 4-51
Biometric Systems in Access Control 4-52
Biometric Performance Parameters 4-57
Privacy and Other Concerns 4-58

Design Considerations 4-59

Access Control Integration 4-59
Occupants 4-59
Assets 4-60
Vehicles and Parking 4-61
Access Level Matrix 4-61
System Failures 4-64
Building Codes 4-65
Notification Requirements 4-65

Communications 4-66

Serial Communications 4-66
Optical Fiber for Extended Distances 4-66
Analog Communications 4-66
Transmission Control Protocol/Internet Protocol (TCP/IP) or Network Communications 4-67
Databases 4-67
Local Database 4-67
Distributed Database 4-68
Integration 4-69

System Programming 4-70

Overview 4-70
Database Conversion/Transportation 4-72
Data Entry 4-73
Report Generation 4-73

 © 2012 BICSI®

System Verification Testing and Startup 4-74

System Training 4-76

Overview 4-76
System Administrators. 4-77
System Operators 4-77
Managers 4-78
Information Technology (IT) Staff 4-78
Maintenance Personnel 4-78
Training Schedules 4-79

Figures

Figure 4.1 Request to exit devices 4-17
Figure 4.2 Electrified exit hardware 4-18
Figure 4.3 Door contacts 4-19
Figure 4.4 Calculation chart 4-24
Figure 4.5 Types of relay configurations 4-29
Figure 4.6 Electric strikes 4-33
Figure 4.7 Magnetic locks 4-35
Figure 4.8 Electric locksets 4-36
Figure 4.9 Electric latch and bolt 4-37
Figure 4.10 Control trim 4-38
Figure 4.11 Delayed egress devices 4-39
Figure 4.12 Door closer hardware 4-41
Figure 4.13 Biometric characteristics 4-52
Figure 4.14 Biometrics in physical access control application 4-54
Figure 4.15 Biometrics in user identification application 4-55
Figure 4.16 Biometrics in logical access control application 4-55
Figure 4.17 Example of access control system floor plan 4-63

Tables

Table 4.1 Circular mils of standard American wire gauge conductors 4-27
Table 4.2 Voltage drop per 30 meter (m [100 feet (ft)]) run of paired wire (61 m [200 ft] total length of wire) 4-28
Table 4.3 Comparing smart card technologies 4-48
Table 4.4 Personal identification biometric systems 4-53
Table 4.5 Sizing for biometric applications 4-56
Table 4.6 Biometric performance parameters 4-57
Table 4.7 Access level matrix 4-62

 © 2012 BICSI®

Access Control Systems (ACS)

Introduction

Access control refers to the proven practice of controlling access to a property, building, or select space within a facility for authorized persons only.

In the early history of access control devices, access was accomplished using simple means and materials. 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.

Access control systems (ACS) determine who is allowed, where they are allowed, and when they are allowed to enter or exit.

Purpose of Access Control

The strategy of access control is to develop a means of regulating access by individuals to specific resources or physical spaces through the use of an item or object (e.g., credential) that possession or knowledge of provides access to a secure space. Access control can be accomplished using multiple techniques that can vary from relatively simple technologies to more advanced integrated electronic systems. Early ACS were mechanical rather than electronic. Some examples, which are still currently in use, are the push buttons on a door lock that require entering some type of combination to unlock the door.

Today, the most common type of ACS incorporates a device requiring the presentation of a badge with encoded information. This access device is often placed near the door. This device reads the information on the card and, based on predetermined decision-making by the ACS, either unlocks the door or refuses to allow passage. Other options that do not require cards include biometric systems that recognize a part of the person (e.g., eyes, fingerprints) or radio frequency identification (RFID) tags that identify objects as they move throughout a facility.

When credential holders present their cards to an access reader, the ACS can display a variety of information on the credential card holder, including the cardholder's name, picture, job title, and other pertinent data. This information can assist security personnel, emergency personnel, and human resources in knowing how many people are present at the facility, where they might be, and when they left.

Purpose of Access Control, continued

The varied uses of ACS have increased from controlling access to sensitive areas to controlling access to a variety of valuable items. Access devices are available that require employees to place their card into a desktop holder to log into the computer system. An access card can be used to check out cameras, sensitive documents, and other resources that may be available at the facility, perhaps in conjunction with an RFID tag system.

College campus environments are utilizing one-card systems that allow a student to access classroom buildings, purchase food and vending items, log into the computer systems, and enter the dormitory.

One of the fastest growing segments of ACS is Internet protocol (IP) devices that utilize a twisted-pair cable to quickly communicate with the central ACS. These devices combine powerful features with less cabling and ease in expanding the system after initial installation.

Authority Having Jurisdiction (AHJ)

When reviewing building codes and standards, an electronic safety and security (ESS) designer should begin with the guidelines adopted by the municipality. The ESS designer should recognize that codes and standards change over time and that the officially adopted edition is considered superior, even if a more recent version is available.

When reviewing codes and standards, the ESS designer should recognize that different levels of occupancy and uses might have different requirements. In case of conflict between codes and standards, the more stringent code or standard prevails. In the end, the authority having jurisdiction (AHJ) determines which code or standard is applicable.

The AHJ is typically a building inspector or fire code enforcement official, but it also may be the building owner or the building's insurance company. The AHJ is generally considered to be an agency or organization rather than an individual.

Door Hardware

To meet legal requirements (e.g., Americans With Disabilities Act [ADA]), handles, pulls, latches, locks, and other operating devices may be required to have a shape that is easy to grasp with one hand and does not require tight grasping, tight pinching, or wrist twisting to operate. Lever-operated mechanisms, push-type mechanisms, and U-shaped handles are acceptable designs. Hardware required for door passage is required to be mounted within accessibility standards.

The ESS designer must coordinate the power and integration requirements of all electrified locking devices to ensure that egress requirements are met. Although the ESS designer is not responsible for selecting door hardware, the ESS designer must have a thorough understanding of door hardware and coordinate the design of the ACS with the door hardware. ACS components interact with electrified door hardware to control access and egress through an entrance and to monitor the status of that entrance portal. Life safety also must be considered.

 © 2012 BICSI®

Door Hardware, continued

Door Closers

Under many AHJ requirements, if a door has a closer, it must be adjusted so that the door takes at least three seconds to move from an open position of 70 degrees to a point 75 millimeters (mm [2.95 inches (in)]) from the latch measured to the leading edge of the door.

Revolving Doors and Turnstiles

To comply with the AHJ and applicable codes (e.g., NFPA 101), revolving doors and turnstiles must not be the only means of passage at an accessible entrance or along an accessible route. For example, an accessible gate or door must be adjacent to the turnstile or revolving door and must be designed to facilitate the same use.

Areas of Application

Overview

ACS are available for every market and building type. Some of the most common applications include:

- ACS for buildings and secure spaces.
- RFID device for inventory and asset tracking.
- Point of sale (POS) with smart chip debit cards.
- Revenue collection systems (e.g., transit fares, electronic toll collection, parking fees).
- Time and attendance.
- Watch tour or guard tour.

Many government facilities require limited access to protected areas of a building or grounds. Based on the importance of the facility's contents and occupants, zones of protection are often created around and within the site perimeter.

Businesses have a number of applications for ACS, including:

- Data centers, computer rooms, and information technology systems (ITS).
- Executive protection.
- Human resources department databases.
- Warehousing operations.
- Research and development facilities.
- High-value storage.
- Sensitive data.

Additional facilities where ACS are used include the following:

- Retail
- Warehousing and distribution
- Seaports and airports
- Financial institutions
- Border crossings
- Commercial
- Health care
- Education
- Transit, highway, and parking systems

 © 2012 BICSI®

Single Structure Sites

One example of a single structure site is a parking garage. ACS could be used in a parking structure to record a time tag of an inbound card for the purpose of billing. Additionally, ACS might be used to control access in certain areas of the parking structure (e.g., reserved parking, private lot).

Residential applications for ACS are increasing and are an example of a single structure. The ACS could be used to restrict access to persons on a needs basis. For example, the babysitter could be provided with access on Friday evening yet would not be able to enter the residence other times during the week.

A manufacturing building is another example of a single structure site. A facility could have ACS at the main entrances and within the building to protect access to the manufacturing floor, data centers, or areas containing sensitive or proprietary information.

With the development of smart card technology, personnel also can utilize the ACS card for other purposes like purchasing food and vending items.

A chemical plant is an example of a large facility with many buildings located on one site. On such a site, a single plant entrance for employees and a separate entrance for construction companies are usually provided. The ACS could be used to generate muster reports in the event of an emergency at the plant. Each building inside the fence line could have ACS to prevent unauthorized people from entering hazardous areas and to protect valuable items and inventory.

Multiple Structure Sites

One example of multiple buildings on one or more sites is a college campus. A college campus may be spread out over many acres and consist of a variety of buildings. A campus may be located on a single site or may have buildings located at many different sites within a community.

Another example of a multiple structure site is the school system for a town, city, county, or region. A large metropolitan school system might have many different buildings (e.g., schools, administration, maintenance, supplies).

In educational facilities, the ACS may be used to limit or prevent intruders from gaining access to students inside the school. This system also may be used to identify visitors using a visitor management system.

Many health care facilities within a given community may include many types of buildings located on a campus or across town instead of in one location. An ACS could be used to provide doctors and nurses access to the hospital and to the neighborhood clinic utilizing the same access credential.

Toll roads and transit systems also can be considered multiple structure sites because entrance and egress points are separated by a significant distance. Tracking these points is key to determining authorized access and calculation and collection of toll and fare revenue.

Multiple Structure Sites, continued

The type of use for a facility often will determine the application of the ACS. Many different uses of the ACS may be found in a typical hospital, including:

- Employee identification.
- Card access control in hospital data centers, employee-only areas, and other sensitive areas.
- Limited access to computer data.
- Pharmaceutical dispensing and tracking.
- Infant abduction prevention systems.

 © 2012 BICSI®

System Structure

Overview

The basic components of an ACS include a computer, one or more control panels, and one or more peripheral devices connected to the control panels (e.g., card reader, siren, sensor, locks, position switch, request to exit [REX] sensor).

The host computer 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 provides the graphical user interface (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 computer-aided design (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 video surveillance systems [VSS]) of the person pushing the intercom button to request entry into the lobby.

One of the many tasks control panels perform is managing the activation of peripheral devices. The activation is managed by turning the devices on or off and controlling access into certain areas through card readers and door-locking hardware.

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.

The ACS may be divided 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)

Central Equipment Processing (Level 1)

Server

The server is primarily where the ACS database resides.

The servers may be in a number of locations, depending on the application. It may be collocated with information technology (IT) servers in a computer room or be a stand-alone computer in an office. The server commonly runs a number of applications that are part of the card access system. The number of applications depends on the size of the installation.

Applications that may run on a server include:

- Badging software.
- Card reporting software.
- Card entry software.

A large server typically runs the database only. The computing power and size of the installation determine the server requirements. Certain applications may require the use of dedicated or multiple servers. The hardware requirements of the server must be in alignment with the recommendations made by the ACS manufacturer.

The server communicates with ACS components through various media. The types of communication the client expects to have in the system determine the number and type of additional communication cards to be installed in the server.

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.

Event Recording

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 include:

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

 © 2012 BICSI®

Central Equipment Processing (Level 1), continued

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

Some examples are:

- Digital tape backup.
- Hard drive.
- Digital versatile disc (DVD) recorded disc.
- Compact disc (CD)-read/read-write (R/RW) disc containing the event data and the appropriate surveillance image, if one is available.

Backup Requirements System

Backup requirements for the ACS are determined by the length of time the information must be made available and the amount of data that is stored. The manufacturer determines the drive size once the amount of data required has been established. Appropriate hard drive space must be provided as part of the machine purchase. The ACS server should provide long-term secure storage.

Computer Hardware

The ESS designer should specify the computer hardware in coordination with the client and the ACS manufacturer. A good practice example would be to install a machine that exceeds 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 monitor type and size also must be determined. The size of the monitor 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.

Software

The ESS designer should be aware that some ACS operate using proprietary software, which may limit their interoperability. License and maintenance fees also must be considered when selecting the ACS platform. Licenses are purchased (and may be a limiting factor to system expansion) based on the number of devices and credential holders.

Central Equipment Processing (Level 1), continued

Backup Power

The ACS power also should have a backup. All computers should be provided with an uninterruptible power supply (UPS) that can provide the required length of operation. The minimum time required to initiate an orderly shutdown and saving of all data with a software/hardware connection to the ACS computers should be 15 minutes.

The card reader panels should have some type of battery backup for the electronics and, possibly, the doors controlled by the reader panel. A four-hour backup is commonly provided for the door operation. The length of time for the reader panel backup must be determined by applicable codes and given the final approval by the AHJ. If emergency power is available, the ESS designer should consider connecting the ACS to this source as well as to the UPS.

In addition to backup power requirements, many clients and equipment manufacturers may require dedicated access control branch circuits for the primary power source for ACS equipment. Coordination with electricians, building/facility maintenance personnel, and others may be required to meet this requirement.

Environmental Conditions

Environmental conditions must be considered when locating any equipment associated with the ACS. The spaces used for the card reader panels and input/output (I/O) panels must have adequate environmental conditioning.

The manufacturer must indicate the maximum and minimum operating temperatures and the humidity levels for its equipment's operation. If any equipment must be placed outside, it should be located in an appropriately rated weatherproof enclosure. Depending on the location, additional air conditioning and heating may be required in the enclosure.

Computer hardware has more stringent environmental requirements. The space in which a computer is installed must maintain recommended air conditioning and heating levels. If the space has to be modified to add additional heating or cooling, the ESS designer should seek the services of a mechanical engineer to help with the design of the heating, ventilating, and air conditioning (HVAC) system. The engineer will need the British thermal unit (Btu) or wattage of each and every piece of equipment added to the space. The UPS, computers, printers, monitors, and any additional equipment should be included in the Btu and power calculations.

Reliable long-term operation of air-cooled systems requires cleanliness and dust-free conditions.

 © 2012 BICSI®

Central Equipment Processing (Level 1), continued

Space Requirements

Space requirements for the electronics and computers associated with ACS must be coordinated with the installation site. The location of the reader panels and I/O panels is determined by the equipment's space requirements and proximity to the I/O devices. Coordination with the facility owner is required during such process. The equipment location must account for the required working clearances. Equipment must not be located in an inaccessible ceiling space.

Computer workstations (e.g., processor, monitor, printer) take up valuable desk space. The type of computer and monitor must be considered in relation to the available desk space.

Workstations

Access Control Workstation

The ACS workstation is primarily used for entering system data through some type of GUI interface 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.

Badging System

The badging station normally consists of the following:

- Workstation and software
- Camera
- Backdrop
- Camera lighting
- Badging printer and supplies

The badging station may be located in the security or the human resources office, depending on who is responsible for photography. The initial information about the cardholder may be manually or automatically entered into the system.

Central Equipment Processing (Level 1), continued

Images may be captured by a:

- Video capture card located in the workstation. (The card is connected to the camera.)
- Universal serial bus (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.)

Lighting and background color/conditions may be an important part of image capture. Taking pictures without a flash or adequate lighting under a fluorescent lamp produces a bluish tint and other unwanted colors in the images. Additionally, some organizations utilize colored or patterned backgrounds as a part of identifying authorized levels of access.

Visitor Management

The need to implement visitor management systems has increased. The key reasons for this need are that:

- Workplace violence, child abduction, industrial espionage, and global terrorism threaten the security of visitors, personnel, and property. When facility entrances are not secure, organizations are not only vulnerable, but they also are liable.
- A visitor lobby is the first line of defense. A lobby must support security physically, electronically, and procedurally. Client-specific procedures must accurately and rapidly capture the visitors' images, business cards or driver's licenses, and signatures, and they must authenticate these credentials and crosscheck the information using the security watch lists.
- Digital information outperforms paper trails when it comes to security. Logbooks may be illegible, and the visitors may fail to sign out and return temporary badges.
- Visitor management systems offer benefits beyond security. Electronic visitor registration is quicker and more reliable. Preprinted badges enhance a professional image for the company, improve visitor services (e.g., wayfinding), enhance confidentiality, and may enhance emergency response because the visitors' 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.

 © 2012 BICSI®

Controllers for Intelligent Field Processing (Level 2)

A system controller provides multiple purposes and benefits as a critical element in an ACS.

The system terminology varies by manufacturer. For the purpose of this manual, the following terms may be used interchangeably:

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

Access Controller

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.

Controllers are available in multiple configurations, hardware styles, and capacities. Controllers are designed to interface with specific access control server software. This interface is the controller's distinguishing characteristic.

Controllers from different manufacturers share similar design characteristics, including the:

- Industrial grade central processing unit (CPU).
- Internal flash memory for the controller's software and configuration.
- Internal memory for historical events.
- Watchdog software for monitoring the controller's electronics.
- Power supply.
- Battery backup.
- Communication ports.
- Door interface modules.
- Auxiliary inputs.
- Auxiliary outputs.
- Fuses to protect the electronics.

Controllers for Intelligent Field Processing (Level 2), continued

Controller Configurations

Controller configurations vary by manufacturer and have no standard appearance or dimensions. Two main controller configurations are often encountered in the marketplace. In the first configuration, 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.

The second configuration utilizes multiple enclosures that 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.

A typical access control panel may have:

- Two to four card readers.
- Two matrix keypads.
- Sixteen alarm inputs.
- Four to eight relay outputs.
- A 5,000 to 25,000 card capacity.
- A 6,600 to 10,200 event buffer.

Expansion boards are available for additional relays. Communications may be carried out through either a 20 milliamperes (mA) loop using American standard code for information interchange (ASCII) text characters or multidrop using RS-232 or RS-485 protocols. The panel typically operates at 12 volts direct current (Vdc) and the locks at 24 Vdc. Light-emitting diodes (LEDs) are used to designate when a relay is energized.

 © 2012 BICSI®

Peripheral Devices (Level 3)

Four fundamental peripheral components or devices are required for an ACS to function as designed:

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

Request to Exit (REX)

An REX (also known as RX, RTE, or RQE) 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.

The REX device has three purposes in ACS:

- Signal some function that occurs at the time of egress—The most common is to shunt a door contact so that an alarm is not generated by a proper egress.
- Unlock a door from a remote location—For example, a receptionist might buzz someone into a normally locked area.
- Unlock a door from the egress side to exit an area—This most commonly will be the case with magnetic locks. When an REX device is used for this purpose, its use is guided by standards, building codes, and the local AHJ. Safety considerations will need to be considered above the requirements for security.

Several types of REX devices include a:

- Passive infrared (PIR) motion detector.
- Door release button.
- Microswitch within door hardware (e.g., mechanical, electromechanical, pneumatic).

Card readers and keypads also may function as an REX device.

Peripheral Devices (Level 3), continued

Passive Infrared (PIR) Motion Detector

The PIR detector is a device that senses a person's body heat in the form of invisible infrared (IR) energy.

The level of IR energy radiated by a person entering the sensing area of the PIR is compared with the amount of IR energy that existed before the person approached this area. The dramatic change in IR energy prompts the PIR to send a signal to the ACS to bypass the door alarm. The PIR also may be used to open the locking device automatically.

The PIR is installed:

- On the secure side of the door.
- On the ceiling, wall, or doorframe.
- Above the floor 2.1 meters (m [7 feet (ft)]) to 4.6 m (15 ft).

Mortise Lock

When including the option of an REX switch turning, the inside lever activates the microswitch within the lock.

Door Release Button

Another common REX device is the door release button. The door release button may be either mechanical or pneumatic. The door release button REX is usually a momentary switch manually pressed for activation. When pressed, the switch changes state, signaling the ACS to bypass the door alarm. The door release button also may be used to open the locking device automatically.

The door release button REX is installed:

- On the secure side of the door.
- On the wall adjacent to the door latch.
- 1067 mm (42 in) to 1220 mm (48 in) from the floor.

Door release button REX devices are typically used for electromagnetic locks. Although the preferred locking method is electromechanical, there are instances where electromagnetic would be used. PIR REX should never be used with an electromagnetic lock because it is more susceptible to interference from the unsecured side of the door than a door release button.

 © 2012 BICSI®

Peripheral Devices (Level 3), continued

Panic Bar

The panic bar is a metal push bar and latch mechanism installed on the secure side of the door 1015 mm (40 in) from the floor. Pressing the push pad activates the microswitch within the bar. The delayed egress panic bar has a timer that can be set in accordance with the AHJ to delay the egress until a specific wait period is reached. This style of REX is usually used on emergency exit doors. These panic bars can be used to trip a local sounder or trigger a camera aimed at this door to start recording. This configuration is used to discourage individuals from using the door for anything but emergencies.

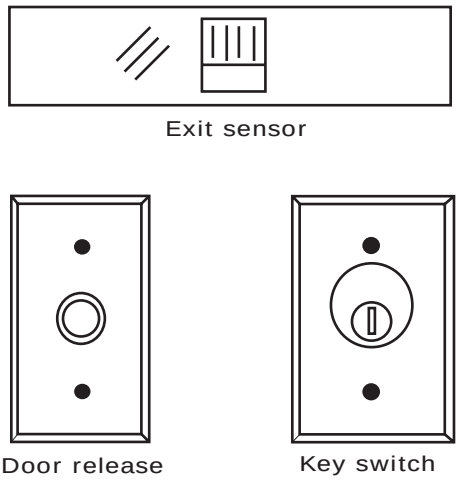
Panic bar options are:

- Mechanical.
- Electromechanical.
- Pneumatic.
- Delayed egress.

Key Switches

A key switch is simply a switch that uses a mechanical key to operate the switch. The key switch may be mounted in a plate that may have LEDs, indicating its normal or changed state. Its purpose is to change normal operation at a door rather than control normal operation (see Figure 4.1).

Figure 4.1
Request to exit devices



Peripheral Devices (Level 3), continued

Electrified Exit Hardware

Electrified exit hardware is often called panic hardware. The use of panic hardware is often required in the means of egress and is common in double door applications (see Figure 4.2). There are several options for electric exit hardware—electrically operated trim, electric dogging, electric latch retraction, delayed egress, and alarmed.

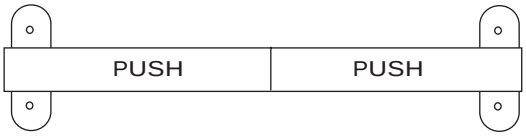
Common considerations include the following:

- Electric latch retraction exit hardware normally requires special power supplies because of the initial power inrush necessary to unlock devices. The power drop concern for these devices often leads to placing the power supply near the controlled doors.
- Electrically operated trim normally does not require special power supplies as there is typically no inrush requirements. Electrified trim can be either fail-safe or fail-secure.
- Because the actuating solenoid is on the door (inside the hardware case), a power transfer from the doorframe is necessary.
- In retrofit applications, many existing models of panic devices can be electrified without purchasing new hardware. This capability eliminates altering the original hardware design. If the door is in the means of egress, an ESS designer should ensure that the modifications are listed for the intended purpose.

Figure 4.2
Electrified exit hardware



Powered panic egress push bar



Nonpowered egress push bar

 © 2012 BICSI®

Peripheral Devices (Level 3), continued

Door Contacts

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 (see Figure 4.3).

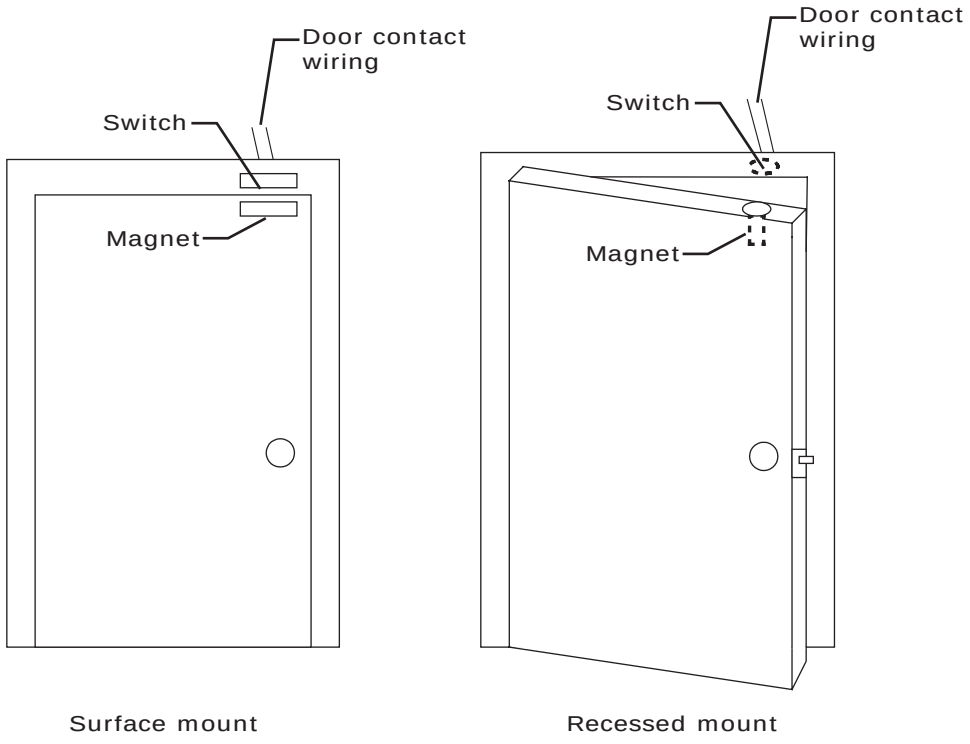
Two main mounting options are available:

- Surface mount
- Recessed mount

Door contact locations need to be coordinated with the door frames. In large construction projects, door contact and frame drilling information may be indicated on a door schedule.

NOTE: The door contacts should be mounted in accordance with manufacturers' recommendations to minimize opportunity for defeating the door contacts.

Figure 4.3
Door contacts



Peripheral Devices (Level 3), continued

Defeating Door Contacts

In the surface mount option, the location of the door contact magnet is easily found. The magnet may be defeated by presenting another magnet near the reed switch. When positioned correctly, the substitute magnet holds the reed switch in place as if the door were still closed. Surface-mounted door contacts are vulnerable because they may be easily compromised by shorting a jumper wire across the normally closed terminals.

The recessed mount option is the more aesthetically pleasing as well as secure of the two options based on its physical characteristics. Both parts of the door contact are hidden. This option is preferred because an attempt to interrupt the hidden contact with another magnet would probably jam the door or not close it properly. The switch and magnet may be harder to find. This option also makes an unauthorized entry more difficult.

High-Security, Balanced Magnetic Switch

Defeating a recessed mounted magnetic door contact is possible. For high-risk areas, high-security biased door contacts are often used. The high-security contact uses a biasing magnet, mounted inside the reed switch part of the package. This biasing magnet pushes the contact's reed switch to the door open or alarm position when the external magnet is not present and trying to pull the reed switch the other way.

The contact's actuator magnet (that is usually installed in the door) has the perfect balance of magnetism and opposing polarity as the biasing magnet. When the actuator magnet is installed at the recommended distance from the switch, it balances out with the biasing magnet. The position of the switch's contact remains in the door closed position.

If an unfamiliar or secondary magnet is positioned near the switch, the opposing and balanced magnetism between the bias magnet and the actuator magnet may be disturbed. The reed switch changes to the door open state. This would then send an alarm to the systems connected to it.

To increase security, a triple-biased door contact may be used. This device has three reed switches with three biasing magnets in one half of the package. The other half of the door contact includes three balanced actuator magnets. Defeating this device is considered difficult.

 © 2012 BICSI®

Peripheral Devices (Level 3), continued

Electrified Door Hardware

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—from a simple remote button to the ACS software.

The selection of release hardware is based on a number of factors, including:

- Facility's normal operations.
- After-hours operations.
- Building code and life safety standards.
- Security considerations.
- Retrofit (existing hardware) or new construction.

Designing and specifying door release hardware requires extensive knowledge of several factors about the facility, including:

- Door configuration (single or double, with or without mullion).
- Door material.
- Frame material.
- Lock hardware (function, style, and finish).
- Door hanging.
- Fire labeling.
- Exit signs at selected doors.
- Support hardware (door closers).

When building a design includes new doors, an ESS designer may have fewer limitations as new doors may be specified before any components are supplied. The ESS designer should confirm that the plans are current and complete and obtain updates on any subsequent changes.

In construction, the ability to match specified hardware and door preparation can lead to improved aesthetics, economics, security, and safety. The preparation may be based on approved standards (e.g., Builders' Hardware Manufacturers Association [BHMA]), custom, or left for field preparation. In new or retrofit installations, close coordination will be required with architects and door vendors or installers to ensure compatibility and correct fabrication of the door and associated materials (e.g., frames, hinges) prior to and during installation. Recommended installation and location of preparation for hardware may be based on information provided by the Door and Hardware Institute.

Peripheral Devices (Level 3), continued

Electrified door release hardware is typically employed to provide controlled access into an area or facility. From the outside, the door release is activated by electronic signal. The final door design is often determined by the building code and life safety standards that focus on egress though a door. These overriding parameters often lead to using mechanical methods of door release for egress out of an area or facility.

When employing electromechanical door locking hardware in a building interior, coordination with egress paths is required so that dead end corridors are not created.

IMPORTANT: Life safety design considerations take precedence over security.

Security issues extend beyond the basics of determining the persons allowed to access each door and the times of access. For example, for pure access control considerations, an ESS designer may specify releasing an electric strike upon the presentation of a valid card. Based on security considerations, an ESS designer evaluates the electric strike grade and status monitoring, latch guard specifications, and door contact shunt.

This section introduces the concepts that apply to most types of electrified door release hardware design. It then reviews the different types of release hardware available to the ESS designer. Support hardware necessary to complete the design is reviewed. Some discussion relative to portals other than doors (e.g., turnstiles, other specialty applications) is also included.

As with all design considerations, it is necessary to understand how the client or occupant plans to operate under normal usage and how these conditions may change throughout a 24-hour day. An ESS designer should consider and remind end users that all designs require ongoing attention and maintenance.

Fail-Safe/Fail-Secure/Fail Latched

Electrified door release hardware, like all hardware, may fail. How it fails is a critical design element. Electrified door release hardware may be classified as fail-safe or fail-secure.

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.

If a fail-secure device is kept unlocked for long periods of time, the device must be rated for continuous duty. Employing an inline power conditioner to minimize direct current (dc) voltage surges also is recommended to extend the life of the device.

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.

 © 2012 BICSI®

Peripheral Devices (Level 3), continued

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

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

Limitations of Fail-Secure and Fail-Safe

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 does 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.

Verifying performance of the REX is critical. The following items have to be verified:

- 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?

Power Distribution

Peripheral devices are typically powered by either 12 Vdc or 24 volts alternating current (Vac) 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 a multifused 12–24 Vdc/Vac power supply centralizes the power sources for multiple devices and accessories. This is in lieu of having alternating current (ac) outlets installed near each device. Voltage drop and wire size must 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 ac powered individually, more UPS circuits are required than a multifused power supply. A multifused power supply also simplifies placing a UPS circuit to one source for the multiple devices or accessories.

Peripheral Devices (Level 3), continued

Load Characteristics

The following characteristics of the various loads affect the amount of power (watts) that is required for these loads:

- Resistance
- Inductance
- Capacitance

Inductance and capacitance cause a difference between the real power (in watts) and the apparent power (in volt-amperes) required by the load in an ac circuit.

Ohm's Law

Ohm's law states that V = IR where:

I = current in amperes

V = voltage in volts

R = resistance in ohms

Ohm's law also can be expressed as:

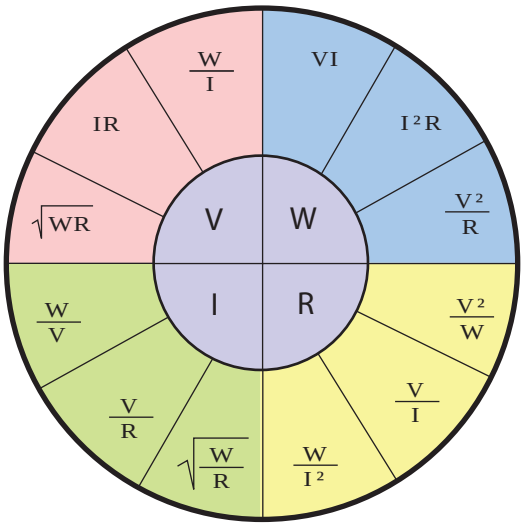
R = V/I and I = V/R

The formulas to calculate power in W in a circuit are:

$W = VI$
$W = I^2R$
$W = V^2/R$

These and other formulas are shown in Figure 4.4.

Figure 4.4
Calculation chart



 © 2012 BICSI®

Peripheral Devices (Level 3), continued

The formula for Ohm's law always applies to dc circuits, but it only applies to ac circuits that are purely resistive (e.g., incandescent lamps, resistive heating elements). However, many ac circuits (e.g., communications, data processing) have reactance (X) as well as resistance. Reactance is expressed in ohms and is the opposition to the flow of ac current caused by inductance and capacitance.

The net reactance is equal to the difference between capacitive and inductive reactance. This reactance can be combined with the resistance to calculate the impedance (Z), which is the total opposition to ac current flow and is measured in ohms.

The formulas to find Z are:

- When volts (V) and amperes (I) are known:

  $$Z = V/I$$

- When resistance (R) and reactance (X) are known:

  $$Z = \sqrt{R^2 + X^2}$$

- When resistance (R), inductive reactance (X_L), and capacitive reactance (X_C) are known:

  $$Z = \sqrt{R^2 + (X_L - X_C)^2}$$

Inductive Reactance (X_L)

Inductive reactance (X_L) is the portion of impedance that opposes a change in current flow because of magnetic field coupling. Because conductors in balanced twisted-pair cabling are in close proximity, together their mutual inductance has an impact on X_L and, therefore, the impedance of the circuit.

Capacitive Reactance (X_C)

Capacitive reactance (X_C) is the portion of impedance that opposes a change in voltage because of electric field coupling. Because conductors in balanced twisted-pair cabling are in close proximity, together their mutual capacitance has an impact on X_C and, therefore, the impedance of the circuit.

Peripheral Devices (Level 3), continued

Voltage Drop

Electrical conductors have resistance, and power is consumed because of this resistance. This consumption of power can result in voltage drop. Calculating the voltage drop is important when determining the conductor sizing for a circuit. Voltage drop can be calculated if certain factors are known.

These factors are:

R = resistance per foot of the conductor (ohms/ft)

I = current in the conductor (amperes)

L = one-way length of circuit (footage)

A = cross-sectional area of conductor (circular mils)

NOTES: The cross-sectional area of the conductor is expressed in circular mils. The cross-sectional area of standard American wire gauge (AWG) conductors is shown in Table 4.1.

K = specific resistance

K equals the specific resistance of the conductor material that is 0.3 m (1 ft) long with a diameter of one mil (i.e., 1 in divided by 1000 [1 mil = .001 in]). K value changes with temperature.

K = 12 for circuits loaded to more than 50 percent of allowable carrying capacity (copper conductor)

K = 11 for circuits loaded less than 50 percent of allowable carrying capacity (copper conductor)

K = 18 for aluminum conductors (30 degrees Celsius [ºC (86 degrees Fahrenheit [ºF])])

One place the resistances of standard conductors can be found is in the National Electrical Code®.

When these factors are known, the following formulas may be used to determine the voltage drop (V_d):

For two-conductor single-phase and three-wire single-phase circuits:

$$V_d = \frac{2K \times L \times I}{D}$$

For three-conductor three-phase circuits:

$$V_d = \frac{2K \times L \times I}{D} \times 0.866$$

 © 2012 BICSI®

Peripheral Devices (Level 3), continued

Table 4.1
Circular mils of standard American wire gauge conductors

Size (AWG or kcmil)	Circular Mils
18	1620
16	2580
14	4110
12	6530
10	10,380
8	16,510
6	26,240
4	41,740
3	52,620
2	66,360
1	83,690
1/0	105,600
2/0	133,100
3/0	167,800
4/0	211,600
250	250,000
300	300,000
350	350,000
400	400,000
500	500,000
600	600,000
750	750,000

AWG = American wire guage
kcmil = Thousand circular mil

Peripheral Devices (Level 3), continued

Locking Power Options

The voltage shall meet the requirements of the manufacturer. Considerations for selecting voltage also should include the following:

- 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 (see Table 4.2).
- 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 to 15 percent.
- Power for the door release hardware should be separate from power for any other electronics.

Power supplies must be sized to provide adequate power for the connected devices and have a source of primary power at their location. 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. This type of power inrush is most commonly seen with electrified exit or panic hardware.

Table 4.2
Voltage drop per 30 meter (m [100 feet (ft)]) run of paired wire (61 m [200 ft] total length of wire)

Gauge (AWG)	0.5 A Load Current	1 A Load Current	2 A Load Current	4 A Load Current	10 A Load Current
10	0.10	0.20	0.40	0.80	2.00
12	0.16	0.32	0.64	1.27	3.16
14	0.25	0.50	1.01	2.02	5.04
16	0.40	0.80	1.60	3.20	8.00
18	0.64	1.27	2.54	5.09	12.71
20	1.01	2.02	4.03	8.07	20.17
22	1.60	3.20	6.40	12.81	32.02

A = Ampere
AWG = American wire gauge

 © 2012 BICSI®

Peripheral Devices (Level 3), continued

Relays

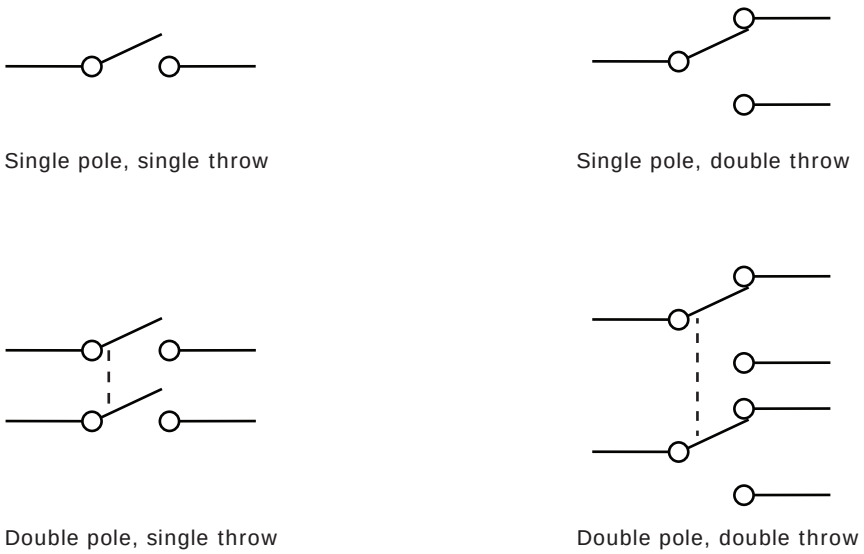
Control devices consist of lock output and relays for auxiliary inputs and outputs. Relays are typically used for auxiliary inputs and outputs to the ACS. The reason for relays is that the current required by the load is too much for the control device.

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.

A relay commonly has one of four configurations (see Figure 4.5):

- A single pole, single throw (SPST) relay simply opens or closes a signal path.
- A double pole, single throw (DPST) relay is two SPST relays, but they are energized from the same coil.
- A single pole, double throw (SPDT) relay provides one open and one closed path.
- A double pole, double throw (DPDT) relay is two SPDT relays that are energized from the same coil.

Figure 4.5
Types of relay configurations



Peripheral Devices (Level 3), continued

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

- Form A relay or normally open relay—An SPST relay that remains open until it is energized.
- Form B relay or normally closed relay—An SPST relay that remains closed until it is energized.
- Form C relay—An SPDT relay.

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 [s]), a time is assigned to the egress device (normally 0 s), and a default pulse time is assigned to the lock (approximately 10 s).

Metal Oxide Varistor (MOV)

A metal oxide varistor (MOV) should be used across electronic lock inputs at the door to mitigate the possibility of reverse current presented by the lock toward the controller or power supply when the lock de-energizes. If not implemented over time, the reverse current can damage the controller or lock power supply. An MOV is voltage rated, and the ESS designer must ensure that the MOV is rated for the voltage application.

Fire-Rated Hardware and Doors

The fire ratings of door release hardware and doors affect the design process. Fire-rated hardware must always be used on fire-rated doors. The hardware must be listed for the intended purpose by a nationally recognized testing laboratory (NRTL) or another nationally recognized testing facility. The ESS designer should be familiar with NFPA 80, *Standard for Fire Doors and Other Opening Protectives*, which describes requirements for fire doors.

In retrofit applications, fire-rated doors may be identified by the labels affixed to the hinge side edge of the door. On newer wooden doors, the label may be on the top edge of the door. The door should be checked closely as the label may have been painted over.

Fire-rated doors are manufactured and listed to meet particular requirements. They generally are manufactured for specific hardware. Building plans are used for documenting how the doors were originally designed and installed. In retrofit applications, doors may not be field modified. In limited situations, they must go through a relisting process by a listed testing agency. Otherwise, modifications may only be done in certified shops. The changes are then documented, and the doors are relabeled.

 © 2012 BICSI®

Peripheral Devices (Level 3), continued

Lock Types, Functions, Grades, and Styles

To coordinate proper door release hardware, an ESS designer must have a thorough understanding of basic door locks, including:

- Bored locks—Mounted by boring a hole through the door. They latch to a strike cut into the center of the frame of a door and may be divided into cylindrical locks and deadlocks.
- Rim locks—Mounted to the surface of the door and latch to a surface-mounted strike.
- Mortise locks—Embedded (mortised) into the door and latched to a strike cut into the center of the doorframe.
- Vertical rod locks—Use vertical rods that latch to the top and/or bottom of the door. Concealed vertical rods indicate that the locking rods are concealed within the body of the door.

All locks operate differently. The way they work is known as a lock function. Some of the most common lock functions are:

- Entrance locks—When pushed in, an inside button locks the outside lever. When the button is released, the outside lever is unlocked. When the outside lever is locked, a key must be used for access. The inside lever always allows free egress.
- Storeroom locks—These locks are key operated from the outside because the outside lever is always locked. The inside lever always allows free egress.
- Classroom locks—The outside lever is accessed by key when it is locked. The outside lever is locked and unlocked by the same key. The inside lever is always free egress or may lock from the inside.
- Vestibule locks—The outside lever is accessed by key when it is locked. A key in the inside lever determines if the outside lever is locked or unlocked. The inside lever always allows free egress.

The term grade is often used to classify door hardware by durability. Hardware grades are defined in several standards, including those issued by American National Standards Institute (ANSI)/BHMA. A grade 1 lock has been tested to be more durable than a grade 2. A grade 2 has been tested to be more durable than a grade 3. Grades also are used for locks and many other types of door hardware.

Lock styles and finishes are important when adding or changing hardware to keep a consistent look. This is best achieved by continuing to use the manufacturer of the existing hardware. The key-way (keyhole) also should remain the same.

Peripheral Devices (Level 3), continued

Electric Strikes

Electric strikes replace the strike where a lock latches to the frame of a door. Upon application (fail-secure) or removal (fail-safe) of power, a solenoid electrically activates the keeper, allowing a lock's latch bolt to pass. Electric strikes are considered the most common type of door release hardware (see Figure 4.6).

Common considerations are:

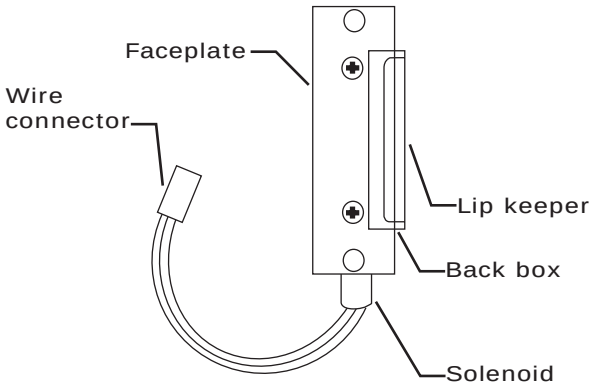
- Electric strikes are cut into the frame of a door for bored locks, mortise locks, and vertical rod devices or surfaced mounted for rim-type exit devices.
- Egress from an area is normally the same as if there were no electric strike. Often, current lock hardware does not need to change. However, the mechanical lock function must be locked at all times if control of access is to be approved by the ACS.
- Electric strikes are most commonly fail-secure as the locking hardware normally allows free egress mechanically, and it maintains the desired locked status.
- Electric strikes have performance ratings that indicate static strength, dynamic strength, and endurance levels. For example, a grade 1 strike can withstand 6670 newtons (N [1500 pound-force (lbf)]) in a static strength test, withstand 95 joules (J [70 ft. lb]) in a dynamic strength test, and operate for 500,000 cycles (door opens/closes).
- Electric strike's unlock time is normally set by the ACS.
- Electric strikes must be matched to the type of locking hardware employed.
- Electric strikes may be furnished with optional monitoring switches:
  - Latch bolt monitor—Checks that the latch bolt extends into the strike pocket.
  - Locking cam monitor—Checks that the strike keeper returns to the locked position.
  - Dead bolt monitor—Similar to the latch bolt monitor, it checks that the dead bolt extends into the strike pocket.

NOTE: Each monitoring switch requires additional wiring between the device and the controlling electronics. Electric strikes are not permitted for use at fire stairs where building code requires stair side of door to be unlocked in an emergency.

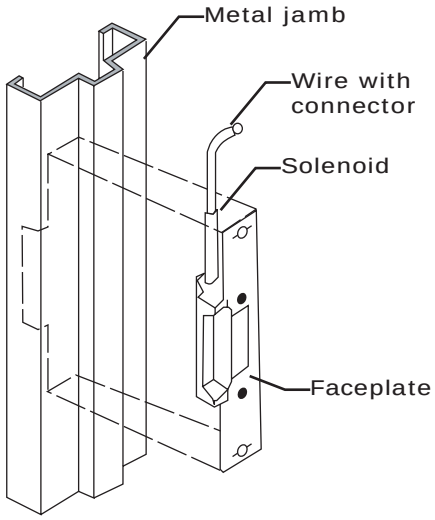
 © 2012 BICSI®

Peripheral Devices (Level 3), continued

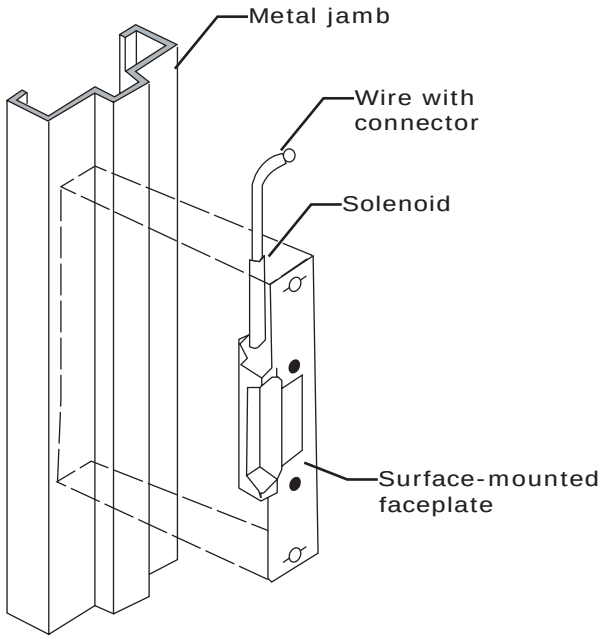
Figure 4.6
Electric strikes



Electric strike



Hollow metal jamb with electric strike



Surface-mounted electric strike

Peripheral Devices (Level 3), continued

Magnetic Locks

Magnetic locks may be divided into two general types: direct hold and shear locks (see Figure 4.7). With the direct hold type, an electromagnet is mounted on the doorframe opposite the metal plate (strike) known as the armature. When energized, the lock bonds to the armature and locks the door. Normally, a magnetic lock is mounted to the top of the doorframe on the lock edge. The armature is mounted to the door.

The shear lock type uses both magnetic and physical properties for locking. In a concealed mounting application, the electromagnetic lock body is mortised into the door's frame, and the armature is mortised into the door edge. Indentations in the armature receive protrusions in the lock body. The combination of these properties considerably increases holding force.

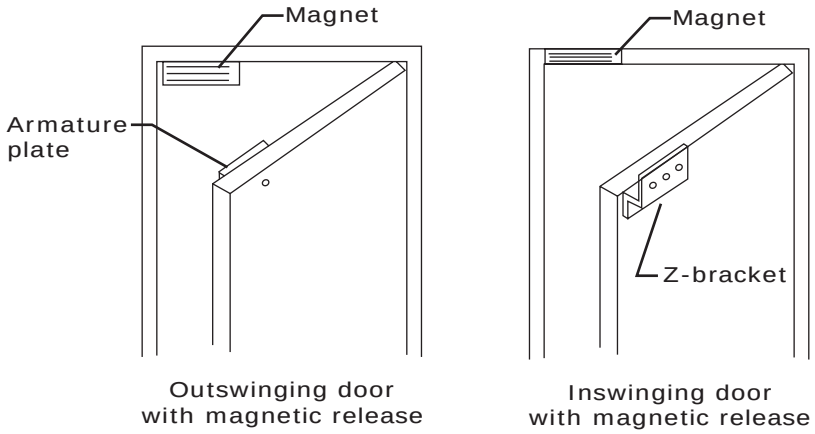
Common considerations are:

- Magnetic locks are fail-safe and may not be used as the only hardware on fire doors (latching is necessary). However, no other locking hardware may be on the door.
- Magnetic locks are fail-safe, and doors are unlocked in the event of power failure, allowing a potential security breach.
- For egress purposes, some method of release is required from the egress side. Building code requirements of magnetic locks are typically categorized into the heading "Access Control Egress Doors," and some jurisdictions require two means of release. One of the methods may need to be a mechanical switch (not an electronic switch). If a push to exit button is used, it must be a pneumatic type so that the door is released for a full 30 seconds. It must be mounted within 1.5 m (4.9 ft) of the door at a height between 1015 mm (39.9 in) and 1220 mm (48 in) above finished floor (AFF).
- If a fire alarm system or automatic sprinkler system is present, magnetic locks should be connected to the fire alarm system so that they release upon alarm activation. The doors must remain unlocked until the fire protective system is manually reset.
- Magnetic locks come in a range of holding forces. The greater the holding force, the less susceptible the lock is to attacks. Common holding forces are 317.51 kg (700 lb), 544.31 kg (1200 lb), and 748.43 kg (1650 lb).
- Direct hold magnetic locks are noiseless. Shear locks energize with a significant clunk.
- Adding a magnetic lock to the doorframe in the means of egress may not reduce the vertical height from the floor to less than 1981 mm (78 in [or door width less than 813 mm (32 in)]).

 © 2012 BICSI®

Peripheral Devices (Level 3), continued

Figure 4.7
Magnetic locks



Peripheral Devices (Level 3), continued

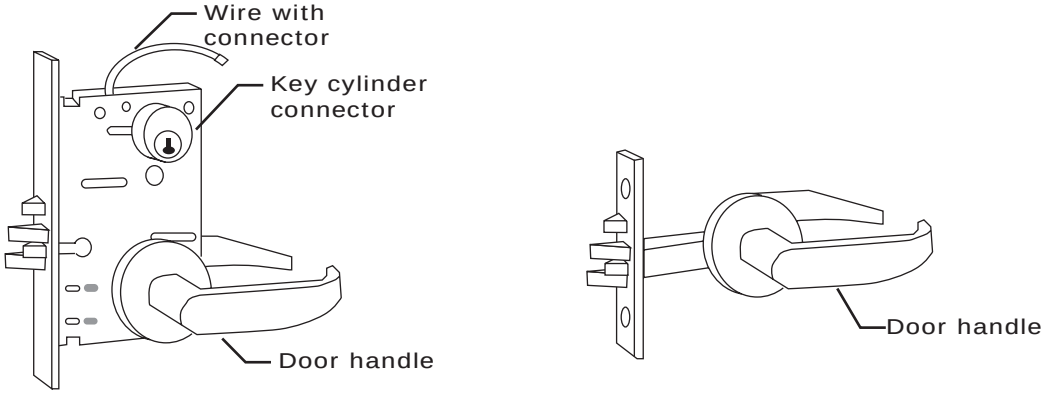
Electric Locksets / Electric Latch

Electric locksets incorporate actuating solenoids that lock or unlock the lockset, duplicating or replacing the function of a traditional mechanical key (see Figure 4.8).

Common considerations include the following:

- Electric locksets are typically cylindrical lever sets or mortise locksets.
- Egress at the door is the same as with a standard lockset.
- Mechanical key override is typically provided as a backup option in the event of electronic failure for access purposes.
- Low-voltage power is provided to the solenoid on the door inside the lock body. A power transfer device from the frame of the door to the lockset is necessary.
- Wiring between the power transfer device and the lockset may be achieved in a number of ways. An ESS designer should review considerations for fire-rated doors before any of the following methods are considered because applicable codes (e.g., International Building Code [IBC], National Fire Protection Association [NFPA]) and NRTL standards relating to the fire rating of the doors may limit or prohibit modifications:
  - Surface-mounted raceway (e.g., conduit, wood trim)
  - Wire routed through the existing channels in the door
  - Coring the door's width from the hinge side to the latch side

Figure 4.8
Electric locksets



Electric mortise lock with handle and key cylinder

Electromechanical cylindrical lever lock

 © 2012 BICSI®

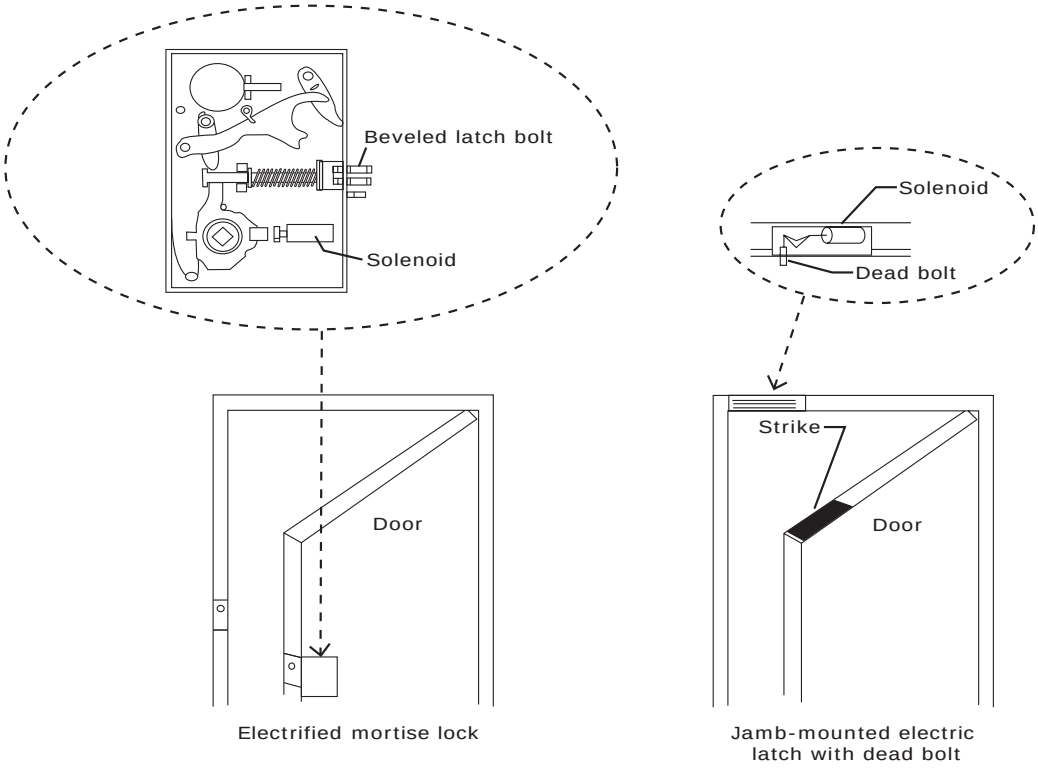
Peripheral Devices (Level 3), continued

Electric Bolts

Electric bolts are conceptually similar to electric locksets. Their applications are best suited to situations other than the usual door access control. Similar to a standard mechanical dead bolt, electric bolts are better suited for security purposes than access purposes (see Figure 4.9). In a common access scenario, a door unlocks electronically, the passage occurs, and the door closes, latches, and locks without further action. On the other hand, a dead bolt once retracted must be specifically relatched (even electronically) or left unlocked.

These devices are best suited for high-security applications where normal life safety issues may be secondary or applications (e.g., storage closets, cabinets) where people do not move in and out of an area.

Figure 4.9
Electric latch and bolt

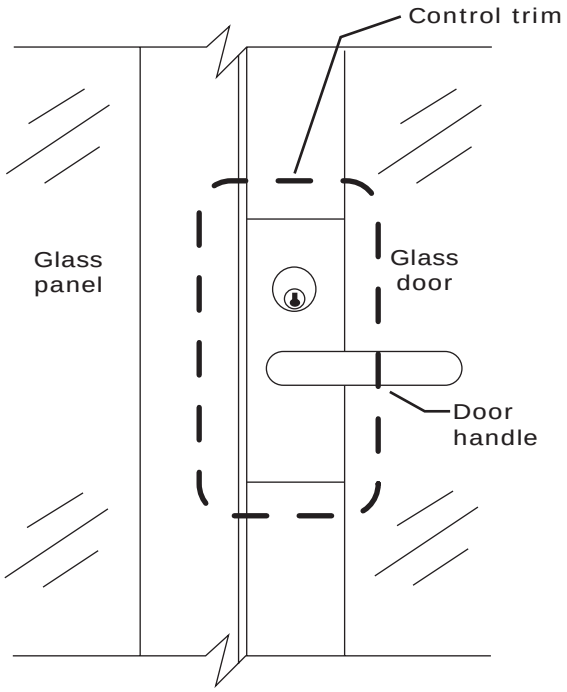


Peripheral Devices (Level 3), continued

Control Trim

Trim is the hardware on the side of the door opposite from the locking hardware. It is often just the pull that a person grasps to open a door from the outside. Control trim may be linked with an egress device, but the actuating solenoid is within it rather than within the hardware on the other side (see Figure 4.10).

Figure 4.10
Control trim



 © 2012 BICSI®

Peripheral Devices (Level 3), continued

Delayed Egress Devices

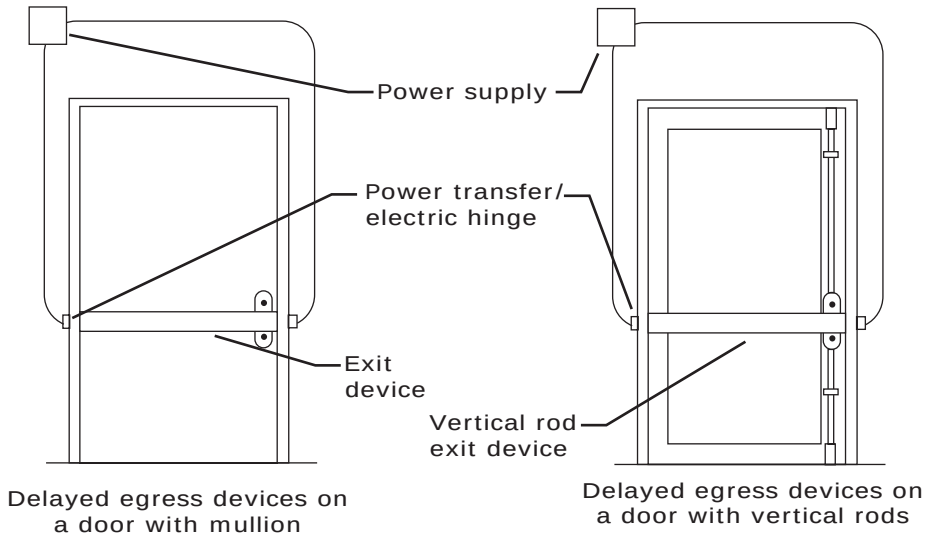
Delayed egress devices are employed to control a person's departure (egress) from an area rather than access (see Figure 4.11). Its concept is to delay a person attempting to leave the area, thus allowing premises management to respond to the door. Because life safety considerations always trump security considerations, a person is always allowed to leave. In most cases, a person is delayed for 15 seconds.

Common considerations include the following:

- The AHJ should always be consulted about delayed egress doors to ensure compliance with applicable codes (e.g., NFPA 101, IBC).
- Local codes may require that delayed egress devices must be connected to an approved supervised automatic fire detection system or an approved supervised automatic sprinkler system so that they are released immediately in the event of fire alarm activation.
- Delayed egress devices emit a local alarm, indicating the initiation of the REX.
- On the door adjacent to the release device, a visible durable sign should be posted with the letter minimum height and width of 25 mm (0.98 in) 3 mm (1/8 in), respectively, and a contrasting background, reading, "Push until alarm sounds; door may be opened in XX seconds."
- Emergency lighting must be provided. This may come from a nearby electrically illuminated exit sign.
- Where approved by the AHJ, a delay not exceeding 30 seconds may be permitted.
- A person may only be stopped once by a delayed egress device in the means of egress.

NOTE: This is not permitted in all types of occupancies.

Figure 4.11
Delayed egress devices



Peripheral Devices (Level 3), continued

Power Transfer Devices

Power transfer devices transfer power and signal from the doorframe or the wall next to the frame to the door itself. A number of different types of power transfers exist. Each of these performs the basic functions of providing a path for wiring and protecting the wiring. Some types are invisible when a door is closed, thereby affording protection from vandalism or other attack and do not affect aesthetics. Certain transfers limit the quantity or gauge of their wiring.

Door Loops

Door loops, sometimes referred to as door cords, are basically armored cables with mounting caps on each end. They are usually mounted near the top. Door loops are normally empty channels, but they may come with internal wiring.

Electrified Hinges

Electrified hinges come with internal wiring. The number of conductors and wire gauge must be specified. Because the electrified hinge is replacing a standard door hinge, the size and finish also must be specified. Electrified hinges may have up to 10 conductors, but wire gauge is limited. Electrified pivot type hinges also are available.

Mortised Transfer

This type of power transfer is mortised into the doorframe and the door itself. When the door is closed, it is completely invisible. Certain versions include telescoping steel tubes to protect the wiring and allow for heavy gauge wiring. Because of its design, the wiring is less susceptible to breaking.

 © 2012 BICSI®

Peripheral Devices (Level 3), continued

Door Closers

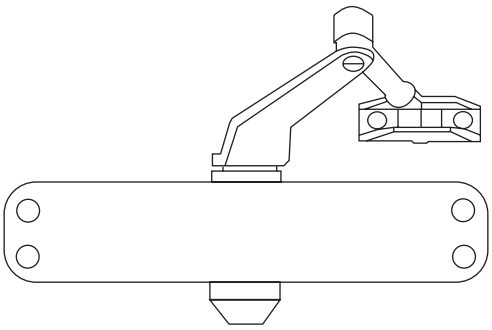
Door closers are a crucial element of access control hardware. In typical installations, a door is opened, the passage occurs, and the door is pulled closed by a door closer (see Figure 4.12). If the door does not close at the proper speed, the hardware does not relatch and lock the door. If the door closes too hard, it also may not latch properly or, at a minimum, cause hardware failure more quickly.

In new construction, the architect selects an appropriate closer for the door. In retrofit applications, an ESS designer has to check that a closer is present and confirm that it is working properly. If it is closing too strongly or too weakly, the closer should be replaced or repaired.

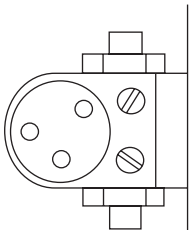
NFPA 80 places door closers into the following three categories:

- Self-closing—The door closes and latches each time it is opened.
- Automatic closing—The door contains either a separate or an integral hold open mechanism that automatically closes the door during an alarm condition.
- Power operated—The door must be equipped with a releasing device that will automatically disconnect the power operator at the time of fire, allowing a self-closing device to close the door regardless of power failure or manual operation.

Figure 4.12
Door closer hardware



Front view



Side view

Peripheral Devices (Level 3), continued

Latch Guards

Latch guards are usually designed to protect the lock latch so that it cannot be compromised. Doors that open outward into an unsecured area are the most vulnerable. There is normally a doorstop hindering access to the latch on swinging doors. On properly installed well-designed doors, the amount of gap between door and frame may not be of concern. If the frame is solid and the gap cannot be spread, the need to protect the latch is greatly reduced.

When an electric strike is installed, however, it is often necessary to cut away part of the frame first. This creates a larger gap between the door and the frame and reduces the strength of the frame. When installing electric strikes, it is recommended to install a latch guard to protect the latch.

Astragals and Coordinators

An astragal is a piece of material attached across the length of a door on the latch edge. It is sometimes used on pairs of doors without a mullion to cover the gap between the doors. Its purpose is to act as either a doorstop or firestop. If it is present, it needs to be considered for impact on access control design.

A coordinator also is employed on pairs of doors without a mullion. Its purpose is to ensure that one of the two doors closes before the other does.

Door Hold-Opens

Door hold-opens are designed to control smoke by closing doors in the event of fire. They are often used on hallway doors, which are held open in normal operations. For the purpose of fire safety, however, such doors must close and latch in the event of fire. Two general types of door hold-opens are controlled by the fire alarm panel—magnetic and fire closer/holder.

Typically, the magnetic type is a wall or floor mounted magnet, whereas the fire closer/holder devices are typically integral to a door closer unit.

Revolving Doors

Revolving doors generally are used for special applications where access control is employed for greater numbers of personnel entering an area. Revolving doors employ physical routing and speed limitations to achieve the desired access control goals.

Security considerations are generally low as they allow traffic to flow in two directions. Sometimes, revolving doors are used to control the loss of heating or cooling or for aesthetic purposes.

 © 2012 BICSI®

Peripheral Devices (Level 3), continued

Revolving doors must comply with the following, even if they are not within the required means of egress:

- Revolving doors should be capable of collapsing into a book-fold position.
- Revolving doors must not be used within 3 m (10 ft) of the foot or the top of stairs or escalators. A dispersal area acceptable to the local AHJ must be located between the stairs or escalators and the revolving door.
- Revolutions per minute of powered revolving doors must not exceed the values designated by the AHJ and applicable codes (e.g., NFPA 101).
- Local codes often require each revolving door have a conforming side hinged swinging door in the same wall as the revolving door within 3 m (10 ft).

Revolving doors shall comply with the following if they are a component in the means of egress:

- Revolving doors must not be given credit for more than 50 percent of the required egress capacity.
- Revolving doors must be capable of collapsing into a book-fold position when a force not exceeding 578 Newtons (N [130 pound-force (lbf)]) is applied to the wings within 75 mm (2.95 in) of the outer edge.

Because of the above elements, architects are more likely to consider revolving doors for access issues. ESS designers are more likely to look to the required doors near revolving doors for their access applications. The ESS designer should understand the operational requirements of the revolving doors as they relate to areas such as after-hours operation (locked, entry/exit or exit only), modes of operation during a loss of power (fail-safe, fail-secure), and other nonstandard situations that may affect the ESS design.

Turnstiles

While revolving doors are generally on the perimeter of a building, turnstiles will generally be inside a building controlling access to an area. Like a revolving door, a turnstile is used for special applications where access control is employed for greater volumes of personnel entering an area and employs physical routing and speed limitations to achieve its desired goals. Turnstiles may be used for something as simple as counting people accessing an area, to control the flow of people to a guard station, or for ACS involving fare collection (e.g., transit systems).

Turnstiles have life safety considerations, even if they are not a component of the means of egress. Those considerations include the following:

- Turnstiles exceeding 991 mm (39 in) in height shall meet the requirements for revolving doors.
- Turnstiles that restrict travel to one direction shall not be placed so as to obstruct any required means of egress. There are specific exceptions that must be approved by the local AHJ.

Peripheral Devices (Level 3), continued

Interlocks

The basic concept of an interlock, sometimes referred to as a mantrap, is to physically control access by having an approved person pass first through one barrier, making the barrier close and lock, and then passing through a second barrier after access is granted. This is a high-security device as passage through the second barrier may occur only after the first barrier is resecured.

Two common types of interlocks are safety interlocks and security interlocks.

Door Operators

When it is necessary to open a regular side-hinged door upon command, a powered door operator is the most common answer.

Common considerations are as follows:

- Door operators are either electrically powered or pneumatic.
- Door operators can be concealed in a new construction. In retrofit applications, they look like a door closer when surface mounted.
- Door operators can be mounted either on push or pull side.
- In vestibule applications, units can be configured for sequential operation. If one is a push device and one a pull device, they both are installed within the vestibule if aesthetics are an issue.
- Most door operators also function as door closers.
- An operator may be activated by a paddle (button), radio frequency (RF) transmitter, access control credential remote push button, or all of the above.
- An operator may be obtained with a power assist feature that activates it with minimal pressure of pushing or pulling on the door.
- Primary electrical power is required for electrical units at the operator and for pneumatic units at the pneumatic headend. Pneumatic tubing must run from the headend to the operator for pneumatic drive units.
- The ESS designer should consider regulatory requirements (e.g., ADA) when coordinating with door operators. In addition, where card readers are located at portals equipped with door operators, the ACS should interface with the door operator equipment such that the door operator is only enabled when the latch is retracted.

 © 2012 BICSI®

Peripheral Devices (Level 3), continued

Readers

A reader transfers information from a credential (level 4) to a controller (level 2). The type of credential to be used is the most important consideration in selecting a reader. Descriptions of the type of reader are included with the credential description on the following pages.

An agile reader can read RFID tags operating at different frequencies or using different methods of communication between the tags and readers. A design consideration when dealing with RFID is sensitivity to interference caused by adjacent metallic surfaces.

Hoteling Systems

Hoteling systems are usually stand-alone, battery-operated systems. Commonly used in dormitories and hotel rooms, the lock and card reader are contained in the same physical housing and installed on the door. There is no hardwired or wireless connection to a controller, software, or databases.

When cards are presented at a non-hoteling card reader connected to the database, the programming for the hoteling system card reader is encoded on the card. Whenever a new card is presented to a hoteling card reader, the programming encoded on the card updates the hoteling card reader. Doors with heavy usage (e.g., main entrances) should be hardwired so that new updates are encoded on the cards frequently.

The advantages to these systems are low cost and, unlike keys, the ability to remove users or limit access to a specific time period with software. System disadvantages include not being able to change access rights at the hoteling card readers without physically presenting new programming and the inability to obtain real-time reporting.

Web-Enabled Access Control

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.

Internet Protocol (IP) Card Readers

IP ready card readers are devices that have all the connections for the lock, REX device, and door position sensor (DPS) for an access door. All that is required for connectivity is a balanced twisted-pair cable and one power cable from the main distribution frame (MDF) or intermediate distribution frame (IDF) 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 power over Ethernet (PoE), which eliminates the need for a separate power cable. While PoE is tempting, most major metropolitan areas require that lock power drop when the fire alarm detects an alarm condition. This requirement is easier and less expensive to implement when there is a single power source.

Internet Protocol (IP) Controllers

IP controllers are mounted on the secure side of the door, allowing for both fail-secure and fail-unsecure 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.

Credentials (Level 4)

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

Radio Frequency Identification (RFID)

An RFID system consists of a tag made up of a microchip with an antenna and an interrogator or reader with an antenna. The reader sends out electromagnetic waves, and the tag antenna is tuned to receive these waves. A passive RFID tag draws power from the field created by the reader and uses it to power the microchip's circuits. The chip then modulates the waves that the tag sends back to the reader, and the reader converts the new waves into digital data. An active RFID tag performs similarly but utilizes a battery to increase the read range.

The read range of passive tags depends on many factors (e.g., frequency of operation, power of the reader, interference from other RF devices). In general, low-frequency tags are read from 0.3 m (1 ft) or less. High-frequency tags are read from about 1 m (3 ft), and ultrahigh frequency (UHF) tags are read from 3 to 6 m (10 to 19.7 ft). When longer ranges are needed (e.g., for tracking railway cars or motor vehicles), active tags use batteries to boost read ranges to 91 m (299 ft) or more.

Access Control Cards, Credentials, and Biometrics

Access cards use various technologies and are often the size of a credit card.

Some examples of credentials in card form include:

- Smart card.
- Proximity card.
- Wiegand effect card.
- Magnetic stripe card.
- Bar code card.

Personal Identification Verification (PIV)

Personal identification verification (PIV) cards contain varied information on the credential, often including biometrics. PIV cards allow interaction between the credential and the reader for more secure physical access. Originally a U.S. government employee requirement, many corporations and institutions looking for common access cards, including health care centers, are adopting PIV credentials instead of traditional physical access cards. The U.S. Office of Management and Budget issued memorandum M-11-11, directing U.S. government agencies to require the use of PIV credentials.

 © 2012 BICSI®

Credentials (Level 4), continued

USAccess

In 2004, the President of the United States issued Homeland Security Presidential Directive 12, HSPD-12, mandating a security standard for government employees, members of all branches of the U.S. military, and contractors. Federal Information Processing Standard (FIPS) 201 specifies detailed technical requirements of the common identification standard, including biometrics for U.S. federal employees and contractors requiring access to government facilities and information systems. USAccess is a General Services Administration program that provides common enrollment and HSPH-12 compliant credentials to U.S. government employees.

Personal Identity Verification Interoperability (PIV-I)

Personal identity verification interoperability (PIV-I) is an interoperable standard used by private corporations as well as U.S. state and local governments to issue a single multipurpose credential to replace multiple cards. The PIV-I framework has the ability to verify identity on the card and in the physical ACS match. The use of a single trusted credential and verification software can allow quick access to PIV-I cards for enterprise employees located across countries and improve efficiency.

Personal Identity Verification (PIV) Examples

Transportation Worker Identification Credential (TWIC) is a U.S. Transportation Security Administration mandate for tamper-resistant biometric credentials to prevent individuals without clearance from entering secure areas of ports and vessels. First Responder Access Credentials (FRAC) are U.S. federally approved identification cards for local, state, and federal agencies along with private security first responders. Many ordinary citizens have obtained PIV credentials by using e-passports. Many government e-passports contain biometric information and digital photos used for identification.

Credentials (Level 4), continued

Contactless Smart Card

The smart card works in a similar way as the proximity card, but at a different operating frequency. The smart card contains a small transmitter chip and an antenna that sends and receives radio frequencies to and from the card reader. Table 4.3 shows a comparison of smart card technologies.

Table 4.3
Comparing smart card technologies

Frequency	**13.56 MHz**	**13.56 MHz**	**125 kHz**
Standards	**ISO/IEC 14443**	**ISO/IEC 15693**	**None**
Read range	Up to 100 mm (3.94 in [20 to 30 mm (0.787 to 1.18 in) typical])	Up to 1 m (3.28 ft [60 to 80 mm (2.36 to 3.15 in) typical])	Up to 1 m (3.28 ft [60 to 80 mm (2.36 to 3.15 in) typical])
Memory capacity range	64 to 65 kB	256 bytes to 4 kB	8 to 256 bytes
Data transfer rate	Up to 848 kb/s	Up to 26.6 kb/s	Up to 4 kb/s
Read/write ability	Read/write	Read/write	Read/write
Mutual authentication	Challenge/response	Challenge/response	No

in = Inch
ISO/IEC = International Organization for Standardization/International Electrotechnical Commission
kB = Kilobyte
kb/s = Kilobit per second
kHz = Kilohertz
m = Meter
MHz = Megahertz
mm = Millimeter

 © 2012 BICSI®

Credentials (Level 4), continued

Smart card readers are usually mounted vertically on the surface of a wall. The card reader contains an antenna that propagates radio frequencies to and from the smart card. The reader emits electromagnetic energy that will energize the chip in the card when the card gets close to the electromagnetic field, causing it to transmit its identity (the number recorded in the card). The receiving circuit inside the reader decodes this transmission and forwards the card number to the access control panel.

Inside the smart card is another small chip. This chip has memory areas that can be written to and read from much like random access memory (RAM) on a computer. The smart card is essentially a read/write card. The most commonly used cards have a memory size of 256 to 2000 bytes of data. These smart cards are used in conjunction with special equipment that can write information to the application areas on the microchip and readers that can read the information. There also is equipment that can do both. This equipment is called a reader/writer.

There are various scenarios or applications for which these cards may be used. The simplest application is holding information. This could be personal information (e.g., a person's name, finger scan, address, telephone number). A more advanced application allows portable medical records to be written to the card, read from the card, and rewritten to the card.

For example, vending machines are often installed with smart card reader/writers. Instead of using cash to buy snacks, the amount of money on the card is debited. When the customer presents the smart card to the vending machine and makes a product selection, the vending machine reads the amount of money on the smart card. If the sufficient amount is on the card, the vending machine deducts the amount for the product from the total on the smart card and rewrites the new total on the card. The vending machine then vends the product.

Proximity Card

The proximity card works on a frequency lower than the smart cards. Proximity cards work at the frequency of 125 kilohertz (kHz). The operation of identifying the card's internal encoded number is the same as the smart card. Unlike the smart card, the proximity card has no memory and cannot have information written to it for storage.

Proximity cards and readers are often categorized by their read range. Read range is the maximum distance from the reader at which a card and tag may communicate, generally a function of the reader and tag antenna size. A larger antenna in relation to the overall size of the reader and tag usually provides a greater read range.

The size of proximity readers varies. The housing is typically made of plastic material and mounted on the wall surface.

The manufacturer providing the proximity readers for the ACS also should provide the proximity cards. The encoding process that occurs between the reader and the card is usually proprietary. For example, the proximity reader from manufacturer A will not read a proximity card from manufacturer B.

Credentials (Level 4), continued

Wiegand Card

The Wiegand card uses special wire that is inserted and molded in the plastic card. This creates two distinct magnetic regions in the same piece of wire when passed over a magnetic field provided by a Wiegand reader. These magnetic regions are separated based on the placement of the wires.

As the card passes through the Wiegand reader, magnetism passes through a coil in the reader. This burst of magnetic energy may be described as a pulse. Each pulse is translated to a digital 0 or 1, depending on magnetism. The wire is embedded in the card so that 0s and 1s create the individual code.

The card is usually black and made of molded plastic. A slot in the middle of the reader is used for card swiping. The reader may be surface mounted either vertically or horizontally.

Magnetic Stripe Card

The magnetic stripe card works on the same principle as the Wiegand card. The difference is that magnetic pulses pass through the card's black magnetic stripe instead of wires. Three strips or tracks are generally available to record the information. As the magnetic head from a reader writes to the magnetic stripe, it records the individual code (card number) directly on the card.

The magnetic stripe reader varies in size. The reader is usually mounted vertically and on the wall surface.

Bar Code Card

The bar code card has a series of black vertical lines. Bar codes are most commonly recognized for their use on universal product code (UPC) labels. The length of the black vertical lines is the same. The width of the lines and the width between the lines change. The reader usually consists of a scanner and a decoder. The scanner reads the lines and passes the information to the decoder. The decoder determines the width of the lines and spaces and translates them to numbers.

 © 2012 BICSI®

Credentials (Level 4), continued

Card Formats

Initially, access control cards were ordered for a specific location, and card manufacturers kept track of the locations to which the cards were shipped. As the popularity for access control increased, it became nearly impossible to provide cards without duplicating the encoded numbers as there are only a certain number of data bits (1s and 0s) available in each card format.

To limit the amount of duplicate numbers, a system was developed to segment the encoded numbers. Rather than increase the available number of data bits used to formulate each number, site codes were created to provide a larger quantity of cards available by duplicating card numbers.

In this system, an encoded number is separated into two segments. The two segments are the site code (or facility code) and the card number. These two segments are composed of a binary number, which is a series of 1s and 0s next to each other. The quantity of 1s and 0s determines how large the encoded number of the card can be. In other words, the more placeholders there are, the larger the encoded number.

The site code segment is made up of the most significant bits (or the placeholders with the most value). The placeholders are on the left side of the binary number. The card number segment is made up of the least significant bits (or the placeholders with the least value), which are on the right side of the binary number.

When a new ACS is installed in a location, it is given a site code that was not previously used in that area of the country. This method reduces memory requirements in the hardware because the control panel equipment does not have to store the site code in each of the encoded numbers as all of the cards on a site have the same site code.

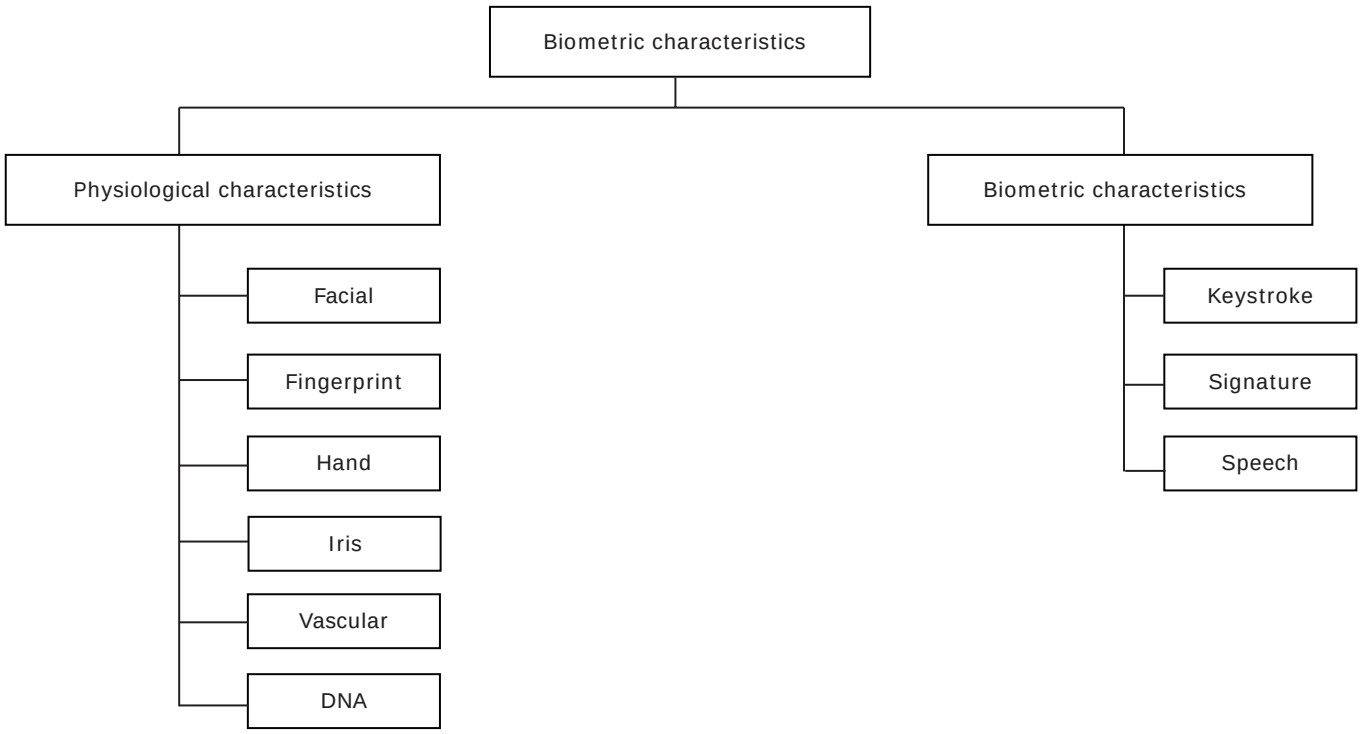
Credentials (Level 4), continued

Biometric Systems in Access Control

Biometrics is the field of technology devoted to identifying individuals using biological traits commonly referred to as "something they are." Biometric identification technologies collect and analyze unique human traits. These technologies use automated methods, comprising readers, processors, and powerful algorithms, to recognize an individual based on one or more physiological or behavioral characteristics (see Figure 4.13).

A sample is collected from a user, processed into a digital template, and stored for later comparisons. Biometrics can be used to verify the identity of an individual or to determine if a record of the person exists in a larger database.

Figure 4.13
Biometric characteristics



DNA = Deoxyribonucleic acid

 © 2012 BICSI®

Credentials (Level 4), continued

Physiological characteristics are related to the unique shape of the body, while behavioral characteristics directly relate to one's behavior (see Table 4.4).

Table 4.4
Personal identification biometric systems

	Iris Scans	Facial Recognition	Fingerprints	Hand Geometry	Speech Verification	Vascular Recognition
Description	A sensor analyzes the the unique features of the iris.	A still or video camera analyzes the geometry of the face, including relative distances between features like the nose and eyes.	Fingerprinting measures the dimensions of the fingertips.	Cameras measure the dimensions of the hand, including the shape and length of the fingers.	A microphone captures the voice and measures specific patterns, including pitch, cadence, and tone.	Passive infrared light analyzes patterns in the veins of the fingers, palms, and back of the hand.
Application Examples	Facility access, border security, and high-security areas.	Access to high-security areas, border security, military, and law enforcement.	Physical and network access control, background checks, and immigration and border control.	Access control to high-security facilities, including nuclear plants, airports, DoD facilities, and R&D testing facilities and laboratories.	Telephony applications to select and access financial accounts.	ATM transactions and data and command centers.

ATM = Automatic teller machine
DoD = Department of Defense
R&D = Research and development

Credentials (Level 4), continued

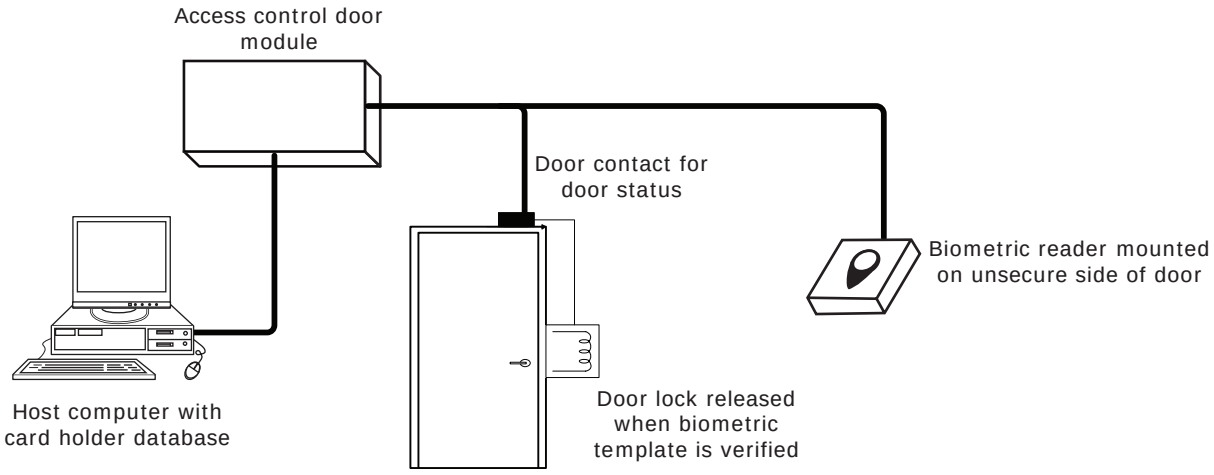
Figures 4.14 to 4.16 show a simple biometric system; the main operation of the system is enrollment and verification. During the enrollment phase, biometric information from an individual is collected and stored either on a smart card or in a secure database. During the verification phase, biometric information is collected and compared against templates stored in the database, on a smart card, or in another storage medium.

The systems can be designed to provide the following functions:

- Verification—This function authenticates its users from a combination of parameters, including PINs, user name, or identification numbers. This function matches the biometric template of the user against corresponding parameters, and if a match is detected, access can be granted.
- Identification—This function authenticates its users from the biometric characteristics alone without the use of any other matching parameters.

In Figure 4.14, the biometric template can reside either in the access control door module or on the smart card.

Figure 4.14
Biometrics in physical access control application

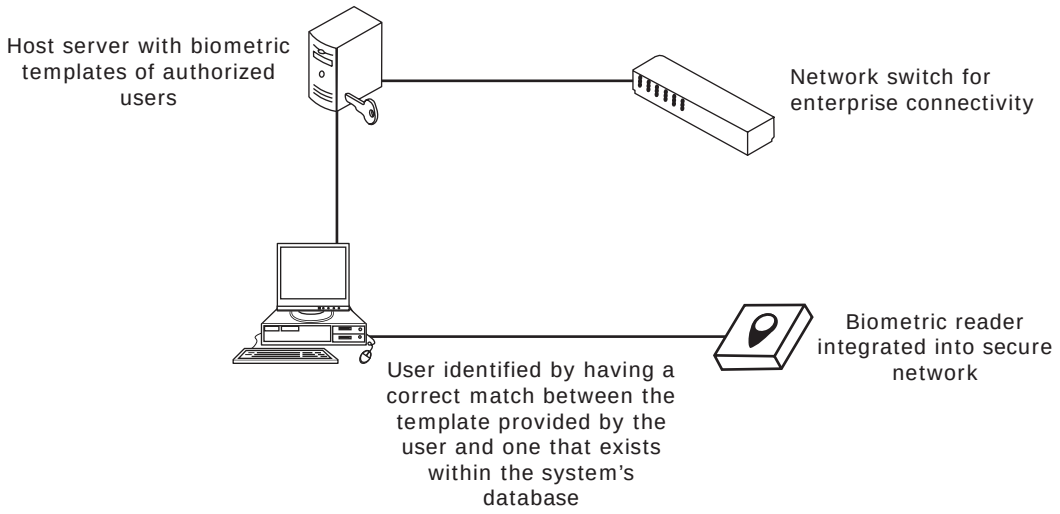


 © 2012 BICSI®

Credentials (Level 4), continued

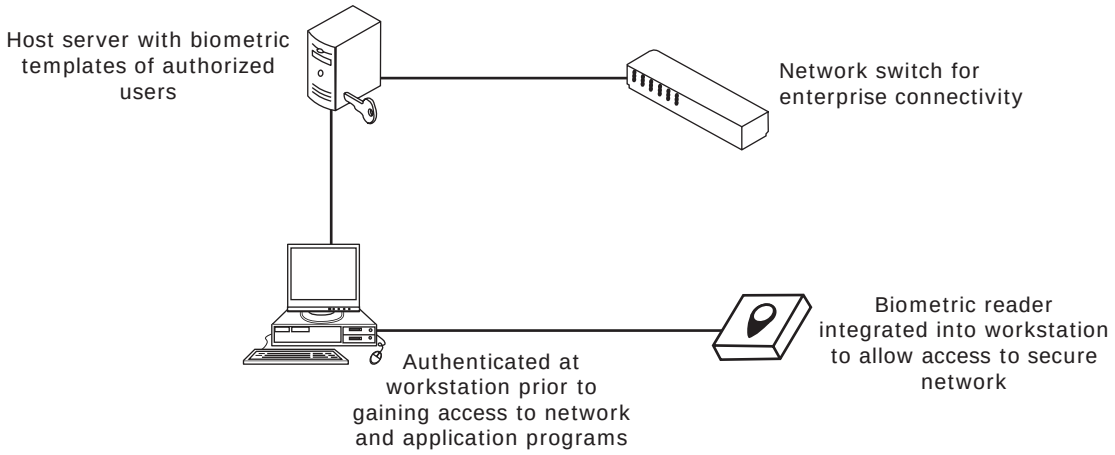
In Figure 4.15, the biometric template is stored on servers and verified against the user template prior to authenticating the user's identity.

Figure 4.15
Biometrics in user identification application



In Figure 4.16, the biometric template is stored on servers and verified against the user template prior to granting access to workstation or application programs.

Figure 4.16
Biometrics in logical access control application



Credentials (Level 4), continued

In an access control application, the smart card may hold a biometric template in the card. A biometric template is the result of an algorithm or formula from a biometric reader that analyzes the selected physical metric and translates special characteristics into coded information.

The coded information can be stored on the smart card instead of in a computer database to protect the privacy of the individual. The individual becomes the exclusive owner of the biometric information.

The biometric reader collects the token by prompting the subject to present the smart card (e.g., fingerprint) to the biometric reader. The reader reads the fingerprint, runs it through the algorithm, and compares this result with the coded fingerprint information written on the smart card. If they are the same, it sends a command to open the door.

Table 4.5 shows the data sizing requirements for various biometric applications.

Table 4.5
Sizing for biometric applications

Biometric Technology Type	Sample Template Size
Hand scan	9 bytes
Retina scan	96 bytes
Finger scan	250 bytes
Iris scan	512 bytes
Facial scan	1,300 bytes
Signature scan	1,500 bytes
Voice scan	2,000 bytes–10 kilobytes

 © 2012 BICSI®

Credentials (Level 4), continued

Biometric Performance Parameters

The effectiveness and overall reliability of a biometric system can be measured using the criteria listed in Table 4.6.

Table 4.6
Biometric performance parameters

Parameters	Description
FAR or FMR	The probability that the system incorrectly declares a successful match between the input template and one stored in the database when the input is not in the database.
FRR or FNMR	The probability that the system incorrectly declares a nonmatch between the input template and a matching template stored in the database.
EER	The rate at which both accept and reject errors are equal. The lower the EER, the more accurate the system is considered to be.
FER	The percentage of templates not registered by the system because of a faulty sensor, resulting in poor quality of the templates captured or damage to the characteristics required by that particular biometric system/device.
FTC	The probability that the system fails to detect a biometric template when presented by an authorized user.
Throughput	One issue that must be considered in any biometric system is the throughput rate of users. Throughput of a biometric system is the time it takes for a person to use the device until a result is provided by that device. The elapsed time from presentation to identity verification is the "verification time" and typically runs two to four seconds for most systems. If a PIN is part of the identity process, then the verification time could be longer and must be considered in the design process.

EER = Equal error rate
FAR = False acceptance rate
FER = Failure to enroll rate
FMR = False match rate
FNMR = False nonmatch rate
FRR = False rejection rate
FTC = Failure to capture
PIN = Personal identification number

Credentials (Level 4), continued

Privacy and Other Concerns

Biometric identification systems are increasingly being used to provide logical and physical access to various forms of government-issued credentials, including driver's licenses, passports, and frequent flyer identification cards. The increase in the use and acceptance of biometric technology has raised some concerns, including:

- Companies might collect and sell biometric data the same way they sell e-mail addresses and telephone numbers.
- A government-owned biometric database could be built that contains vital information about its citizens to be used for both good as well as nefarious purposes.
- Biometric templates could be manipulated and used without the owner's consent or knowledge.

In addition to the potential for an invasion of privacy, some critics have raised several concerns about biometrics and the systems they foster, including:

- Over reliance—The perception that biometric systems are foolproof might lead to a false sense of security.
- Accessibility—Some systems cannot be adapted for certain segments of the population (e.g., those with a disability, the elderly).
- Interoperability—In emergency situations, agencies using different systems may need to share data, and valuable time can be lost if the systems cannot communicate with each other.

As the use of biometric systems increases, user acceptance will be central to their success. Several factors have an impact on acceptance:

- The device must cause no discomfort or concern to the user.
- The system must be easy to use.
- The system must be intuitive.
- The system must have a high rate of reliability; that is, it must work.

A well-designed and operational biometric system accomplishes two things—it keeps unauthorized people out and allows authorized people in to a protected facility.

 © 2012 BICSI®

Design Considerations

Access Control Integration

There are no widely adopted standards associated with ACS. While cabling standards enable interoperability between multiple cabling component vendor solutions, the same is not true for ACS. ACS manufacturers have proprietary components that, in spite of transmitting data using industry standard protocols, do not work together (e.g., not all peripheral devices work with all door controllers). A complete system solution is required to ensure functionality and compatibility.

The only form of standard that does exist is card readers and accompanying credentials that have become more interoperable. The specifics for these technologies are discussed in greater detail later in the card format section in this chapter.

Similar to other technology-based industries, manufacturers of ACS have selected dealers and business alliances that often are referred to as system integrators or security contractors. Furthermore, manufacturers often limit the number of dealers in a particular market. This is a critical distinction in understanding the basic relationship within the ACS industry.

Vendors who are not the authorized dealers for a specific system cannot procure or provide a full warranty on the hardware. All parties must consider these factors during the product installation decision-making process. They must understand that by choosing a specific product, an installing and servicing dealer also is selected. The selected dealer will be the main point of contact for the system's service, move, add, or change (MAC). Changing dealers may require a change in system components, which often can be cost prohibitive.

Some suggested elements for evaluation when qualifying dealers include:

- Number of technicians.
- Number of trained engineers.
- Number of similar installations.
- Average incident and service request response time.
- Verifiable references.
- Service parts inventory.

Occupants

The ESS designer will encounter many situations that require electrical locking hardware. ESS designers should be aware of the life safety implications of installing locking doors inside and on the perimeter of a facility. Impeding the occupant egress under all conditions will result in reducing the safety of building occupants. Once a locking scheme is selected, the method of access should be considered.

Occupants, continued

Families of codes apply to any given facility. (Codes are discussed in greater detail in Appendix A: Codes, Standards, Regulations, and Organizations.) These codes will describe the types of:

- Fire rating.
- Egress requirements.
- Locations.
- Criteria for employing electrical locking hardware.

The ESS designer should be aware that unsuitable applications of locking hardware may compromise the safety of building occupants, void the client's insurance protection, and ultimately fail the ESS designer's conceptual goals.

Occupants may include clients, tenants, contractors, visitors, cleaning crews, security personnel, and any others in the facility, whether permitted or not. For example, a federal courthouse building, prison, and hospital all require ACS, but the systems requirements vary greatly based on the people involved. A thorough understanding of the occupants and how they use the facility is required to properly design the ACS.

An ACS allows several levels of security. Once the number and type of people are determined, a user or access level should be established for each person. Access levels are incorporated into the system integration and determine the areas of access. Factors affecting the user level include security clearances, job title, rank, and employee type. The access level is determined by the building's physical layout and directly related to the doors and other portals they control.

Assets

Assets have many forms. Tangible assets include cash, bonds, materials, pharmaceuticals, weapons, and other items that are at risk of being stolen or compromised. Property assets include real estate, offices, land tracts, individual rooms, and any space where control must be maintained. Assets also include intangible information assets and other confidential information that, if stolen, could harm the client (e.g., sales projections, marketing plans, financial data, personnel records, trade secrets). Other important assets that also could be harmed by a security event are the client's employees, reputation, and perceived level of security.

The assets within a building often are as important to control as the people who enter them. Pharmacies, armories, mailrooms, nurseries, storage rooms, and loading docks are prime examples of these. The type of assets and threat levels should be determined and reviewed for incorporation into the ACS.

In some cases, an asset protection system is the best solution (e.g., nurseries with infant abduction prevention systems, retail stores with radio or RFID tags). These types of systems are covered elsewhere in this manual. In other situations, the best solution is to control the access of unauthorized personnel to those assets. In those cases, the location of these assets should be noted and considered when developing the ACS and the access level matrix.

 © 2012 BICSI®

Vehicles and Parking

Access to parking lots is often controlled. Ample public space should be available if the lot gates are controlled with card access control, key codes, or automatic gate openers. Access also may be controlled through remote operator switches as part of security consoles with video display.

In case of fire, emergency vehicles require access to the entire building perimeter; therefore, emergency situations should be considered during the ACS design (e.g., fire alarm interfaces).

Access Level Matrix

After all of the spaces are identified, the doors marked for access control, and the system installed, the system is still not operationally complete. The personnel who will utilize the space still need to be granted access to the building, but only for the permissible parts of the building and particular times and days. This matrix, which identifies and groups the various spaces and doors together and then links them to employee types (and ultimately individual employees), is known as the access level matrix.

This graded level of security protection is based on the threat assessment and the specific user requirements. No building has the same situations and levels of access as another building, so no process will work for all buildings. Table 4.7 and Figure 4.17 demonstrate how access levels are determined and who is granted access.

The access level matrix (see Table 4.7) links employees with the doors that lead to the spaces they are permitted to access (see Figure 4.17). In addition, a time schedule is included since access to some areas is permitted during regular business hours or only after hours. This matrix is used to assign each person permitted in the building a specific level of access. The size and complexity of such a matrix depend on the type and size of the facility.

Access Level Matrix, continued

Table 4.7
Access level matrix

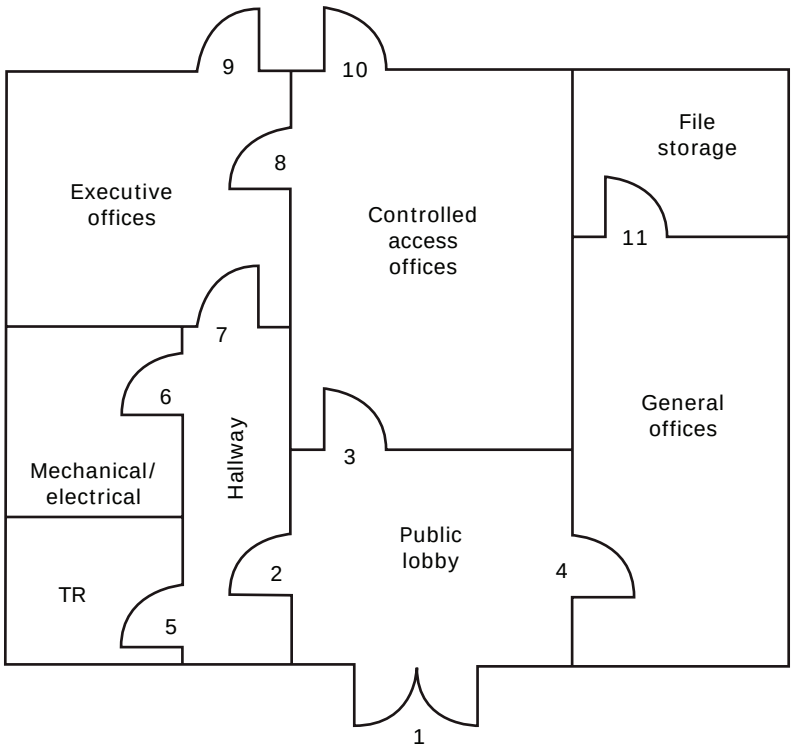
Door		1	2	3	4	5	6	7	8	9	10	11
Access Level	Time Schedule	Front Entrance	Hallway Entrance	Controlled Office Entrance	General Office Entrance	Telecommunications Room	Mechanical/Electrical Room	Executive Offices	Executive Office Inside Door	Executive Office Read Door	Controlled Office Fire Exit Only	HR File Storage
General employee	8a-5p	X			X							
Executive	24 h	X	X	X	X	X	X	X	X	X		X
HR employee	8a-5p	X			X							X
HR director	24 h	X			X							X
IT personnel	24 h	X	X		X	X						
Maintenance	24 h	X	X		X		X					
Cleaning crew	6p-12a	X	X		X							
Temporary employee	8a-5p	X		X	X							
Visitor	8a-5p	X			X							

h = Hour
HR = Human resources
IT = Information technology

 © 2012 BICSI®

Access Level Matrix, continued

Figure 4.17
Example of access control system floor plan



TR = Telecommunications room

System Failures

In addition to determining the system's operational requirements, documenting performance requirements in both normal modes and degraded modes of operation is needed.

An ESS designer must consider critical aspects of a system in a degraded mode of operation, including:

- Physical properties of electronics equipment.
- Primary equipment power.
- Software.
- System cabling.

Types of failure that may be encountered in a system's degraded mode of operation are:

- ACS server failure.
- Cabling failure.
- Communications failure.
- Card reader failure.
- Power failure.

A set of design steps can help minimize the effects of one or multiple simultaneous failures until the system is restored to full operation.

Design verification is based on the installation of the system and the following determinations:

- Verify if UPS power is provided at the controllers.
- Verify if UPS power is provided at the server.
- Verify if emergency power is available.
- Verify if the ACS doors are equipped with physical key locks for use without power.

Other design steps vary with the system type and manufacturer and are based on the following determinations:

- Verify if system redundant servers are required.
- Verify if the door controllers act in a stand-alone mode after the loss of signal from the main controller or server.
- Verify if the card reader will allow for a PIN code override in the event of card reader failure.
- Verify if the cabling system is supervised, notifying the administrator in the event of failure.

 © 2012 BICSI®

Building Codes

ESS designers must be aware of all local AHJ codes and other requirements pertaining to the design of the ACS. ESS designers must understand how the ACS are coordinated with, integrated with, and possibly overridden by fire alarm, heating, ventilation, and building automation systems (BAS) as well as how local AHJ requirements may dictate what, how, and where devices need to be installed.

Only a few codes and standards (e.g., NFPA 730 and 731) pertain to the location and selection of access control devices. When local codes do not state that an ACS is required, the ESS designer must determine the extent of the system and what regulations need to be followed.

Notification Requirements

If an individual does not monitor the system continuously, automatic notification may be useful. Such a system would notify the responsible parties of any events in the ACS.

Some notification methods include:

- Automatic e-mail.
- Audible or visual alarm.
- Workstation window pop-up.
- Digital communicator.
- Pager (telephone or text).

Communications

Serial Communications

In a hardwired copper system configuration, the host computer communicates to the control panels through one of its serial or communications ports using the RS-232 communication protocol. An RS-232 to RS-485 converter may be used to convert the RS-232 signal to an RS-485 signal. The converter must be located within 15.2 m (50 ft) of the host computer. This conversion to RS-485 may be preferred because of a distance limitation on the communication between the devices using RS-232 (15.2 m [50 ft] compared to 610+ m [1968+ ft] with the RS-485 protocol).

This first control panel also can communicate to other control panels through the RS-485 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.

Optical Fiber for Extended Distances

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.

Analog Communications

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.

 © 2012 BICSI®

Transmission Control Protocol / Internet Protocol (TCP / IP) or Network Communications

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.

Databases

Some access control manufacturers develop their own database technologies, while other manufacturers use third-party databases that are open database connectivity (ODBC) compliant. An advantage of this approach is compatibility with the customer's databases. An ACS database must be flexible and easily searchable. Most databases support keyword searching, allowing a person to enter terms in a search box. Most databases allow one search field, but some may combine several fields. An ACS database also should be relational. Several fields may need to be combined in a search to find a common denominator or generate a report.

Another important feature to consider when using databases is the ease of data entry or edits. A database that enables all data entry in a single window is the best choice. Such databases assist quicker data input and limit confusion and missing important fields. Editing features (e.g., spelling and grammar, find and replace, copy and paste) help to ensure that the information is entered correctly.

The database also should have import and export capabilities in multiple formats for programs like Microsoft® Excel®, Access®, and FoxPro® to ensure integration with other security equipment. Selecting a versatile database enhances the value of the ACS. Such a centralized system allows other systems to connect and be accessed from a single point. Multiple reports can be run from a single system and used to synchronize events, assist in investigations, or troubleshoot problems.

Local Database

An ACS uses either a local database or a distributed database in processing events gathered by the control panels. The following describes the differences between the local and distributed databases.

The credential or user database contains the name of the user, the location accessed, and the time of the access. This information often is called access-level profile. In a local database system, the decision to allow or deny access is made at the host computer where the database is stored.

Databases, continued

For example, the reader passes the credential information to the control panel. The control panel then passes the credential information, the time, and the reader's location to the host computer. The host computer first verifies that the credential is in the database and then checks its validity by matching up the access level to the reader. The final check ensures that the access level was valid for the reader at the particular time. If the credential is valid, the host computer sends a command to the control panel to open the door.

Such local configuration is currently uncommon. It would take too long by today's standards for the host computer to check the information, send the control panel the command, and then execute the proper locking or unlocking task. This configuration used to be a popular method of avoiding the high cost of holding large amounts of memory at each controller. It was less expensive to store a database in one location than in every controller. At present, the price of memory is relatively inexpensive, thus holding a credential database in each controller is not a concern.

Distributed Database

In a distributed database configuration, the control panel makes the decision to allow or deny access because the access level profile or credential database resides in the control panel. The control panel microprocessor checks its local database when a credential is presented to the reader. If all access-level criteria are met, the control panel grants access without checking with the host computer.

A distributed database is spread out among the control panels. The user's access level profile information is saved in the nonvolatile memory of the control panel that grants access to any reader the person is allowed to access. If a person is not authorized to access a particular area, that person's access-level profile information is not stored in the control panel protecting that area. It is distributed only to control panels protecting the areas the person is allowed to access.

In the distributed configuration, if communication cannot be established with the host computer, no interruption occurs in the system functionality. The control panel continues processing transactions and opens the door accordingly. The transaction information is held in the control panel's memory until communication is reestablished with the host computer. When communication is reestablished, the transactions, events, and any alarms that were in the control panel's temporary memory are uploaded to the host computer for archiving.

 © 2012 BICSI®

Integration

Advances in computer software and technology have enabled integration of various security systems. Integrating systems allows one system to respond to a particular event from another system electronically and automatically.

The key benefit of security system integration is that the system administrator or security guard can monitor all alarm points, events, and activities on one display, which allows a more effective use of resources and space.

It is common to find the following systems integrating with access control:

- Fire notification (secondary notification only)
- Surveillance
- Time and attendance
- Intercom
- Photo identification badging
- Paging
- Intrusion detection
- BAS (e.g., data communication protocol for building automation and control network [BACnet®], LonWorks®, object linking and embedding [OLE] for process control [OPC]) for control of lighting, HVAC, and similar systems
- Fire alarm control panel and surveillance (e.g., analog and digital connections)
- Elevator systems

Integration relies on complex software that brings together equally complex subsystems. The integration of dissimilar building systems (e.g., fire and security systems) generally requires that software be written to tie them together. An access control manufacturer usually develops software that would interface with the third-party equipment so that the systems would communicate with each other. An access control manufacturer generally requires purchasing additional licenses for each system or user that needs access.

The company installing the ACS typically installs the integration software. Companies that install such complex systems are called security integrators. Security integrators usually sell and install security equipment from multiple vendors and are experienced in establishing communication among multiple systems. Integrators test the systems to ensure functional communication. Integrators ensure that the events or alarms pass between the systems and trigger the correct action or output.

Complex security systems involving integration require that the security integrator provide appropriate training to the client. The training should cover how all the systems work both independently and together, what the various screens look like, what alarms may be triggered, and how to respond to them appropriately.

System Programming

Overview

Programming an ACS requires a thorough understanding of the system, the facility in which it is installed, and the needs of the customer. The starting point is a thorough review of the ACS drawings, which indicate all of the access control points in the facility.

A master configuration list has to be made for the facility and specific items that are relevant to each specific access point checked off. The list should be divided into three sections:

- Configuration
- Event
- Alarm/status

The configuration encompasses specific attributes of each point of access. The following information may be included:

- Single or double door
- Card reader
- PIN code pad
- REX device
- Magnetic contact
- Magnetic starter (for motors)
- Magnetic lock
- Electric lock
- Emergency exit
- Hardware

 © 2012 BICSI®

Overview, continued

Each configuration is then linked and cross-referenced to specific events. Some common events include the following:

- Authorized card—When a valid card is presented, the central system logs the event and approves unlock.
- Undefined card—When a card that is not in the system is presented, the central system logs the event, disapproves unlock, and reports alarm.
- Invalid area.
- Invalid time period.
- Expired card.
- Inactive card.
- Passback attempt.
- Reader tamper.
- Invalid facility code.
- Door restore (when a door has been closed).
- Door open detect alarm (when a door is open longer than the programmed entry time).
- Invalid PIN code.
- Duress PIN code—When a code for specific duress condition is entered, the central station logs the transaction, approves unlock, and initiates alarm at central station.
- Forced door alarm—When a door has been opened without a valid card or PIN, the central system logs the event and initiates alarm at central station.

Finally, each configuration and event has a corresponding alarm/status signal. The central system may:

- Log the event.
- Approve unlock.
- Disapprove unlock.
- Report an alarm.
- Indicate door status.
- Disapprove operator cycle.

The next step in the process for an ESS designer is to consult with the customer and obtain a complete roster of all personnel granted access to the facility. This list is then annotated with information regarding specific access points that may be used, the day of the week, the time period that access is valid, and any other relevant information. This information may then be organized into various common groupings, which are then used to assign various levels of access to different groups of individuals. All of this information is assembled into an access level matrix for the facility and its personnel.

Overview, continued

A report writer application function needs to be established to properly log, time, and date stamp all of the various events and generate reports of access that can be used to monitor the personnel flow in and out of the facility. An ESS designer also should make appropriate provisions in the system for emergencies so that egress of personnel from the facility during an emergency is not hindered and rapid access is enabled to emergency personnel. The security and emergency response personnel at the facility define the facility strategy with local emergency response departments in the municipality.

When programming is completed, all of the various possible events at each access point should be reviewed with the customer to ensure that all possible combinations of events have been considered. The access level matrix should then be carefully reviewed with the customer to ensure that the proper access levels are granted to each person given the cards or permitted the use of PINs.

Certain personnel are granted the right to escort visitors, or a separate visitor management system may be implemented. Attention to detail is critical in programming an ACS that meets all of the requirements a customer has for the facility and its personnel.

Database Conversion / Transportation

Any new installation of an ACS may require importing large amounts of data. This task may be accomplished in several ways. If the installation involves a new system, each card should be entered, and if the cards also are identification badges, the identification photos are required.

Attention to this detail in preplanning makes the process start smoother. With the digital cameras and the ability to download pictures to a computer, pictures can be taken at the times and locations convenient for employees.

If the installation is a retrofit of an existing system, providing a means to import the existing picture files and database reduces the overall workload of the process start considerably. An old database table configuration is likely to be different from a new table. Some programs allow the user to import or append records in a database. In most cases, the old database allows the user to export the data to a text file to read into the new database.

Picture files are typically standard file formats (e.g., Joint Photographic Experts Group [JPEG], graphic interchange format), with a few exceptions. Before committing to importing existing picture files, an ESS designer should confirm the format, overall quality, and age of the picture files.

 © 2012 BICSI®

Data Entry

An ESS designer should confirm the levels of access for groups and individuals early in the process. An administrator or supervisor typically has access to the entire system while other employees are granted access based on the business need and respective job functions. This is part of the required programming.

As previously described, information provided during the system design review should be entered at this time, including:

- Access levels.
- Time zones.
- Access groups.
- Employee information:
  - Name
  - Address
  - Telephone number
  - Department
  - Start date

Report Generation

An ESS designer should set aside time to meet with the client and to define useful reports based on the information in the card access system. These reports may range from reports that can be displayed on the screen to reports that can be printed out on a local or network printer. The complexity of these reports is limited by the report generation software provided by the system manufacturer. Most systems come with a variety of predefined reports that fill most customer needs.

Some of the reports the customer may ask for are:

- Time in and out by door and employee.
- Time and attendance reports.
- List of all employees and contractors.
- Muster reports.

System Verification Testing and Startup

The access control hardware and software installation must be inspected both visually and electrically. The verification process is commonly referred to as commissioning.

The items most commonly subject to verification during commissioning ensure that:

- The system has been installed in accordance with specifications and drawings and follows manufacturer's recommendations.
- Record drawings are completed and turned over to the architect and engineer for use during testing.
- All test reports called for are handed over to architect and engineer for review.
- Headend equipment and intermediate access control equipment are installed as called for 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. They must be kept separately from the other devices housed in the equipment room.
- All cabinets are clean inside.
- Card reader licenses have been provided for the specified number of personnel, readers, and badgers.
- Access control matrix has been developed, and all information has been properly programmed at the access points and their respective card readers.
- Directories for each panel, listing the card reader interface slot locations, names, and utilized channels, are provided.
- All low-voltage security and access control cables are installed in conduit, boxes, and locked enclosures when required and meet all applicable codes.
- All enclosures, panels, card readers, and keypads are properly labeled.
- All cable and termination points are properly labeled. Tag numbers on record drawings also should be provided.
- All door position switches are located on the open side of the door at the top, not on the hinge side.
- All door hardware is properly installed and meets all manufacturer requirements for installation.
- All power supplies are hardwired. Plugs should not be used, unless called out in the drawings or specifications.
- A fire alarm interface to the ACS and alarm points meeting NRTL approval requirements is provided. Upon fire alarm notification, the doors in the fire alarm zone and adjacent areas must be fail-safe. Proper fire alarm input ports should be assigned to the card reader and door contacts to activate the magnetic lock to an REX condition.

 © 2012 BICSI®

System Verification Testing and Startup, continued

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 a fire alarm condition and verifying that all fail-safe doors open properly upon contacting the central station and fire alarm respondents. An ESS designer should verify that all door open/closed status conditions are properly represented in the system.
- 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, REX) 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.

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 ACS 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.

System Training

Overview

An ACS is a valuable part of the overall security solution. Many other systems depend on proper utilization and operation of the ACS. Therefore, the users should know how to use the entire system properly.

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 ESS design may affect the system's operation.

Most ACS 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.

The ACS users may be divided by different roles or job requirements into:

- System administrators.
- System operators.
- Managers.
- IT staff.
- Maintenance personnel.

 © 2012 BICSI®

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.

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.

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.

Information Technology (IT) Staff

This training course generally focuses on IT department personnel who need to know how the ACS connects to the LAN or wide area network (WAN). The bandwidth and other items, including data requirements, are discussed as well as:

- Network topologies.
- Communication to each control panel.
- Encryption strategies and capabilities.

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.

ACS 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.

 © 2012 BICSI®

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 ACS 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. In case of many ACS, the administrator screens should be programmed before the operator screens to facilitate the programming flow. Cross training between the various roles is recommended.



Chapter 5
Video Surveillance Systems

Chapter 5 provides an overview of video surveillance fundamentals and the technology, design, and operation of a security surveillance program. Designing with a perspective-oriented approach is discussed along with design challenges, including privacy issues and government regulations.

Table of Contents

Video Surveillance Systems (VSS) 5-1
Introduction 5-1
Video Surveillance Systems (VSS) by Function 5-3
Privacy, Liability, and Legal Considerations 5-4
Video Surveillance Systems (VSS) Components 5-7
Analog Video Systems Overview 5-8
Internet Protocol (IP) Video Systems Overview 5-8
Image Capture / Video Sources 5-11
Cameras 5-11
Analog Video Camera 5-12
Internet Protocol (IP) Video Camera 5-14
Internet Protocol (IP) Video Encoders 5-17
Compression Technology Overview 5-18
Overview of Imager Resolutions 5-20
Camera and Image Capture Types 5-22
License Plate Capture (LPC) Cameras 5-22
Recognition Devices 5-22
Color versus Monochrome or Black and White Cameras 5-22
Cameras with True Day/Night Capability 5-22
Cameras with Noninfrared-Sensitive Day/Night Capability or Chroma Mode Capability 5-23
Infrared (IR) Cameras 5-23
Thermal Cameras 5-23
Film Cameras 5-23
Imagers 5-23
Charge-Coupled Device (CCD) versus Complementary Metal-Oxide-Semiconductor (CMOS) 5-24
Frame Interline Transfer (FIT) Charge-Coupled Device (CCD) 5-24
Progressive Scan Charge-Coupled Device (CCD) 5-24
Image Processing 5-25
Video Motion Detection (VMD), Advanced Video Motion Detection (AVMD), and Automatic Tracking 5-26
Lenses 5-28
Lens Formats 5-28
Lens Features 5-29
Lens Types 5-29

Mounting and Housing 5-34
Lighting 5-35
Luminance and Lighting 5-35
Color Temperature 5-36
Color Rendition Index (CRI) 5-38
Infrared (IR) Illumination 5-38
Imaging and Resolution 5-39
Pixels, Imager Sizes, and Sensitivity 5-42

Transmission 5-43
Principles 5-43
General 5-45
Analog-to-Digital (A/D) Process (Non-Internet Protocol [IP]) 5-45
Copper Cable Types 5-46
Unbalanced (Coaxial) Cables 5-46
Balanced Shielded and Unshielded (Twisted-Pair) Cables 5-48
Optical Fiber Cable 5-48
Fundamental System 5-49
Link Loss Budget 5-50
Wireless Transmission 5-52
Radio Frequency (RF) Transmission 5-52
Free Space Optics (FSO) 5-52
Licensed Microwave Radio Transmission 5-52
Best Practices for Internet Protocol (IP)-Based Video Deployment 5-53

Processing 5-56
Surveillance Matrix 5-56
Multiview Processor 5-56
Video Analytics and Automated Object Detection 5-57
Data Mining and Video Analysis 5-57

Recording 5-60
Analog Recording 5-60
Digital Video Recording 5-61
Digital Video Recorders (DVRs) 5-62
Network Video Recorders (NVRs) 5-62
Video Storage Design 5-64
Video Storage Calculation 5-65

 © 2012 BICSI®

Monitoring Devices 5-67
Monitor Location Methodology 5-68
Video Surveillance Systems (VSS) Layout and Distribution Concept 5-69
Software as a Service (SaaS) or Application Service Provider (ASP) 5-76
Hardware Control System 5-76
Digital Matrix 5-76
Digital Video Management System (DVMS) 5-77
Step-by-Step Approach to System Selection and Deployment. 5-78

Support Infrastructure 5-85
Conditioned Space 5-85
Power Source 5-86
Power Distribution. 5-86
Surge Protection and Lightning Arrestors 5-86
Bonding and Grounding (Earthing) 5-87
Alternate Power Source 5-87
Pathways 5-87
Other Support Elements 5-87

Video Surveillance Systems (VSS) Interoperability Methods and Practices 5-88
Best Practices in Video Deployment. 5-88
Managing the Video System 5-90

Common Terminology 5-91
Internet Protocol (IP) or Network Video 5-91
Video over Internet Protocol (IP) 5-91
Network Video (Internet Protocol [IP]) Camera 5-91
Multichannel Video Encoder. 5-91
Video Decoder 5-91
Network Disk Recorder or Network Video Recorder 5-92
Network Video Recording Server 5-92
Unicast versus Multicast Video Streams 5-92
Structured Cabling and Ethernet Protocol. 5-92
Layer 2 and Layer 3 Switches and Routers 5-92
Imaging and Compression Features. 5-93
Progressive Scan Imaging. 5-93
Megapixel Imaging. 5-93
Back Focus—Automatic. 5-93

Figures

Figure 5.1 Analog camera components 5-12
Figure 5.2 Internet protocol video camera components 5-14
Figure 5.3 Internet protocol camera with analytics 5-15
Figure 5.4 Charge-coupled device imagers and lens compatibility 5-28
Figure 5.5 300 Millimeter lens at f/8 5-33
Figure 5.6 300 Millimeter lens at f/2.8 5-33
Figure 5.7 300 Millimeter lens at f/2.8 5-33
Figure 5.8 Comparison of total reflectance between asphalt and concrete 5-35
Figure 5.9 National Television System Committee waveform 5-43
Figure 5.10 Analog system without matrix switch 5-70
Figure 5.11 Analog system with matrix switch 5-71
Figure 5.12 Internet protocol video system embedded recording 5-72
Figure 5.13 Network video system for point of sale applications 5-73
Figure 5.14 Hybrid Internet protocol video system with recording server 5-74
Figure 5.15 Remote network video monitoring system using software as a service . . 5-75

Tables

Table 5.1 Internet protocol and analog video comparison 5-9
Table 5.2 Image formats and sizes 5-20
Table 5.3 Types of lenses 5-29
Table 5.4 Stop and brightness chart 5-31
Table 5.5 Color temperature 5-36
Table 5.6 Light sources and their behavior 5-37
Table 5.7 Color rendition 5-38
Table 5.8 International Organization for Standardization resolution chart 5-39
Table 5.9 Surveillance video function/resolution/maximum field of view 5-41
Table 5.10 Typical coaxial cable signal losses 5-47
Table 5.11 Frame size estimates 5-65

 © 2012 BICSI®

Examples

Example 5.1 Optical fiber performance calculations worksheet 5-51

Video Surveillance Systems (VSS)

Introduction

This chapter provides an overview of video surveillance fundamentals and is a reference for best practices. It is not intended to be a comprehensive video surveillance design guide. As with all security solutions, a formal risk and vulnerability assessment and security master program is required to analyze and define the design criteria for a specific video surveillance application.

In the past, video surveillance was defined as a self-contained, closed-circuit or electrical path carrying video signals from source to recorder, control systems, and on to monitor for viewing. It commonly was referred to as a closed-circuit TV (CCTV) system. Currently, video surveillance systems (VSS) are called analog video surveillance or Internet protocol (IP) video surveillance to indicate their use of conventional or network-based connectivity.

In this chapter, the term video surveillance refers to both analog and IP VSS. Where unique discussions exist, each system is identified as either analog video or IP video.

The electronic safety and security (ESS) designer must take a perspective-oriented approach in order to provide a system design that meets the requirements of the roles and responsibilities listed below:

- Designer—To the security system designer, the video-based security or surveillance system should meet the end user's expectations at the best value. The system should be simple to maintain and provide years of service if maintained properly.
- Physical security management—Image quality is of key importance to the end user whether the system is used for forensic review or for real-time surveillance. Ease of personnel and object identification in both the recording review and general surveillance under a wide variety of lighting and environmental conditions are important issues that must be addressed by the ESS designer.
- Information technology (IT) professional—Compliance with a variety of common protocols is essential, including dynamic host configuration protocol (DHCP), Institute of Electrical and Electronics Engineers, Inc.® (IEEE®) 802.3at (power over Ethernet [PoE]), IEEE 802.1x (port authentication), and IP version 6 (IPv6). Efficient bandwidth usage is important, especially where it is at a premium, (e.g., wide area network [WAN] services).
- Surveillance professional—Users prioritize real-time viewing instead of forensic recording. For example, camera operators require fast-acting and smooth, positionable camera controls using either a camera controller or a computer keyboard and mouse. Ease of use, multiscreen views, and video management add to the effectiveness of a properly designed surveillance system.
- Loss prevention—Similar to the surveillance professional, camera control with fast response is a requirement as individuals need be tracked as they walk around the space. An interface to transaction systems links video clips to key events such as activities occurring at a cash register.

Introduction, continued

- Safety and operations—The use of video to increase safety and enhance operations is a key function of organization operation and often can be the driver behind a video surveillance security system deployment. These users require metrics and dashboards that indicate safety incidents over time and suggested allocation of resources as well as documented return on investment (ROI).
- Security contractor—Ease of installation, upgrade, and maintenance are key drivers for the security contractor, reseller, or integrator. Systems that integrate seamlessly as standard products are important.
- Surveillance system devices manufacturer—To the surveillance component manufacturer, surveillance products need to be appealing to end users and resellers in multiple market sectors to ensure product line continuity and compatibility. Often on a three-year product cycle, the manufacturer must plan on various upgrades to the individual products to keep them competitive.
- Infrastructure manufacturer—For the manufacturers of network switches, midspan and power injection devices, video storage medium, transport medium, processing and display devices. Surveillance systems and components are manufactured by a wide cross section of companies. The ability for interoperability as part of any system configuration is of utmost importance when designing a functional surveillance system.
- Surveillance standards—To ensure integration and interoperability, there are standards with which surveillance systems must be in compliance. This allows different manufacturers' devices to seamlessly operate on a single surveillance platform. The use of IEEE 802.3at (PoE) power sourcing equipment (PSE) with compliant powered devices (PD) are one such standard in use to power surveillance cameras.

 © 2012 BICSI®

Video Surveillance Systems (VSS) by Function

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.

Determining the primary function of the VSS is the first and most critical step in the security system design process. The cameras and recorders should be matched properly to the user's 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.

The first three applications—observation, investigation, and recognition—also represent general classifications that are often associated with resolution guidelines. For example, the ability for a VSS to automatically recognize the details of a human face will depend on the system's image capture devices or the camera's resolution, often measured in TV lines (TVL), pixels per foot (PPF), or ideally both. The resolution requirements of the recognition application can often be twice as that of observation.

Forensic analysis requires that a greater emphasis be placed on recording as much as possible with as many high-resolution cameras as possible.

Access control systems (ACS) can use specific video cameras for face shots at entrances and allow for direct video verification of the actual credential holder. A number of access control devices, especially biometric readers, offer an optional surveillance camera for the sole purpose of recording video of the access control event for verification and later forensic audit and review.

Video analytics, automated object detection, and video analysis are essential features for the VSS used as intrusion detection, safety, or operations management. Automating the object detection and recognition process is becoming an integrated requirement and must be considered in the initial system selection and design process.

Video Surveillance Systems (VSS) by Function, continued

Surveillance technology trends have been driven by a number of markets, associations, and trade shows. Some of these include the consumer electronics, professional broadcast, data transport, audiovisual, IT, and security markets. Surveillance devices on a corporate or public network are more commonly used. Many best practices for system deployment are centered on the coordination with IT professionals and the management of shared networks.

The high payload of video data, especially in areas with asymmetrical WAN connectivity, creates challenges for the end user wishing to take advantage of security and IT convergence. However, for many users, it is necessary to deploy IP cameras and network video recorders so that valuable video information may be shared on standard Ethernet infrastructure.

Privacy, Liability, and Legal Considerations

ESS receives noticeable attention with regard to privacy rights, particularly with the increasing use of VSS. The legalities of surveillance and privacy are rooted in case law, which varies from country to country and must be part of any surveillance design strategy.

Industry best practices in the use of surveillance are not to apply its use in the areas where a right to privacy is expected. There are variances to this rule (e.g., when the appropriate signage is posted), but if there is any doubt about privacy expectations, an informed legal opinion should be sought and documented. As a result, the use of audio recording associated with a video camera can be restricted by the authority having jurisdiction (AHJ) or corporate policies. For this reason, the design of audio devices associated with VSS is not included in this chapter.

An area of concern is the inherent liability of providing surveillance. The use of this technology implies that monitoring and response would be provided in the areas under surveillance. This information must be kept in the forefront of the ESS designer throughout the project's life cycle.

Other concerns include whether an organization that provides video surveillance of a facility is liable if the systems are only recorded and not monitored. Another issue is whether the use of stand-alone or "dummy" cameras increases the organization's liability.

 © 2012 BICSI®

Privacy, Liability, and Legal Considerations, continued

Creating a false sense of security in and around the facility may be inviting unforeseen liabilities. Some key questions need to be considered to determine if an organization is liable for crimes committed in and around its facility. This discussion highlights the possibilities of liability and does not offer a legal opinion:

- Does the organization have a responsibility to provide a reasonable level of protection to its customers in the form of monitored cameras inside and outside its facility?
- If the organization is located in an area where it is well known that crimes occur with greater frequency than surrounding areas, should this be used as part of the decision process to deploy a surveillance system?
- Does the organization have to pay for services and personnel to continuously monitor its facilities inside and outside, especially during times when crimes may occur?
- Is it reasonable for the organization's customers to assume that all cameras installed are operating properly, monitored, and recorded?
- Do the organization's customers share the organization liability when they enter a facility, knowing that it is located in an area where it is well known that crimes occur with greater frequency than surrounding areas?

Communication is a key element in representing the purpose of a VSS to the people being monitored. By placing signage outside and inside the facility that the installed cameras serve a recording-only (forensic) function, there may be a shared liability should a crime occur on the premises. The negative effect of this is that potential thieves will read the same notice and may act accordingly. Studies support both the decrease of crime and no effect on crime by the installation of VSS.

The use of the video content has varied legal ramifications. One question that is always discussed is: can recorded video be used for evidentiary purposes? Be aware of the supplier that markets the recording device as being "court approved." Video content is not automatically approved for use in legal proceedings. Video, like any other evidence, requires evaluation of its accuracy and will be challenged on its merits as any other witness during a proceeding in a court of law. The acceptance of video images in a court of law will be greatly enhanced if the images are protected by an approved encryption standard as well as a documented chain of custody of the recorded video.

Higher resolution, megapixel technology, and low-light cameras offer an increased opportunity for video to be used in legal matters; however, they do not guarantee it. A number of law enforcement organizations apply a traceable, image-enhancement workflow to a recorded image and offer the enhanced image as possible evidence. The success of enhancement techniques is largely dependent on the quality of the original image and the ability to recognize multiple details that identify a person, vehicle, or object.

Privacy, Liability, and Legal Considerations, continued

Compression technologies can also work against the forensic video analysis process. Some compression schemes offer a "smoothing" algorithm to blend and hide digital artifacts or "tiling." This can have the opposite effect of increasing detail. Moving Picture Experts Group (MPEG)-4 Part 10, or H.264, is a type of compression technology used by some image capture systems to reduce bandwidth requirements across the network.

The use of searchable metadata allows the user to store information about an object and reference the video data without having to share the recorded video content itself. This can maintain the privacy of sensitive video information.

Some examples of this searchable metadata include:

- Date and/or time.
- Position.
- Shape.
- Trajectory.
- Speed.
- Color.
- Volume.
- Direction of travel.
- Location on a global positioning satellite (GPS) grid.
- Presence of an object.

If the metadata associated with the object is separate, the user can analyze this data for trends and possible threat prediction while keeping the video information private (e.g., an end user can associate an object's duration, position, speed, or direction over time with potentially dangerous behavior).

Privacy may also be maintained when an automated sequence of operations is performed after an object's behavior is analyzed (e.g., a flashing light alerts individuals that they have not come to a full stop at an intersection in a busy distribution center without recording the video information). This interdiction signal can reinforce safe behavior while maintaining privacy.

The recording of vehicle license plates can create privacy concerns. A digital video management system can capture and store all images of vehicle tags or license plates for vehicles entering a secure facility. The data associated with these license plate captures (LPCs) can be securely stored to maintain privacy. Should an event occur that requires a forensic review of the video data for an investigation, a license plate recognition system can compare this data with other event criteria. In this case, the license plate recognition process links the plate data with the individual that owns or drives the vehicle accessing the facility.

 © 2012 BICSI®

Video Surveillance Systems (VSS) Components

Categorizing individual components provides the ability to build a system from the various component categories that typify surveillance systems.

For both analog and IP surveillance systems, the components will include a combination of the following:

- Image capture/video sources—Consists of the camera, lens, mount, housing, and in the case of a pan, tilt, and zoom (PTZ) camera, the motorized positioning assembly and control components.
- Transmission—Refers to the protocol and media by which video signals are moved from the capture devices to processing and recording equipment and from processing and recording equipment to the monitoring and viewing components of a system.
- Processing—Collects and processes video images captured by the camera imager and presented in a format that can be viewed, recorded, and archived by the user.
- Recording—Writes the transmitted and processed video signal to a recording media.
- Monitoring and control—Consists of elements that enable viewing, analyzing, and manipulating the captured images and imaging device, which may include monitoring of live and recorded video.
- Support infrastructure—Includes all the remaining elements that make a VSS complete (e.g., encoders, power supplies, media converters, workstations, servers, storage media).

With the basic component categories in place, a discussion of the individual devices follows, and the components specific to analog or IP video are noted. Common platforms, known as hybrid systems, are covered at the conclusion of the section.

Analog Video Systems Overview

If a system is primarily used for real-time surveillance, the design emphasis should be placed on real-time viewing and the refresh rate of the video signal. Minimizing the control latency (both camera control delay and switching delay) is important and is a key benefit of an analog surveillance system. Analog systems tend to be point-to-point (PTP); therefore, controls and images occur in almost real time.

The resolution of an analog system is limited to 720 x 575; this is 720 pixels across the screen (horizontal resolution) and 575 pixels up and down (vertical resolution). The video is captured at intervals called fields, then combined (two fields) to produce a frame. To display and record analog video, it must be compatible with analog TV broadcasting standards.

There are two primary video standards for analog video signals: the National Television System Committee (NTSC), which is used in North America and Japan, and phase alternation line (PAL), which is used in Europe and most other countries.

An analog surveillance system requires a significant amount of infrastructure for deployment. It requires dedicated power supplies for the end devices, such as cameras, separate cables for video, controls, and power, as well as additional requirements for equipment mounting, alternating current (ac) power, cooling, and control switching requirements.

Internet Protocol (IP) Video Systems Overview

Video over IP is defined as video information deployed over a network that conforms to the Open Systems Interconnection (OSI) layer model. This includes support of cameras and encoders transmitting using various protocols, including transmission control protocol/Internet protocol (TCP/IP), user datagram protocol/Internet protocol (UDP/IP), and file transfer protocol (FTP).

Devices that stream video over IP networks transmit frames and packets of video data to a single location or multiple locations for different purposes. A device like a network video camera or multichannel video encoder can send a video stream to a single network video recorder or video decoder location or to multiple locations of the same type of equipment.

With a network infrastructure in place, power over Ethernet (PoE, IEEE 802.3at) devices can be used, eliminating the need and vulnerability of localized power supplies. An end user may have reduced operational overhead as the IP video devices are accessible at any location on the network. The IP video system devices often require less maintenance and system downtime; however, the ESS designer is cautioned to ensure that support exists for the shared infrastructure (e.g., network switches, recording servers). If not, the IP video system can actually be more costly to operate and maintain.

 © 2012 BICSI®

Internet Protocol (IP) Video Systems Overview, continued

Table 5.1 is a comparison of the features of IP and analog video.

Table 5.1
Internet protocol and analog video comparison

IP Video	Analog Video
IP cameras excel in capturing high-definition, megapixel images but have reduced performance in low lighting conditions.	Analog CCD cameras perform well across a variety of lighting conditions and manage motion well.
Dropped frames and video artifacts are commonly seen in IP CMOS cameras.	Analog cameras do not have capabilities above the NTSC/PAL standards.
IP cameras are limited in encoding resources. As a result, choices have to be made with respect to codec, frame rates, and quality where the selection of one decreases quality of another.	Analog compresses the video in the DVR; there are more hardware and software resources available to provide increased video quality and frame rate.
Since the video is being compressed before monitoring, codec compression must be selected that reduces or eliminates latency. Encoding at the camera introduces latency, which becomes an issue when an operator needs to track something with a PTZ controller and overcorrects.	Analog cameras transmit the video image to the DVR uncompressed where it can be viewed live with no latency precompression.

CCD = Charge-coupled device
CMOS = Complementary metal-oxide-semiconductor
DVR = Digital video recorder
IP = Internet protocol
NTSC = National Television System Committee
PAL = Phase alternation line
PTZ = Pan, tilt, and zoom

The typical IP video system is deployed and expanded more quickly and easily as the initial infrastructure investment has been installed and future devices are connected to the nearest accessible network access location, which is usually the telecommunications room (TR). When this is compared with installation of PTP infrastructure and if the facility in question has changing requirements, the deployment of an IP video system becomes a necessity.

Internet Protocol (IP) Video Systems Overview, continued

Live or recorded video may be more easily accessible, permitting a better use of the video system investment. IP video systems are essential parts of public surveillance systems like city center area security and mass transit as there may be an instantaneous requirement to view a single camera by one or many individuals simultaneously.

Open infrastructure permits the integration of video surveillance devices from different manufacturers; however, the ESS designer is cautioned that challenges similar to the analog video system exist where interoperability is required. Even though the transport is standardized with IP video, each manufacturer uses a special version of a video compression engine in the video source that must be decoded by the recording and control system.

There is an accepted method of exchanging such software development kit (SDK) and application programming interface (API) information between manufacturers, and some even have standardized on a single API to ease the burden on the developer. Assuming that integration is proceeding, it is far easier to link disparate systems to a single platform.

NOTE: See Chapter 11: Systems Integration for more details.

The integration of related systems, including access control, intrusion, fire-life-safety (FLS), and communication, can provide for beneficial interoperability.

Higher-end imaging techniques like megapixels and progressive scan are available in the IP video system and represent a distinct advantage over their analog counterparts. Many of the specialized imaging technologies still remain analog and must be converted to IP video through the use of video servers or encoder devices. Megapixels and progressive scan imaging make it easier for objects and individuals to be identified in recordings than their nearest equivalent analog counterparts, assuming the same imaging technologies are used in both devices.

Direct attached storage (DAS) and storage area networks (SANs) are easily scalable and provide future growth for the IP video platform as they can be placed and managed at or from any accessible location on the network. With IP video, there is a need to reduce the risk to the facility's infrastructure, but best practices for network security design usually place devices like these well behind corporate firewalls and are not generally accessible to the public.

Should the IP video device be publicly accessible, the risks are more of 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 in addition to accessing any stored video data within the camera.

It is for this reason that many manufacturers have adopted the use of port authentication protocol (IEEE 802.1x) to better manage video streaming and accessibility of the recording and monitoring devices that exist directly on a corporate network. The ESS designer is cautioned, however, to model all systems that utilize authentication protocols to ensure the level of performance that the user requires.

 © 2012 BICSI®

Image Capture / Video Sources

Cameras

When considering camera technology, functionality, and use, there are several major classifications, including fixed, fixed-zoom, PTZ, unitized dome, board, and miniature. There are various types of cameras, including:

- Indoor box type.
- Outdoor box type.
- Outdoor box type, day/night mode.
- Indoor dome type.
- Outdoor vandal-resistant dome type, day/night mode.
- Indoor, unitized dome PTZ.
- Outdoor, unitized dome PTZ, day/night mode.
- Board cameras.
- Box type PTZ.
- Covert (miniature).
- Infrared (IR) cameras.
- Thermal imaging cameras.

Most of these categories are self-explanatory; however, unitized PTZ cameras are an important subset of the general PTZ camera category. They offer an all-in-one, compact solution where the user needs a positional camera but does not need an extreme zoom lens range or an integrated illumination device. Conventional box type PTZ cameras have a definite use, especially where the zoom lens magnification exceeds that of the more compact unitized camera. Conventional PTZ cameras and fixed cameras may also be used together with IR illumination for unparalleled versatility in difficult lighting conditions.

Some of the individual features of the above cameras require further explanation as they have specific applications for analog and IP video systems.

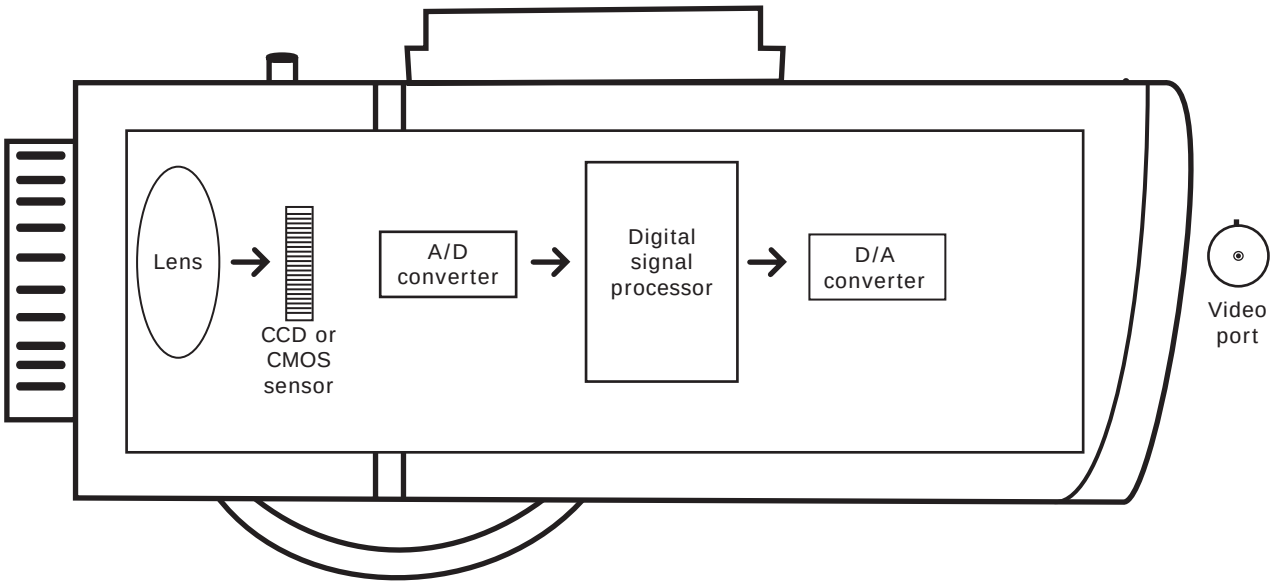
Analog Video Camera

Analog cameras can be fixed or PTZ. Today's analog cameras are actually fully digital inside as they contain a digital signal processor (DSP) that allows various image processing technologies to be applied.

DSP permits the images projected by the lens on the face of the charge-coupled device (CCD) chip to be adjusted, pixel by pixel, to provide the best picture possible rather than, formerly in analog video processing, applying an average value for brightness, contrast, or color (see Figure 5.1).

Although signal processing within the camera is digital, the most common transmission media is analog via coaxial cable. When digital outputs are provided, the signal is often transported by some type of transmission media (e.g., optical fiber, balanced twisted-pair). Power to the camera may be transmitted on a separate cable.

Figure 5.1
Analog camera components



A/D = Analog-to-digital
CCD = Charge-coupled device
CMOS = Complementary metal-oxide-semiconductor
D/A = Digital-to-analog

 © 2012 BICSI®

Analog Video Camera, continued

Analog video cameras typically have the following adjustments:

- Imaging:
  - Dynamic range, backlight compensation
  - Day/night
  - Automatic gain control (AGC)
  - Digital noise reduction (DNR)
  - Privacy zones
  - Back focus
  - Image stabilization
- Control:
  - Manual control mode
  - Automatic pan mode
  - Preset positioning
  - Automatic tracking
- Alarm:
  - Video motion detection area
  - Alarm schedule

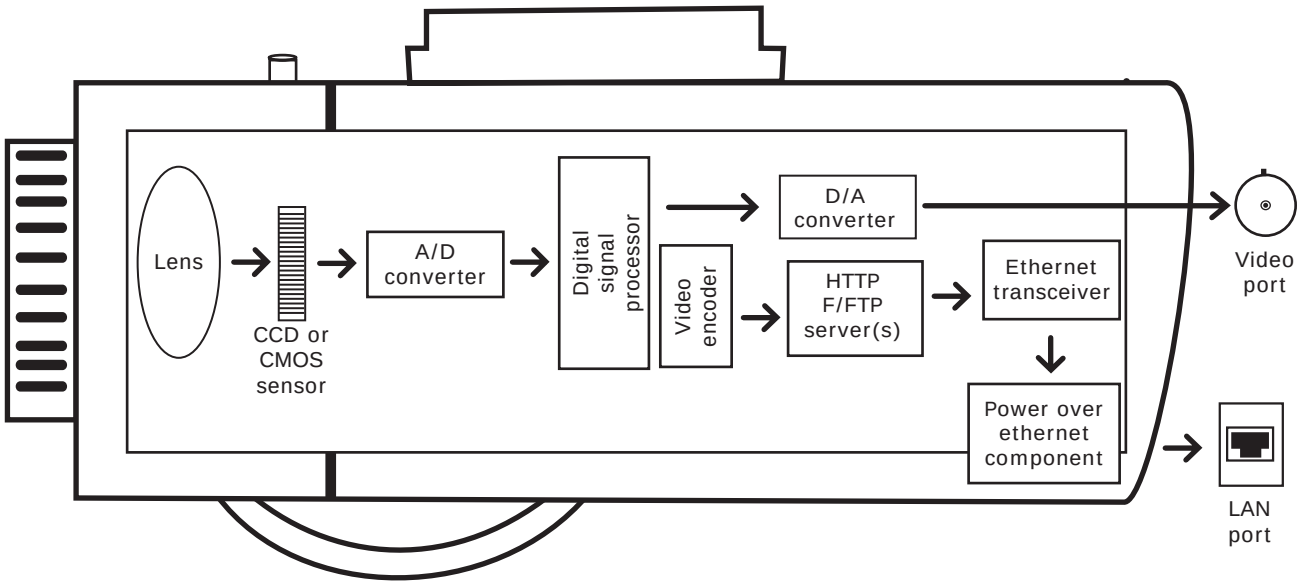
Internet Protocol (IP) Video Camera

An IP video camera is a device that produces a video image and encodes it for streaming over a network. This device combines a lens, imager, DSP, and digital-to-analog (D/A) converter in a single package. The network video camera will, at a minimum, include a connection for the network (see Figure 5.2).

If this is a remotely positionable camera with pan/tilt motion and zoom lens capability, then the position of the camera is controlled via commands sent from a user's computer or network recording/control command center directly to the camera over the network. In addition, the network PTZ camera may have an input/output or serial connector for an additional means of positioning control.

If the device is IEEE 802.3at compliant, the power is sent over the Ethernet cable. If it is not PoE, the low-voltage (usually 12 volts direct current [Vdc] or 24 volts alternating current [Vac] or dual voltage) connections are used for power.

Figure 5.2
Internet protocol video camera components



A/D = Analog-to-digital
CCD = Charge-coupled device
CMOS = Complementary metal-oxide-semiconductor
D/A = Digital-to-analog
F/FTP = Overall foil screened with foil screened twisted-pairs
HTTP = Hypertext transfer protocol

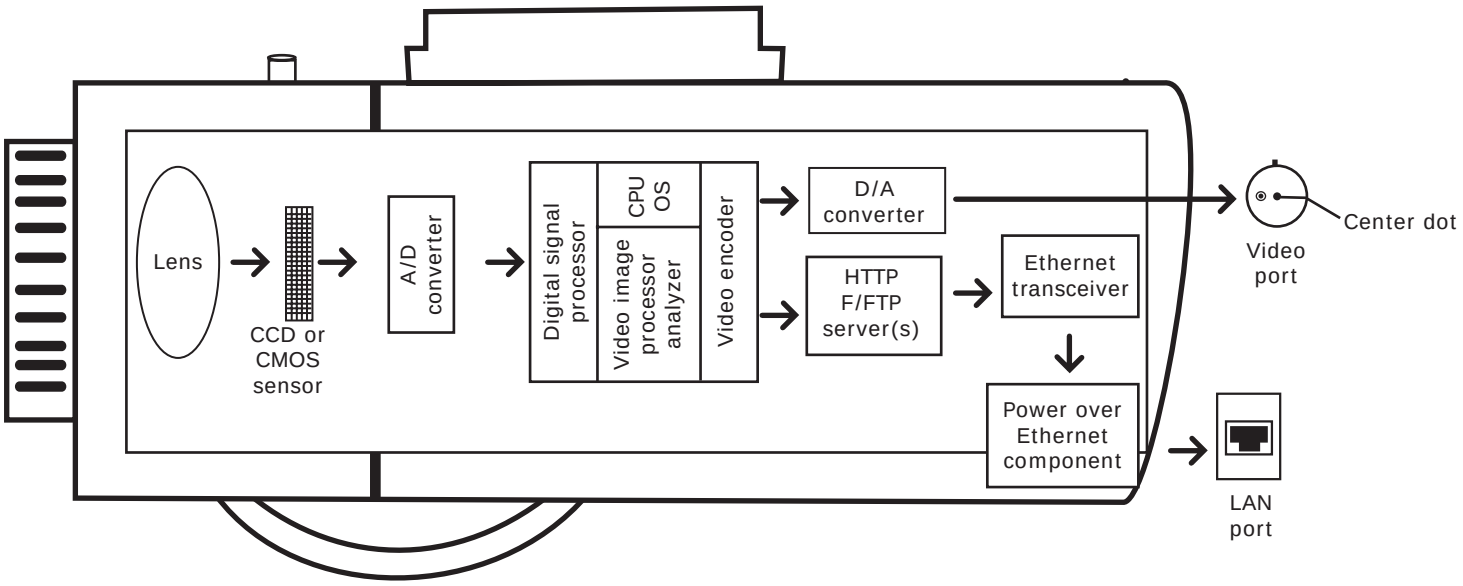
 © 2012 BICSI®

Internet Protocol (IP) Video Camera, continued

Some IP video cameras include advanced features (e.g., object detection algorithms) and can capture metadata at the video source for later processing by network video recorders (NVRs) or image processing servers (see Figure 5.3). A wide range of developers offers algorithms for use in these cameras; however, there is currently no standard means of interoperability between multiple algorithms by different manufacturers.

At the time of this publication, a number of manufacturers offer their individual image processing techniques as standards. It is important to refer to associations like BICSI® and the Security Industry Association (SIA) to see which proposed standards activities have been accepted and recognized.

Figure 5.3
Internet protocol camera with analytics



A/D = Analog-to-digital
CCD = Charge-coupled device
CMOS = Complementary metal-oxide-semiconductor
CPU = Central processing unit
D/A = Digital-to-analog
F/FTP = Overall foil screened with foil screened twisted-pairs
HTTP = Hypertext transfer protocol
OS = Operating system

Internet Protocol (IP) Video Camera, continued

IP video cameras have camera adjustments much like their analog counterparts but with the addition of settings specific to getting the IP camera to communicate properly on the network:

- Imaging:
  - Camera portion:
    - Dynamic range/backlight compensation
    - Day/night
    - AGC
    - DNR
    - Privacy zones
    - Back focus
    - Image stabilization
  - Compression:
    - Image size (pixels)
    - Compression type
    - Image refresh rate
    - Bandwidth
- Control:
  - Manual control mode
  - Automatic pan mode
  - Preset positioning
  - Automatic tracking
- Alarm:
  - Video motion detection area
  - Alarm schedule
- Network:
  - DHCP or static IP address
  - Gateway(s)
  - Router
  - Dynamic domain name service (DDNS)
  - Simple network management protocol (SNMP)
  - Port authentication
  - Host authentication

 © 2012 BICSI®

Internet Protocol (IP) Video Encoders

IP video encoder devices are often referred to as multichannel video encoders or video servers. This device simply converts video from analog cameras into multiple video streams that may be accepted by the network video recorder or control command center. It is usually a four- or six-channel device that may be placed near the analog camera or at some distance to accommodate placement in a TR. The packaging may be as a stand-alone module, rack-mounted device, or card type module that is a blade inside a larger, rack-mounted storage device.

These encoders support one or a number of types of PTZ camera control protocols. The encoder may support PTZ signals that are multiplexed over the coaxial cable or connected via serial.

Many video encoders support additional DSPs for the use of downloadable video analysis algorithms.

Refresh rates of each IP video encoder channel are either dedicated or an aggregate recording rate for the entire encoder and are divided between each channel.

The IP video encoder represents a method to upgrade an existing system that has analog cameras and digital video recorders or analog cameras with a matrix control system and digital video recorders.

The following is a sample upgrade path using IP video encoders.

Step	IP Video Encoder Upgrade Path
1	Verify which analog cameras are currently working and which require replacement.
2	Prepare and install the NVR, control system, and digital video management software.
3	Connect IP video encoders to camera connections directly, and loop-through the output to the existing analog matrix control system.
4	Maintain both systems concurrently.
5	Install new IP cameras, and connect them to the network for direct video streaming to the NVR system.
6	Once all NVR recordings and cameras controls are verified, begin removal of the analog matrix system.
7	Develop a plan for keeping or replacing existing analog cameras.

Compression Technology Overview

After discussing the two types of IP video sources, it is appropriate to now outline the compression technologies that are used.

As previously mentioned, the move to IP video is a combined result of the efficient transport technologies, PoE, and the increasing efficiency of today's IP camera compression schemes.

Uncompressed video uses a significant amount of data. In order to transmit and store video images practically and efficiently, it requires compression before it can be transmitted or recorded. The more the images are compressed (e.g., more information has been discarded), the lesser the quality.

Video compression is performed using codecs:

- MPEG-4, H.264
- MPEG-4, H.263
- MPEG-2
- Motion-Joint Photographic Experts Group (M-JPEG)
- M-JPEG 2000

M-JPEG is commonly used. The camera captures still images and compresses them into Joint Photographic Experts Group (JPEG) format. A camera can capture many images in one second (e.g., 30), which is the same as 30 frames per second (f/s). These images can then be transmitted over the network and viewed in sequence so that they appear just like a movie. However, each frame is a fully detailed still image, which may be relevant for admissibility in court.

MPEG is quite different from M-JPEG. MPEG compares two compressed images. The first is used as a reference. It then transmits only the parts of the second image that have changed compared with the reference.

It is complex in practice and has several variants:

- MPEG-1 (1993) has a target bit rate of 1.5 megabits per second (Mb/s) per video stream and is fixed at 25 f/s. Quality is similar to vertical helix scan (VHS).
- MPEG-2 (1994) has a higher quality, but a higher target bandwidth. Quality is similar to digital versatile disc (DVD) or high-definition TV (HDTV).
- MPEG-4 is a major development. It has a variable frame rate and higher quality.

 © 2012 BICSI®

Compression Technology Overview, continued

Some different types of frames used in compression of IP video are listed below:

- Intraframe compression:
  - JPEG, M-JPEG, and JPEG2000.
  - Code a single image on a stand-alone basis.
- Interframe:
  - MPEG-1, -2, -4, H.261, H.263, H.264 advanced video coding (AVC, also known as MPEG-4 Part 10).
  - Utilizes motion compensation; takes advantage of resiliency between nearby video frames.
  - Based on motion vectors that predict frame content; uses blocks drawn from one or more nearby frames.
- Encoding frames:
  - I-frames (intraframes):
    - Completely self-contained; do not reference any other frames.
  - P-frames:
    - Reference the frame that came before it for image data.
    - Each macroblock of a P-frame can be encoded independently of anything else.
    - P-frames use the similarities found in subsequent frames and are significantly smaller than I-frames.
  - B-frames are called key frames:
    - Bidirectional frames, meaning that they can reference frames that come both before and after itself.

The latest iteration of MPEG-4, MPEG-4 Part 10, H.264, or AVC is the most efficient compression technology to date and the most resource-intensive to decode and display. However, the efficiency of H.264 compression makes this technology suitable where content from real-time video streams needs to be stored and retained for long periods of time.

One efficient practice to accommodate long-term storage involves transcoding existing IP video recordings into H.264 format, which reduces the size of the storage needed.

The user can then apply a set of rules of retention to the individual video source's storage and retain video content required over a given timeframe at a specified resolution and capture rate.

Overview of Imager Resolutions

There are many image size standards and formats as listed in Table 5.2.

Table 5.2
Image formats and sizes

Format	Width	Height	Megapixels
SQCIF	128	96	0.012
QCIF (NTSC)	176	120	0.021
QCIF (PAL)	176	144	0.025
QVGA	320	240	0.077
525SIF (NTSC)	352	240	0.084
CIF (PAL)	352	288	0.101
525 HHR	352	480	0.169
625 HHR	352	576	0.203
VGA	640	480	0.307
2CIF (NTSC)	704	240	0.169
2CIF (PAL)	704	288	0.203
525 4SIF (NTSC)	704	480	0.338
525 SD	720	480	0.346
4CIF (PAL)	704	576	0.406
625 SD	720	576	0.415
SVGA	800	600	0.480
XGA	1024	768	0.786
720p HD	1280	720	0.922
4VGA	1280	960	1.229
SXGA	1280	1024	1.311
525 16SIF	1408	960	1.352
16CIF	1408	1152	1.622
4SVGA	1600	1200	1.920
1080 HD	1920	1088	2.089
2k x 1k	2048	1024	2.097

 © 2012 BICSI®

Overview of Imager Resolutions, continued

Table 5.2
Image formats and sizes, continued

Format	Width	Height	Megapixels
4XGA	2048	1536	3.146
16VGA	2560	1920	4.915
3616 x 1536 (2.35:1)	3616	1536	5.554
3672 x 1536 (2.39:1)	3680	1536	5.652
4k x 2k	4096	2048	8.389
4096 x 2304 (16:9)	4096	2304	9.437
4k x 4k	4096	4096	16.777

1k = Approximately 1000 pixels measured horizontally
2k = Approximately 2000 pixels measured horizontally
4k = Approximately 4000 pixels measured horizontally
CIF = Common intermediate format
HD = High definition
HHR = Half horizontal resolution
NTSC = National Television System Committee
p = Pixel
PAL = Phase alternation line
QCIF = Quarter common intermediate format
QVGA = Quarter video graphics array
SD = Schematic design
SIF = Standard input format
SQCIF = Subquarter common intermediate format
SVGA = Super video graphics array
SXGA = Super extended graphics array
VGA = Video graphics array
XGA = Extended graphics array

Most surveillance camera imagers support formats in a 4:3 ratio. Some of the most popular include quarter video graphics array (QVGA [320 x 240]), standard input format (SIF [352 x 240]), video graphics array (VGA [640 x 480]), extended graphics array (XGA [1024 x 768]), and 4 VGA (1280 x 960). Camera imagers having a total pixel count greater than one million pixels (p) are referred to as multiple megapixels.

High-definition imagers support formats in a 16:9 ratio. Examples include 720 p (1280 x 720) and 1080 p (1920 x 1088) formats.

Camera and Image Capture Types

License Plate Capture (LPC) Cameras

These are specialized cameras that are specifically designed to capture license plate information for processing by a license plate recognition (LPR) system. They have similar components to the IR surveillance camera package described in this chapter. Vehicle tags have a reflective coating that is sensitive to IR illumination, thereby representing an excellent opportunity to perform access control and visitor tracking in a passive manner. LPR systems can be integrated with access control to authenticate vehicle access using license plate information on file.

Recognition Devices

Access control identification portals, like iris authentication devices, can contain built-in (and optional) cameras dedicated to identity verification and access control.

Color versus Monochrome or Black and White Cameras

The decision between monochrome and color depends on the type of application. Monochrome technology requires less lighting to obtain usable video. When lighting is severely limited, monochrome functions are superior to color. This characteristic has led to the development of a camera popularly known as day/night.

The day/night camera is specifically designed for lighting levels that are expected to vary significantly and regularly. When lighting is sufficient, these cameras utilize a color imager to capture realistic scenes. When lighting is insufficient for color technology to operate effectively, the camera automatically transitions to monochrome images. Today's day/night cameras are becoming more affordable and have displaced the use of monochrome cameras with the exception of specialized applications.

Cameras with True Day/Night Capability

Also known as color/black and white cameras, they have the capability of viewing near-IR light, usually in the range of 850 to 880 nanometers (nm). These cameras may be used alone or together with an external IR illuminator that is sensitive in that range.

Incandescent-based IR lights present danger because of the heat and IR radiation, especially when mounted at a low height. Light-emitting diode (LED)-based illuminators do not have this problem.

One of the most versatile features of many of today's fixed and PTZ cameras is the day/night feature. The camera that has automatic and manual color to black and white capability first senses a low-light condition that would be better accommodated by a black and white mode. The camera then automatically removes a built-in IR cut filter, improving its sensitivity to light in that spectrum. The camera then automatically can turn on an IR illuminator and see in near darkness.

 © 2012 BICSI®

Camera and Image Capture Types, continued

Cameras with Noninfrared-Sensitive Day/Night Capability or Chroma Mode Capability

Some cameras offer an increased sensitivity mode and black and white capability, but they do not have a removable IR cut filter. These cameras are not sensitive to IR illumination.

Infrared (IR) Cameras

This refers to specially designed imagers capable of monitoring the very low IR bandwidth. They are sometimes referred to as starlight cameras because of their nighttime viewing capabilities.

Thermal Cameras

These cameras capture heat or temperature values of a scene and not light values, regardless of how bright or dark the scene appears to the human eye. Although the identification of colors and details are impossible with thermal cameras (because they view temperature only), these cameras are especially useful in viewing dark scenes for activities that have heat signatures.

Film Cameras

Film cameras have been on the market for many years, but it is rare to see them still installed. They were popular with retail financial institutions and activated by "hold-up" buttons. These self-sustaining units are equipped with traditional camera film, which permanently stores the scenes. The film requires replacement.

Imagers

Three basic types of imagers are used in both analog and IP video cameras:

- Interline
- Frame interline transfer (FIT)
- Progressive scan

Imagers, continued

Charge-Coupled Device (CCD) versus Complementary Metal-Oxide-Semiconductor (CMOS)

CCD sensors are the most mature technology in the surveillance industry. These sensors are typically more light sensitive than their CMOS counterparts and produce better images in low-light conditions. CCDs have a nonstandard manufacturing process and are more expensive than CMOS imagers.

CMOS imagers continue to advance with imagers offering useful dynamic image processing. Recent advances in CMOS sensors bring them closer to their CCD counterparts in terms of image quality. CMOS sensors are lower in cost to the manufacturer and can use slightly smaller size cameras. They consume less power than CCDs. A pixel on a CMOS sensor has multiple transistors located next to it; the light sensitivity of a CMOS chip tends to be lower.

When a vehicle headlight is aimed directly at a camera containing an interline transfer CCD, a phenomenon known as smear will create vertical streaks, creating difficulties in the identification process, especially at night and at vehicle gates.

For this reason, the FIT CCD was created and virtually eliminates smear. A number of specialized interline transfer CCDs also reduce smear and exhibit similar capabilities as the FIT CCD.

Today's CCD sensors in security video cameras create high-quality, low-noise images and use advanced signal processing techniques that can provide for multiple exposure patterns on a single image.

Frame Interline Transfer (FIT) Charge-Coupled Device (CCD)

FIT cameras contain a memory buffer located between vertical transfer CCD cells and horizontal transfer CCD cells. All the electrons transferred to the vertical cells are immediately transferred to the buffer memory, reducing smear.

Progressive Scan Charge-Coupled Device (CCD)

This is the most powerful application-oriented imager used and is present on many IP video cameras. The progressive scan CCD is equipped with double the vertical transfer cells than interline CCDs, which means one vertical transfer cell for each photodiode pixel. All pixels are transferred in 1/60 s, resulting in full vertical resolution with less motion blur.

 © 2012 BICSI®

Image Processing

The requirement to reproduce images in a high-contrast or backlight environment, such as bright daylight behind low interior light, has been a challenge to the surveillance camera manufacturer.

Some examples of these difficult lighting conditions include:

- Employees entering through building lobbies with glass exterior walls or doors.
- Customers using retail bank automatic teller machine (ATM) vestibules.
- Vehicle gate entrances with requirement to view driver and vehicle simultaneously.

In each of the applications, the dynamic range of the scene may exceed the resolving power of the surveillance camera. Certain unitized PTZ or fixed cameras offer the user an opportunity to tackle difficult lighting conditions that the conventional camera cannot. In the case of a high-contrast lighting or backlight situation, the typical camera will use conventional backlight compensation and reproduce an image of the primary subject that is underexposed.

The dynamic imager produces a smoother, natural reproduction of high-contrast images, regardless of object position, size, or shape.

The following surveillance camera capabilities offer solutions to these high-contrast lighting conditions:

- Backlight compensation enhances darker subjects and overexposes brighter background.
- Adaptive backlight compensation automatically locates multiple darker subjects, enhances them, and overexposes brighter backgrounds.
- Dynamic imaging captures the bright and dark images in a single image, processing pixel-based natural contrast image correction.

Some of these technologies include a double-speed CCD that outputs short and long signals to capture the bright and dark images in a single frame or picture. The camera's DSP then combines these signals in real time to provide a wide dynamic range, often 64 to 128 times relative brightness. An area free, pixel-based natural contrast image correction optimizes the gray scale image in response to the input signal level of each individual pixel.

Image processing techniques can improve the low-light response of the camera. These include:

- Electronic sensitivity boost (vary frame rate; accumulate light).
- DNR.
- AGC.

Image Processing, continued

In extreme low-light conditions, it is possible to boost sensitivity as great as 100 times with minimal impact on varying frame rate. Because noise becomes significant at these low-light levels, it is necessary to digitally enhance the gain to provide usable images (digital AGC). It is necessary to automatically change camera modes and either engage or disable these features. This may be done remotely through the use of the camera control system.

Video Motion Detection (VMD), Advanced Video Motion Detection (AVMD), and Automatic Tracking

Video motion detection (VMD) and advanced video motion detection (AVMD) are image processing capabilities at the camera, video encoder, digital video recorder (DVR), or NVR. VMD areas may be set up within the camera and activated during certain time periods to recognize motion within these areas. Alarms based on this image movement then results in alarm processing, storage, and transmission to the recording or control system.

Many IP video systems use motion detection within the control application and at the recording device instead of the camera. There are advantages to each, with the most significant being the distribution of resources at the recording server or control system. Should resources at the server be unavailable or many cameras are producing motion, it is easier for the application to process alarms already processed at the camera rather than multiple video motion events at the server itself.

AVMD allows for object motion to be processed and camera functions like alarm processing to be performed. AVMD functions differ from video analytic systems primarily in the object detection function. Should it be required that any object be automatically tracked or monitored within a certain area, automatic tracking and AVMD will be suitable. Should a differentiation be needed between person, vehicle, and animal, more advanced video analytics will be required.

The ESS designer is cautioned to evaluate all systems prior to deployment as many AVMD systems will outperform video analytics solutions and vice versa.

Personnel and object identification can benefit from automatic tracking functions that are built into many PTZ cameras. Today's video systems put greater demands on surveillance operators and recording systems to identify multiple objects or people. A lower cost alternative to multiple megapixel cameras is the use of a single PTZ camera with automatic tracking and automatic zoom capability.

 © 2012 BICSI®

Video Motion Detection (VMD), Advanced Video Motion Detection (AVMD), and Automatic Tracking, continued

With an automatic tracking camera, the camera will automatically acquire a person moving into the field-of-view, zoom in, and begin to automatically track them. When the person leaves the field-of-view of the automatic tracking camera, it returns to whatever automatic mode it was programmed for (preset tour, guard tour, or trace pattern).

This type of PTZ camera enables operators to monitor higher quantities of cameras. In the case of a system dedicated for forensic use, it makes efficient use of the cameras deployed and provides for the best possible opportunity to record an identifiable image.

A useful application of the automatic tracking camera is one where it is under the direct control of a video encoder device that controls its movements based on objects that appear in another camera with a wide field of view (e.g., megapixel camera).

Automatic tracking can help both security and facility management departments as the automation is at the video source. It provides some of the functionality of more expensive video processing systems at a similar cost of a PTZ camera. The automatic tracking camera may be activated after hours to help security monitoring teams see initial movements of tracked people. In many cases, the camera can react faster than a security monitoring operator.

Only the type of object, behavior, and motion can determine if the automatic tracking camera is a suitable solution for object identification.

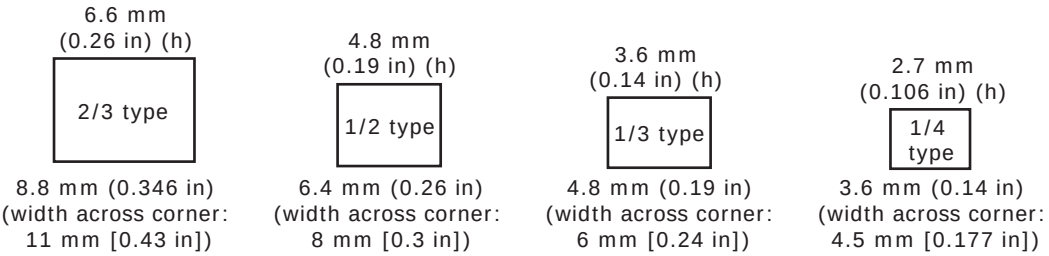
Lenses

A photographer will spend as much as possible on an arsenal of lenses since significant advantages can be gained in having good lenses gather the light and project the image. In the surveillance world, not much is different, and the lens is one component that can make a big difference in improving the overall scene image quality and sensitivity.

Lens Formats

Certain CCD imager sizes are not compatible with some lenses and will cause vignetting (e.g., falloff of light illumination observed at the image corners) to occur. The compatibilities are shown in Figure 5.4.

Figure 5.4
Charge-coupled device imagers and lens compatibility



	Lens Sizes		
CCD Sizes	**1/3 Type**	**1/2 Type**	**2/3 Type**
1/3 type	OK	OK (field angle: 75%)	OK (field angle: 55%)
1/2 type	NR	OK	OK (field angle: 72%)
2/3 type	NR (corners are dark)	NR (corners are dark)	OK

CCD = Charge-coupled device
h = Height
in = Inch
mm = Millimeter
NR = Not recommended

 © 2012 BICSI®

Lenses, continued

Lens Features

There are a number of different lens features as shown in Table 5.3.

Table 5.3
Types of lenses

Lens Features	Applications
Aspheric	Excellent light gathering capability (more usable lens surface area; usually f/1.0, f/0.75 maximum aperture)
Automatic iris	Adjusts to changing light conditions
Fisheye	Wide view/virtual pan capable/high distortion
Image stabilized	Reduces image shake because of vibration more visually apparent on ultra-telephoto lenses
Manual zoom	Stays in focus when zooming
Panomorph	360° x 180° wide view/virtual PTZ capable/high resolution maintained; some distortion
Pinhole	Permits high-quality box camera to be used in a covert application
Varifocal	Lower cost; requires refocus if zoom is adjusted

° = Degree
PTZ = Pan, tilt, and zoom

Lens Types

Automatic Iris Automatic Level Control Lens: Direct Current (dc) Servo/Video Servo

The direct current (dc) control system lens incorporates a control circuit in the camera that automatically adjusts the iris. This method enables the inexpensive production of a lens. This is today's most common system. The video control system incorporates a video signal processing circuit and the iris control circuit into the lens and is considerably more expensive. Most analog surveillance cameras support both dc and video servo lenses systems, but there are a few exceptions. When selecting a lens, check the available specifications for the camera for support and compatibility of both dc and video.

Lenses, continued

Automatic Back Focus or Near Infrared (IR) (Day/Night) Lens

With standard lenses focus changes between visible light and near IR light because of chromatic aberration. Near IR lenses have small chromatic aberration so that the focus is stable between the two light sources. Instead of using a specialized (day/night) lens, a standard lens can be used with a camera having an automatic back focus function. This function is typically built into the camera and automatically moves the imager until focus is achieved. When a camera with automatic back focus changes modes from day to night, the imager is automatically refocused. Unitized PTZ cameras do not need day/night lenses or automatic back focus because they are equipped with automatic focus zoom lenses.

Fixed Iris Lens

A fixed iris lens is not equipped with the iris adjustment function. It is used with electronic light compensation mode for a low-cost system. The shutter adjustment may also be varied to accommodate changing light conditions.

Varifocal Lens

The varifocal lens is convenient for installation because the focal length is variable. A 2x varifocal lens can range from wide to standard focal length, and an 8x varifocal lens can range from wide to telephoto. Unlike a zoom lens, focus needs to be readjusted when changing the focal length. This lens cannot be controlled remotely.

Fisheye and Panomorph Lenses

Immersive virtual imaging is deployed by using lens device and embedded decoding software. This complements applications where multiple fixed cameras are preferred to PTZ cameras. Megapixel imaging is useful with these types of lenses as their effective resolution is increased.

F-Number (Maximum Aperture Ratio)

The brightness of the lens depends on the effective diameter of the lens and focal length. This is the f-number or maximum aperture. Simply explained, a lens with a greater diameter is brighter as it accumulates more light, and a longer focal length lens is darker as its field of view is narrower.

The f-number is defined by the following formula:

f = focal length (mm [in])/effective lens diameter

NOTE: f/1.4 is also described as the maximum aperture ratio 1:1.4.

Keep in mind that a lens that is used wide open (f/1.0 to f/1.4) will create a shallower depth of focus and be difficult to focus. Automatic back focus will help automate this process. Using a light-sensitive camera permits more objects to be in better focus and ultimately better digital recordings.

 © 2012 BICSI®

Lenses, continued

The f-number directly contributes to the overall brightness of the scene (see Table 5.4).

Table 5.4
Stop and brightness chart

F-number	1	1.4	2	2.8	4	5.8	8	11	16	22
Brightness (Times)	1	1/2	1/4	1/8	1/16	1/32	1/64	1/128	1/256	1/512

Zoom Lens/Constant Aperture Zoom Lens

The focal length of zoom lenses may be controlled remotely. The maximum aperture of the lens will typically become smaller as the lens is adjusted to longer focal lengths (image grows darker). With a constant aperture zoom lens, there is no variance to the effective maximum aperture of the zoom lens, and the image does not grow darker with longer focal lengths.

Back Focus Adjustment

The back focus adjustment should be done with a darker environment to let the lens iris open to its widest setting. A smaller depth of focus results in a more accurate adjustment. A neutral density filter or electronic shutter can be used to create a darker environment. Use a clear sharp object or test chart to adjust the back focus more easily.

Depth of Field/Hyperfocal Distance/Depth of Focus

Depth of field is the range in an image, from near to far, that appears to be in focus.

The hyperfocal distance is the nearest distance at which the depth of field extends to infinity. Focus the lens so that infinity is aligned with the engraved depth of field mark for the aperture that is used and that will be the hyperfocal distance for that aperture. The left hand aperture marker for the aperture that is used shows the closest point that will be in focus.

Depth of focus is the tolerance of the imager plane being in focus for a certain lens, focal length, and focus setting. The use of a unitized camera within a dome housing has the effect of adding another optical element and creates a shallower depth of focus.

Some subjects cannot be focused on (see Figures 5.5 and 5.6):

- The smaller the f-number (the more the iris opens), the shallower the depth of field.
- The shorter the focus (wide-angle lens), the deeper the depth of field.
- The closer the object distance, the shallower the depth of field.
- Use the widest angle lens possible for focus improvement.

To clearly capture usable images, it is important for the ESS designer to understand the relationship of camera optics to the area of the subject being viewed and the distance to the camera when designing a VSS.

Lenses, continued

Depth of Field

Depth of field is the distance between the nearest and farthest objects in a scene that appear acceptably sharp in an image. Depth of field is directly affected by the amount of available light, the focal length of the lens, and the aperture setting of the lens.

The greater the focal length of the lens, the more shallow the depth of field (e.g., 35 millimeter [mm] lens will have a wider depth of field than that of a 120 mm lens). The wider the aperture of the lens, the more shallow the depth of field (e.g., a lens with an f/8 aperture will have a wider depth of field than that of an f/2.8 aperture setting); however, the trade-off will be the exposure time needed for the camera's sensor. A wider aperture setting of f/2.8 will gather light quickly, but it will have a shallow depth of field. A narrow aperture setting of f/8 will gather light over a longer period of time, but it will have a greater depth of field. However, faster moving objects will be distorted because of motion blur created by the extended exposure time needed by narrow aperture settings.

Depth of Focus

Depth of focus is the position of an object within the plane of the depth of field. An object's sharpest focus will be located at the center of the depth of field. As an object moves through the plane within a set depth of field, it will become less sharp as it approaches the border limits of the depth of field.

The picture shown in Figure 5.5 was taken with an aperture of f/8 on a 300 mm lens. The depth of field is sufficiently wide enough to provide a clear image of both the vehicle's license plate and driver when the object's depth of focus is centered within the depth of field; however, the vehicle must be moving at a slower rate in order to reduce the affects of motion blur.

The picture shown in Figure 5.6 was taken with an aperture of f/2.8 on a 300 mm lens. The depth of field is greatly reduced, and the depth of focus is centered around the license plate. While the license plate is clear, the driver of the vehicle is no longer in focus.

In Figure 5.7, the picture was taken with an aperture of f/2.8 on a 300 mm lens, but the depth of focus has been shifted farther back toward the driver. If the depth of focus is shifted to show the driver more clearly as shown in Figure 5.7, the driver appears clear while the license plate is no longer in focus. However, the wider aperture will allow the image to be captured even when moving at a greater speed without as much concern regarding motion blur.

In order to widen the depth of field, the focal length of the lens can be reduced, or the aperture can be reduced. If the focal length or aperture cannot be reduced, the speed of the object may be reduced to limit motion blur. For example, capturing the image of a vehicle can be accomplished with traffic devices such as gate arms, traffic lights, and speed bumps.

 © 2012 BICSI®

Lenses, continued

Figure 5.5
300 Millimeter lens at f/8



Figure 5.6
300 Millimeter lens at f/2.8



Figure 5.7
300 Millimeter lens at f/2.8



Mounting and Housing

Surveillance applications include two typical types of camera mounts:

- Fixed—Refers to a camera dedicated to a single view that does not change unless the camera is physically moved.
- Pan tilt mount—Allows for a 180- or 360-degree view that is controlled electronically from a remote viewing station.

The trade-off between the two types is that a pan and tilt mount provides a more flexible area of coverage, but it may not constantly view a single point. Pan and tilt technology can allow automatic panning or moving of the camera in a predefined cycle. Pan and tilt mounts may be interfaced with other ESS systems so that the camera can automatically return to a preset position triggered by a secondary system's event.

Camera mounting locations are typically dictated by the available physical infrastructure, balanced against the required field of views.

Camera mount types include the following:

- Ceiling
- Corner
- Parapet
- Pole or mast
- Wall

Interior cameras should be mounted to clear 2.4 meters (m [8 feet (ft)]) of aberration-free focus, while exterior cameras should maintain a minimum of 4.6 m (15 ft) aberration-free focus. These heights are recommended to prevent intentional and accidental tampering with the camera.

Camera mounting is often governed by aesthetic considerations. Many different sizes and configurations of camera housings are available. Installations include surface or flush type housings with a variety of finishes and concealment methods. Regardless of the mounting type, housings should always take into account environmental conditions and include heating and cooling measures where warranted. Furthermore, mounting should conceal all cable and electronics within a sealed unit.

Specific housings are designed for special conditions, including:

- Moisture.
- Dust.
- Heat.
- Vandalism.
- Explosion (e.g., housing is sealed to work within atmospheres containing explosive vapors).
- Undercarriage (e.g., flush or surface-mounted in-ground capture devices and housing).

 © 2012 BICSI®

Lighting

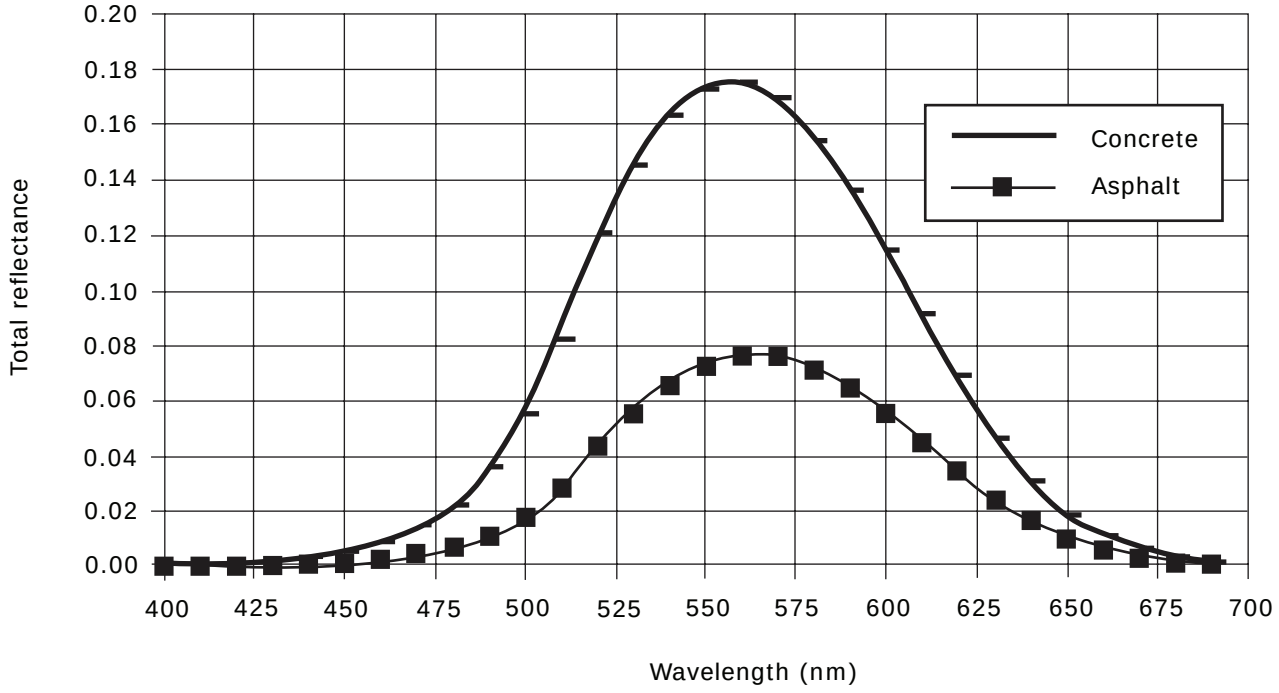
Luminance and Lighting

Additional lighting requirements for a VSS depend on the sensitivity of the imaging devices, the functional use of the VSS, and the existing lighting at the facility. Luminance is used to describe reflected light from flat surfaces and is measured in lux (lx = lm/m²) and is the method of measuring the sensitivity of a surveillance imaging device.

Since a surveillance device depends on reflected light, those surfaces that have greater reflective capability will allow a surveillance device to better reproduce images.

Figure 5.8 shows the relative reflective properties of asphalt and concrete with concrete being the brighter surface of the two. More light will be needed with surfaces like asphalt that have lower reflective qualities to produce the same images that another camera produces near concrete surfaces.

Figure 5.8
Comparison of total reflectance between asphalt and concrete



nm = Nanometer

Lighting, continued

Color Temperature

Color temperature is an important consideration when selecting lighting. Color temperature is expressed in units called Kelvin (K). Some light sources are ideal for reproducing details, especially those greater than 3000 K. There are advantages to light sources that have color temperatures less than 3000 K, but they are not associated with the improved details higher color temperature light sources produce.

Tables 5.5 and 5.6 show the most common light sources and color temperatures.

Table 5.5
Color temperature

Degrees Kelvin	Type of Light Source
1700–1800 K	Match flame
1850–1930 K	Candle flame
2000–3000 K	Sun (at sunrise or sunset)
2500–2900 K	Household tungsten bulbs
3000 K	Tungsten lamp 500 W–1 kW
3200–3500 K	Quartz lights
3200–7500 K	Fluorescent lights
3275 K	Tungsten lamp 2 kW
3380 K	Tungsten lamp 5 kW, 10 kW
5000–5400 K	Sun (direct at noon)
5500–6500 K	Daylight (sun plus sky)
5500–6500 K	Sun (through clouds/haze)
6000–7500 K	Sky (overcast)
6500 K	RGB monitor (white point)
7000–8000 K	Outdoor shade areas
8000–10,000 K	Partly cloudy

K = Kelvin
kW = Kilowatt
RGB = Red, green, blue
W = Watt

 © 2012 BICSI®

Lighting, continued

Table 5.6
Light sources and their behavior

Types	Lighting Behavior
Incandescent lamp	An incandescent lamp reproduces warm colors as red and yellow and casts generally pleasing tones.
Fluorescent	There are four colors of fluorescent lamps: daylight, day white, white, and natural light. For each color, bluish, yellowish, and reddish colors can be selected. However, its CRI is a drawback. Compared with other lamps, its efficiency and life is superior.
Mercury lamp	A mercury lamp is efficient and long-lived, but it is not suitable for color surveillance because of flickering, strong green spectrum, and weak color property as it is a discharge lamp.
Halogen lamp	A halogen lamp is widely used because of its good CRI, immediate turning on and off, small and lightweight body, and easy handling.
Sodium lamp	A sodium lamp is efficient and long-lived, but it is not suitable for surveillance because of its poor CRI. It is used as illumination inside tunnels and for highways as illumination is easy on the eyes.
Metal halide	A metal halide lamp has a high CRI and efficiency, but it cannot be turned on and off immediately as it is a discharge lamp.
LED	LEDs offer long life and low energy consumption as they are an illumination source that uses light emitting diodes.
IR illumination	This is an illumination lamp out of the near-IR area. An incandescent bulb and halogen lamp with the IR transmission filter installed used to be used; however, now high-strength LEDs are far more popular.

CRI = Color rendition index
IR = Infrared
LED = Light-emitting diode

Lighting, continued

Color Rendition Index (CRI)

The color rendition index (CRI) of a particular light source is the definitive measure of accurately reproducing and rendering colors that a surveillance camera "sees" (see Table 5.7).

Table 5.7
Color rendition

Lighting Type	Color Rendition Index	Relative Image Reproduction
Daylight	100	Excellent
Incandescent	97	Excellent
Fluorescent	87–94	Excellent
Halogen	90–97	Excellent
Low-pressure sodium	5	Poor
High-pressure sodium	30	Poor to Fair
Mercury vapor	43	Poor to Fair
Metal halide	70	Good

Infrared (IR) Illumination

IR illumination is an excellent tool to add directional and flood lighting to key areas. Most day/night cameras in their black and white mode are quite sensitive to the near IR light that today's IR illuminators provide, making IR a low-cost way of supplying additional light at night. As previously stated, the IR illuminator must be matched to the imaging device to ensure compatibility.

IR illuminators may be categorized first by their light source:

- Incandescent
- LED

LED-based IR illumination is the safest type, and it is especially required where the light is mounted in close proximity to people. Should the IR light be mounted at higher elevations, incandescent IR illumination is acceptable, although not popular. Should an LED-based illuminator be used, LED degradation compensation is necessary to maintain the LED array's long-term brightness; otherwise, a shorter replacement interval is required as the individual LEDs degrade.

IR illuminators are available in various ranges and fields of view:

- Long distance (213 m [699 ft]) narrow field of view (10 degrees horizontal)
- Medium range (36.6 m [120 ft]) wide angle (120 degrees horizontal)
- Short range (9 m [30 ft]) wide angle (120 degrees horizontal)

 © 2012 BICSI®

Lighting, continued

Other key features of IR lights include:

- Photocell activation—IR light turns on automatically at night or during light failure.
- Remote activation control by camera—IR light follows the day/night mode of the camera through a remote contact.
- Remote telemetry control by camera or control system—IR light automatically selects beam pattern as activated by camera or control system.
- Even illumination—Horizontal-angled elements are more powerful than those at a steeper angle to illuminate objects at shorter distances without washing out details.

The majority of today's IR illuminators are of the LED variety and offer efficiencies and safety better than their incandescent counterparts.

Imaging and Resolution

The ESS designer is faced with the challenge of evaluating and selecting the VSS to match the required functions as outlined in the section on Video Surveillance Systems by function at the beginning of this chapter.

Three functions to focus on are:

- Observation.
- Investigation and forensic review.
- Recognition of objects (e.g., human faces, license plates).

The capability of the VSS to meet the end user's needs for the above functions is a requirement of the entire system and not just the imaging device. There are simplified approaches relating pixel count, imager size, and function, but these are to be used as a guideline and together with International Organization for Standardization (ISO) standard resolution as shown in Table 5.8.

Table 5.8
International Organization for Standardization resolution chart

Format	Width	Height	Megapixels	Maximum Frame Size (Total Macroblocks)
SQCIF	128	96	0.012	48
QCIF (NTSC)	176	120	0.021	82
QCIF (PAL)	176	144	0.025	99
QVGA	320	240	0.077	300
525 SIF (NTSC)	352	240	0.084	330
CIF (PAL)	352	288	0.101	396
525 HHR	352	480	0.169	660
625 HHR	352	576	0.203	792
VGA	640	480	0.307	1200

Imaging and Resolution, continued

Table 5.8
International Organization for Standardization resolution chart, continued

Format	Width	Height	Megapixels	Maximum Frame Size (Total Macroblocks)
2CIF (NTSC)	704	240	0.169	660
2CIF (PAL)	704	288	0.203	792
525 4SIF (NTSC)	704	480	0.338	1320
525 SD	720	480	0.346	1350
4CIF (PAL)	704	576	0.406	1584
625 SD	720	576	0.415	1620
SVGA	800	600	0.480	1900
XGA	1024	768	0.786	3072
720p HD	1280	720	0.922	3600
4VGA	1280	960	1.229	4800
SXGA	1280	1024	1.311	5120
525 16SIF	1408	960	1.352	5280
16CIF	1408	1152	1.622	6336
4SVGA	1600	1200	1.920	7500
1080 HD	1920	1088	2.089	8160
2k×1k	2048	1024	2.097	8192
4XGA	2048	1536	3.146	12,288
16VGA	2560	1920	4.915	19,200
3616×1536 (2.35:1)	3616	1536	5.554	21,696
3672×1536 (2.39:1)	3680	1536	5.652	22,080
4k×2k	4096	2048	8.389	32,768
4096×2304 (16:9)	4096	2304	9.437	36,864
4k×4k	4096	4096	16.777	65,536

1k = Approximately 1000 pixels measured horizontally
2k = Approximately 2000 pixels measured horizontally
4k = Approximately 4000 pixels measured horizontally
CIF = Common intermediate format
HD = High definition
HHR = Half horizontal resolution
NTSC = National Television System Committee
p = Pixel
PAL = Phase alternation line
QCIF = Quarter common intermediate format
QVGA = Quarter video graphics array
SD = Schematic design
SQCIF = Subquarter common intermediate format
SVGA = Super video graphics array
SXGA = Super extended graphics array
VGA = Video graphics array
XGA = Extended graphics array

 © 2012 BICSI®

Imaging and Resolution, continued

An example of the simplified approach involves using the PPF approximate requirement for a given function. These generalized requirements that are entirely dependent on the imaging characteristics and quality of the VSS are as follows:

- Observation—20 PPF
- Forensic review—40 PPF
- Recognition—80 PPF

With a surveillance camera having 640 x 480, 1024 x 768, or 1280 x 960 imagers used in average lighting conditions and producing an image of the highest quality possible, the maximum field of view for each function is calculated as shown in Table 5.9.

Table 5.9
Surveillance video function/resolution/maximum field of view

Surveillance Video Function	Resolution (Pixels per foot)	Horizontal Resolution (Pixels)	Vertical Resolution (Pixels)	Maximum Horizontal Field of View (Feet)	Maximum Vertical Field of View (Feet)
Observation	20	640	480	32	24
	20	1024	768	51	38
	20	1280	960	64	48
Forensic review	40	640	480	16	12
	40	1024	768	26	19
	40	1280	960	32	24
Recognition	80	640	480	8	6
	80	1024	768	13	10
	80	1280	960	16	12

These are guidelines alone, and Table 5.8 must be used together with this to achieve an accurate resolution measurement.

Pixels, Imager Sizes, and Sensitivity

As the quality of today's megapixel imagers increases, the ability to reproduce high-quality images also increases. However, increases in pixel counts may not directly affect an overall increase in image quality and resolution. The ESS designer must weigh the quality of the imager and its ability to produce useable images in varying light conditions during the camera selection process.

Imager size and pixel size directly affect sensitivity and noise (area between pixels). A pixel is made up of a photodiode and captures light from the subject. The larger the photodiode, the more light it can capture, improving the overall image quality.

As imager resolution is increasing today, sensor sizes remain the same. This generally results in a decrease in average pixel dimensions and a decrease in size of the photodiodes. Unless the pixel shape can fit together with other adjacent pixels more effectively, an increase in pixel count can result in an increase in noise.

The sections that follow will explore how video signals are transported, switched, and viewed.

 © 2012 BICSI®

Transmission

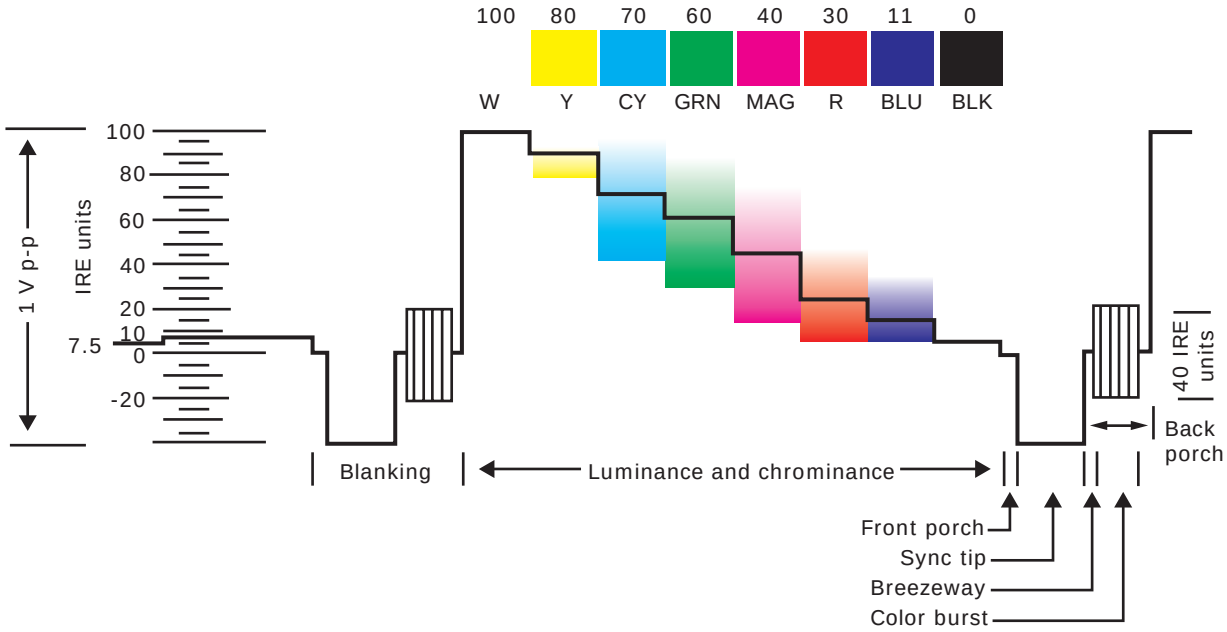
Transmission is the protocol and media by which video signals are moved from the capture devices to processing and recording equipment and from processing and recording equipment to the monitoring components of a system.

How an analog signal or IP video stream gets to its destination is almost as important as imaging systems. The decision on how to transmit signals should be based on several factors, including the distance the signal must travel, the environment the signal will experience on the way to its destination, cost to install, and the upgrade path to IP video.

Principles

The NTSC composite video signal is a relatively complicated ac waveform (see Figure 5.9). Any distortion of this waveform results in poor picture quality. The transmission media is susceptible to distortion because of the low amplitude of the video signal and the distances between the source and the monitoring point, which expose the 1 volt (V) peak-to-peak (p-p) signal to many causes of interference and loss.

Figure 5.9
National Television System Committee waveform



IRE = Institute of Radio Engineers
V p-p = Volt peak-to-peak

Principles, continued

The video signal from a surveillance camera has to provide a variety of information in the correct sequence for an image to be displayed. This may be achieved through the synchronizing pulses transmitted over the interconnecting media that define when to start scanning the screen with the new video information.

The synchronizing pulses are a relatively low-frequency component of the composite video signal. As most analog cameras are interlaced, capturing every other line every other time, the camera captures 60 fields, but a full frame of video requires capturing two consecutive fields.

The composite analog NTSC signal also has a relatively high-frequency (5.8 megahertz [MHz]) component, called luminance, that defines how bright a particular point in the picture should be and another high-frequency (3.58 MHz) component, called chrominance, that defines which colors a particular part of the picture should have. These upper frequencies are primarily determined by the camera resolution and color. The transmission media must be capable of supporting these high frequencies without distortion.

The chosen video transmission media must support a wide bandwidth from low to relatively high frequencies to produce a usable video. The transmission media must not significantly alter the signals' time relationship degradation and amplitude. Additionally, the transmission media should protect the signals' integrity from external interference.

 © 2012 BICSI®

General

All cables have attenuation properties that create the signal loss dependent primarily on the frequency—the higher the frequency, the greater the loss over a distance. This loss is primarily caused by the capacitance inherent in the construction of the cable. In other words, as a video signal travels along a cable, it loses its high-frequency components faster than its low-frequency components. The result is a loss of the fine detail (definition) in the picture.

The distance that a surveillance signal may be run is determined by the:

- Signal strength at the source (camera).
- Required signal strength at the receiving end (monitor).
- Signal loss over the length of the cable.

Low-frequency components are affected primarily by the dc resistance of the cable, which typically results in the loss of stability (rolling and tearing) in the image displayed on a monitor.

Video processing equipment (e.g., recorders, multiplexers) is less tolerant of cable attenuation and may not function adequately. Devices such as waveform monitors or other Institute of Radio Engineers (IRE) measurement devices should be used to analyze the transmission loss of the various component voltages that make up an analog composite video signal to determine if they are received at an acceptable level.

NOTE: The surveillance monitor should never be configured as a test instrument.

Analog-to-Digital (A/D) Process (Non-Internet Protocol [IP])

Digital technology involves conversion of the traditional analog signals to a digital format for transmission. These systems use an analog-to-digital (A/D) converter that can be located either at the camera or anywhere along the path back to the headend monitoring and control location. This type of system uses the traditional coaxial transmission media, but it also may use balanced twisted-pair and optical fiber cable. If a distributed architecture is used, the transmitted video signals can be recorded and distributed using standard network protocols and systems.

This conversion process is fairly common in upgrading and retrofitting an existing analog camera system. A/D converters or baluns can be used to either convert analog video signal to digital or transmit digital signals over an existing coaxial cable system.

Copper Cable Types

Two main types of copper cable are used for transmitting video signals:

- Unbalanced (coaxial)
- Balanced (twisted-pair)

The majority of traditional analog surveillance signal transport has been accomplished through coaxial cable.

Unbalanced (Coaxial) Cables

An unbalanced signal is one in which the signal level is a voltage referenced to ground. For example, a video signal from the camera is between 0.3 and 1.0 V above zero (ground level). The shield is the ground level.

Impedance is measured between the inner conductor and the outer sheath. Cable with a characteristic impedance of 75 ohm is the standard used in VSS. Coaxial cables with an impedance of 75 ohm are constructed from various materials, each having their own effect on signal propagation. For example, some cables with 75 ohm characteristic impedance have a center conductor constructed of copper-clad steel. This cable is well suited for the distribution of community antenna TV (CATV) type signals because of the high strength provided by the steel center conductor. These signals are composed only of high-frequency components, which flow well on the copper-clad outer skin of the center conductor.

These CATV or master antenna TV (MATV) cables are not suitable for surveillance signals because steel is not particularly well suited for the transportation of the relatively low-frequency signal component of a composite video signal. Solid center conductors are not recommended for locations subjected to continuous flexing (e.g., external pan and tilt drives).

Similarly, the construction of dielectric insulation between the center conductor and shield has an effect on the cable's capability to transport the high-frequency component of a composite surveillance signal. Different sheath materials produce different capacitance from the shield to the center conductor.

Other techniques (e.g., using dielectrics constructed from foam material) also provide low capacitance, but they may be problematic if used in environments where water ingress or pulling difficulties are expected.

The conductor material and impedance are critical properties of a transmission media that must be considered during the design process. Center conductors and shields may include both copper and aluminum.

Multiple ground references connected to the shield may create a ground loop. The difference of potential on the shield ground may generate loss of signal in the center conductor. The most frequent symptom of this defect is the rolling of dark bands through the picture in regular intervals.

 © 2012 BICSI®

Copper Cable Types, continued

The outer jacket must be properly designed to match the environment in which the cable is installed. The cable assembly must meet code requirements for flame spread and smoke characteristics in the most restrictive environment where it is installed.

When installed outdoors in an aerial application, the outer jacket of the cable should be constructed of ultraviolet (UV) resistant polyethylene or another like substance and may contain water-excluding gel if approved for direct burial. Cables used in ordinary applications are typically jacketed with plastic or other durable coverings.

At this end is the signal loss over the cable run, which varies depending on the frequency of the signal. The standard rules are as follows:

- Mini coaxial—107–152 m (351–499 ft) color signal
- Series 59—230–305 m (755–1001 ft) color signal
- Series 6—305–457 m (1001–1499 ft) color signal
- Series 11—671–915 m (2201–3000 ft) color signal

Using powered baluns on both ends over balanced twisted-pair, the signal will go up to 2743 m (8999 ft). Using strategically placed amplification may extend these distances. However, conversion to another media may be more cost effective and provide better results. Refer to Table 5.10 for typical coaxial cable signal loss.

Smaller diameter series coaxial cables (e.g., miniature coaxial) may be used for short distances (e.g., jumpers for interconnecting components installed in consoles or equipment racks).

Table 5.10
Typical coaxial cable signal losses

Frequency	Channels	Mini 59 (dB per 100 ft)	Series 59 (dB per 100 ft)	Series 6 (dB per 100 ft)	Series 11 (dB per 100 ft)
1		0.6	0.4	0.2	0.2
10		1.8	1.4	0.6	0.4
50	2-6	3.9	3.3	1.4	1.0
100	2-6	5.4	4.9	2.0	1.6
200	7-36	7.5	7.3	2.8	2.3
400	7-36	10.4	11.2	4.3	3.5
700	7-36	13.5	16.9	5.6	4.7
900		15.2	20.1	6.0	5.4
1000		15.9	21.5	6.1	5.6
1450				7.8	5.9
1750				8.7	6.3
2050				9.3	6.8

dB = Decibel
ft = Foot

Copper Cable Types, continued

Balanced Shielded and Unshielded (Twisted-Pair) Cables

Balanced shielded and unshielded twisted-pair cables transport signals with energized conductors and usually do not reference ground as a conductor. Their noise immunity comes from the twisted construction in which induced noise is canceled out when it crosses the twisted conductors.

A balun, short for balanced to unbalanced transformer, provides conversion and matches the impedance of the native 75 ohm output to a single pair of 100 ohm or 600 ohm media. These passive devices are capable of effectively transporting analog video signals over greater distances than coaxial cable and do not have the potential for ground loop problems.

Twisted-pair transceivers may be active or passive devices that equalize and amplify a video signal by boosting the frequencies.

Optical Fiber Cable

The use of optical fiber cabling presents an opportunity to reduce the negative impact of electromagnetic interference (EMI) and noise. The use of optical fiber as a means of video transport is also widely used in outdoor applications to reduce damage because of lightning and other transient electromagnetic phenomena.

The different types of optical fiber transmission devices fall into three major categories:

- PTP optical fiber transceivers
- Multiplexed PTP transceivers
- Drop and insert digital broadband multiplexing

Optical fiber cable is an effective means of transporting video signals across great distances. In its simplest form, surveillance signals modulate a beam of light that is transmitted through the optical fiber cable to a receiver where it is demodulated into its original form.

Optical fiber cable provides the ability to span great distances without degrading the video signal. Because the transmission media is resistant to EMI from outside sources and because of its immunity from lightning-induced voltage surges, the signal retains its original fidelity.

Optical fiber cable has advantages over coaxial and balanced twisted-pair cable for video, telephony, and data transmission. It has the ability to transmit higher bandwidth over greater distances.

The two types of optical fiber cable are:

- Singlemode.
- Multimode.

 © 2012 BICSI®

Optical Fiber Cable, continued

Because of the smaller core and the ability to carry higher bandwidth, singlemode optical fiber has greater advantages over multimode optical fiber.

Outside plant type, indoor, and indoor/outdoor rated outer sheaths may be specified. The outer jacket composition may include metallic armored, general-purpose metallic, and all nondielectric.

Multimode optical fiber core sizes are available in 50/125 and 62.5/125 micrometers (µm). The singlemode core size is 8/125 µm nominal.

Fundamental System

The key factors in determining which optical fiber cable to use in a given application are the:

- Type of active equipment.
- Distance between two points.
- Bandwidth requirements (data rates).

At the heart of design is the application to be served. This determines which electronics and passive equipment are available to support the application.

The distance between two points, the decibel loss, and the capability of the active equipment determine how far apart the end points may be. The distance, the capability of the active equipment, and the bandwidth requirements determine the optical fiber type and size.

Expected losses are determined by calculating the decibel loss from the cable length and the number of connectors and splices. The ESS designer can make a preliminary calculation of these decibel loss factors during the design process. The optical cable manufacturer provides the cable performance characteristics to determine bandwidth.

Link Loss Budget

The link loss budget is the maximum allowable loss for the end-to-end cable system. To find the loss budget, the system's gain and receiver sensitivity must be determined.

System gain is the difference between the average transmitter power and the receiver sensitivity. Power penalties are factors that adjust the system gain, including the operating margin, receiver power penalty, and repair margin.

The system gain subtracts the receiver sensitivity from the transmitter average power. This gives the maximum allowable decibel loss between the transmitter and receiver.

Power penalties are added decibel loss values for the operating margin, receiver power penalty, and repair margin. Subtracting the total value in decibel for all of the power penalties from the system gain equals the link loss budget.

NOTE: See Example 5.1 for an optical fiber performance calculations worksheet. The latest editions of BICSI's *Telecommunications Distribution Methods Manual* (*TDMM*) and *Information Technology Systems Installation Methods Manual* provide more detailed information on optical fiber cable and system principles of transmission.

 © 2012 BICSI®

Link Loss Budget, continued

Example 5.1
Optical fiber performance calculations worksheet

A. Calculating Passive Cable System Attenuation

1.	Calculate optical fiber loss at operating wavelength		Cable distance		1.5	km
		x	Individual optical fiber loss	x	1.5	dB/km
		=	Total optical fiber loss		2.25	dB
2.	Calculate connector loss (exclude Tx and Rx connectors)		Connector pair loss		0.75	dB
		x	Number of connector pairs	x	4	
		=	Total connector loss		3.0	dB
3.	Calculate splice loss		Individual splice loss		0.3	dB
		x	Number of splices	x	3	
		=	Total splice loss		0.9	dB
4.	Calculate other components loss		Total components (none)		0.0	dB
5.	Calculate total passive cable system attenuation		Total optical fiber loss		2.3	dB
		+	Total connector loss	+	3.0	dB
		+	Total splice loss	+	0.9	dB
		+	Total components	+	0.0	dB
		=	Total system attenuation		6.2	dB

B. Calculating Link Loss Budget

	Example manufacturer's electronic specifications		System wavelength		1300 nm	
			Optical fiber type		62.5/125 µm multimode	
			Average transmitter output		–18.0 dBm	
			Receiver sensitivity (10^9 BER)		–31.0 dBm	
			Receiver dynamic range		11.0 dB	
6.	Calculate system gain		Average transmitter power		– 18.0	dBm
		–	Receiver sensitivity		– (-31.0	dBm)
		=	System gain		13.0	dB
7.	Determine power penalties		Operating margin (none stated)		2.0	dB
		+	Receiver power penalties (none stated)	+	0.0	dB
		+	Repair margin (2 fusion splices at 0.3 dB each)	+	0.6	dB
		=	Total power penalties		2.6	dB
8.	Calculate link loss budget		System gain		13.0	dB
		–	Power penalties	–	2.6	dB
		=	Total link loss budget		10.4	dB

C. Verifying Performance

9.	Calculate system performance margin to verify adequate power		Link loss budget		10.4	dB
		–	Passive cable system attenuation	–	6.2	dB
		=	System performance margin		4.2	dB

µm = Micrometer
BER = Bit error rate
dB = Decibel
dBm = Decibel milliwatt
km = Kilometer
nm = Nanometer
Rx = Receive
Tx = Transmit

NOTE: 4.2 > 0. Therefore, the system will operate as installed.

Wireless Transmission

Three primary types of wireless technologies are used for transmitting video signals:

- Radio frequency (RF)
- Free space optics (FSO)
- Microwave

Wireless transmission can aid in meeting the needs for rapid deployment of security surveillance devices such as surveillance cameras. These technologies can be limited to line of sight (LoS) applications, requiring careful site surveys to determine potential signal obstructions.

NOTE: The ESS designer can refer to the latest edition of BICSI's *Wireless Design Reference Manual* for additional information on the design and deployment of wireless technologies.

Radio Frequency (RF) Transmission

RF transmission typically uses low-power unlicensed radio transmitters and receivers to convey the surveillance signal and typically operates in the 2.4 gigahertz (GHz) or 5.8 GHz band.

Free Space Optics (FSO)

FSO utilizes many of the same principles for transporting video signals that an optical fiber cable 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, fog).

Licensed Microwave Radio Transmission

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 ESS designer must allow for sufficient time when selecting this transmission media to allow for the governmental application process.

 © 2012 BICSI®

Best Practices for Internet Protocol (IP)-Based Video Deployment

IP-based systems can use dedicated or shared networks. Video over IP systems on a dedicated network make simple network switch selections to procure the best switch that is affordable. The cabling infrastructure design and deployment, however, must be left to those recognized professionals who can select the copper, optical fiber, or wireless cabling needed, design the wiring plant, and enforce standards and best practices for connections, cable paths, and power.

For shared networks, the integrator or IT professional must be involved to determine compatibility with the existing infrastructure:

- Is the cable or network service point (switch/router) bandwidth limit or wire speed greater than the sum of the IP-based device load?
- Is a core network switch being used?
- Has failure been accommodated for?

There are some situations where video over IP deployment is dependent on higher protocol levels. If those protocols are supported only by the core switch, failure at that point can affect video device streaming at other locations.

Avoid a central point of failure by designing a redundant pathway that will allow signal continuity in the event of a single device/link failure on the network.

Software support and licensing fees may be applicable.

The ESS designer should consider using standards-based power such as PoE (IEEE 802.3at) and the following practices:

- Determine the area system power requirement.
- Determine how many powered devices may be connected to a single PoE switch.
- Use midspan devices to distribute power to PoE-enabled equipment.
- In mission-critical applications, interleave power or route the cabling of adjacent cameras to different TRs' midspans. Power loss at one TR will not disable the entire single area.
- Consult IEEE 802.3at standards or manufacturer interpretations.
- IEEE 802.3at or PoE+ standard and the infrastructure deployed must support this.

Best Practices for Internet Protocol (IP)-Based Video Deployment, continued

When considering the selection of network switches, the ESS designer should consider the three basic types of network switches and their function on the network. The ESS designer will typically specify only the edge switches or make recommendations for protocol and power compatibility to the IT professional.

The three types of network switches are:

- Core:
  - Centralized location
  - Higher management functions
  - Security management policy delivery point
  - Upgrade portal
- Aggregate:
  - Act as a manager of multiple edge-located switches that must communicate with the core switches
- Edge:
  - Support various network-enabled devices:
    - Video cameras
    - Telephones
    - Access control readers
  - Provide PoE

For the ESS designer, the functions that are critical to edge network switches include:

- Switch selection criteria.
- Aggregate throughput.
- Connectivity.
- Classification/protocols supported.
- Authentication.
- PoE capacity.
- Logical network segmentation.
- Remote support, diagnosis, and testing.

 © 2012 BICSI®

Best Practices for Internet Protocol (IP)-Based Video Deployment, continued

When connecting IP cameras and devices to broadband Internet service, the ESS designer should consider the following connectivity issues:

- Use symmetrical digital subscriber line (not asymmetric digital subscriber line) or business cable.
- Router will allow several devices to use the same Internet address through network address translation and port forwarding.
- Static IP or DDNS service:
  - For a fee, a dedicated (static) IP may be obtained from the service provider.
  - For less of a fee, a subscription to a DDNS service may be purchased, which keeps track of the IP address assignments as they change from the service provider. This is not recommended for mission-critical systems.

Processing

Video processing switches and carries video inputs to selected video outputs. The traditional system for the control and display of analog video is the cross-point matrix. This system takes in a number of surveillance camera signals and then switches these cameras to outputs for viewing and recording. Typically, the number of inputs is higher than the number of outputs.

Surveillance Matrix

The surveillance matrix switch switches and distributes video signals from multiple inputs to multiple outputs. This is accomplished through a mesh architecture technology that allows an administrator or user to interface with the system to control the desired operations.

The ESS designer must evaluate the:

- Quantity of video inputs and outputs.
- System's life cycle and potential growth.
- Other considerations when selecting the capacity of the matrix.

The traditional product is available in multiples of 8 or 16 inputs and outputs.

Matrices may be connected in single large or small systems and master-slave configurations, allowing for a distributed architecture and resulting in several benefits, including:

- Flexibility.
- Scalability.
- Reliability.

The traditional video surveillance matrix system transmits all video to the matrix at all times, regardless of whether the video is viewed. The digital systems, based more on IT processes, attempt to make the most efficient use of the bandwidth. The video frame rate and resolution also may be tailored to the bandwidth. These controls allow the video to share the network with other applications.

Multiview Processor

The function of the multiview processor is to consolidate groups of video inputs into a single video output. The new video channel is structured to allow multiple inputs to be simultaneously displayed in a single output image. The typical output image may consist of a grid display with multiple layouts.

The ESS designer should keep in mind that consolidating multiple video inputs into one video output results in lower resolution of each individual input in the grid format. To view the detail, the operator may need to call up the video in a single view on a larger screen. Therefore, the ESS designer should consider if the application warrants routing the video outputs from multiview processors into a matrix as a single video input.

 © 2012 BICSI®

Video Analytics and Automated Object Detection

Applications that use video analytics can perform complex repetitive functions like object detection and recognition on many channels of video simultaneously.

The ESS designer should consider a system like this if:

- The system uses a large quantity of cameras that require monitoring for specific conditions or behaviors that are capable of being recognized.
- The setup and installation of the video analytics subsystem is relatively simple and has high, sustained accuracy for the types of behaviors and objects recognized.
- Modifications may be made by the end user easily and effectively without the constant involvement of the integration professional; otherwise, software as a service (SaaS)-based solution should be considered.

When selecting the video analytics and object detection subsystem, the ESS designer should consider the following:

- Processing at imaging source (camera or encoder) or at the server.
- The trend toward more complex image processing is driving server-based solutions.

Data Mining and Video Analysis

One significant technology that is common for these opportunities is the use of data mining and enhanced video analysis. This technology will enable the typical electronic security system to be more useful to other departments and even to predict trends not apparent to the typical organization or operations manager.

One application of data mining involves the use of video analysis in the prevention of crime and the optimization of staff hours.

With video analytics, the user can leverage existing VSS through:

- Monitoring and ensuring that a stranger spends a minimum amount of time in a sensitive work area.
- Using real-time video analysis to discourage loitering in sensitive areas.
- Using forensic video analysis to investigate behavior related to computer crime and network vulnerabilities.

Data Mining and Video Analysis, continued

The process of real-time video analysis can be as follows:

- Enter object duration, position, speed, or direction threshold to identify negative or potentially dangerous behavior such as:
  - Loitering.
  - Object left behind.
  - Color, shape, and size of object.
  - Virtual fence.
- Develop rules and associated interdiction, including:
  - Computer input lockdown.
  - Security alert and messaging.
  - Local interdiction signaling.

Forensic video analysis then may be processed in the following way:

- Collect video metadata and analyze for baseline behavior and normal activity.
- Create baseline event chart.
- Use scoring engine; apply to chart.
- Video motion detection system detects multiple behaviors; compares with baseline data.
- Rules engine ignores or recognizes multiple behaviors; applies sequence of operations.

It is important for the ESS designer to consider the staff hour needs with such program-intensive solutions. The ESS designer should consider the following device costs when planning a video analytics subsystem:

- Server costs will continue to decrease, so the total cost of application plus server is lower.
- Camera costs will decrease, but will not always permit the latest analyzer upgrade or have the power necessary for the given unit price.
- An intermediate device can be introduced to keep the camera costs down, and distribute processing around the network.

 © 2012 BICSI®

Data Mining and Video Analysis, continued

Benefits of a video analytics subsystem and related video analysis are that the end user can take advantage of both short-term and long-term (automated) improvements.

Examples of static video analysis use for the security operation are:

- Use different criteria, generate reports, and compare data.
- When an incident occurs, detail information for future correlation of the incident.
- Use reports for immediate resource planning.
- Predict security guard resource requirements.

Examples of video analysis use for automation in the physical security program are:

- Produce real-time abnormal behavior summary and response.
- Improve security level and responsiveness.
- Periodically increase analytic accuracy.
- Allocate response according to the frequency, severity, and type of behavior and alarms.
- Reduce costs through security monitoring efficiency, false alarm reduction, and effective security guard resource planning.

In each of these cases, video analytics, video analysis, and data mining represent areas of constant improvement for the ESS designer to maintain.

Recording

This section discusses the devices that write the transmitted signal to recording media.

Analog Recording

Analog recording is the linear writing of video image data to a media for the purpose of storage.

Approaches to analog recording include:

- A single video input to a single recording device.
- Multiple video inputs (multiview processor) to a single recording device.
- Multiplexed video input to a single recording device.

The ESS designer must evaluate the appropriate frame capture rate when selecting the density of video inputs to a single recording device. This selection will affect the quantity of images and the duration of the recorded signal. Analog recording systems may allow for selecting the quantity of multiplexed cameras. The longer the selected duration, the lower the frame rate.

An analog recording device may be set for 12 or 24 hours, lowering the frame rate by half. If the interspersing of video frames is added, 8 or 16 cameras may be interspersed, which results in recording a limited number of frames from each camera view. This approach often leads to missing some events because of the time between the frames, which lowers the overall value of the video for forensic use.

Tape change out is chiefly a manual operation, so video could be missed because of operator error and tape degradation caused by constant rerecording. Because of the retention times required for certain applications, tape storage may become a major issue. For these reasons, the industry has moved away from analog recording.

 © 2012 BICSI®

Digital Video Recording

Digital recording is the nonlinear writing of video image data to a media for the purpose of storage.

Approaches to digital recording include:

- Embedded DVRs.
- Embedded NVRs.
- Recording servers (also NVRs).
- SANs.
- Network-attached storage (NAS).
- Redundant array of independent disks (RAID).
- Stand-alone disks and digital tapes.

Whether the ESS designer is working with DVRs or NVRs, there is a set of criteria that needs to be considered in the selection process:

- Number of fixed cameras
- Number of PTZ cameras
- Command structure—camera
- Image size and quality
- Compression type (JPEG, MPEG4)
- Compression level (super fine, fine, normal, extended)
- Resolution (megapixels, VGA, common intermediate format [CIF])
- Number of days to store and retain image
- Recorder image rate (images per second [IPS])
- Individual camera image rate (IPS)
- Hours recording per day
- Percentage of time with motion (100 percent if recording all images)
- Number of workstations
- Refresh rate required at workstations
- Connectivity from workstation-to-DVR/NVR
- Record on motion and other triggers versus continuous recording without defined triggers
- Online storage versus offline (archived) storage
- Centralized versus distributed storage
- Recording at the edge versus traditional storage medium and systems

Digital Video Recorders (DVRs)

To the consumer, any video or image captured digitally and stored may be classified as a DVR. To the security industry, a DVR is a multichannel analog input device that captures composite video, stores it on digital media, and permits search, playback, and video analysis functions for single or multiple users. Multiple capture cards or DVR cards, together with a server and digital video management software that also does the above, could collectively be a DVR.

DVRs are multichannel devices with a proprietary, embedded, or built-in real-time operating system that acquires video images at a preprogrammed format and capture rate and writes and stores the same data in a proprietary format on nonremovable hard disk drives.

The A/D conversion takes place right in the recorder, so it is capturing as fast as the coaxial, balanced twisted-pair, or optical fiber cable is transporting the analog signal.

Analog video systems include a digital recording subsystem. This subsystem accepts analog inputs and digitizes the video.

Digital recorders may or may not use the same frame rate as the capture device. Because of the digital nature of the information, some systems may capture frames at a high frame rate for viewing and record at a different frame rate.

Typical frame rates are 1 f/s, 3.75 f/s, 7.5 f/s, 15 f/s, and 30 f/s. The frame rate for any given application is custom to each situation.

A digital recording system also is capable of using the capture device for motion detection and altering the recording frame rate. In such an application, the system detects changes in the video frame and increases the recording rate only when motion is detected, allowing conservation of storage space.

Digital video recording enables retrieving and viewing video without interruptions in the recording process, scanning video for activity, and viewing cameras over LAN and WAN connections.

DVRs, being analog input devices, will have some resolution limitations, but analog camera resolution is still increasing and will exceed 600 TVL. DVRs offer the user a cost-effective way to get real-time or near real-time recording with a cabling method that is not dependent on network infrastructure.

Network Video Recorders (NVRs)

NVRs represent an important, growing product segment for the deployment of video over both dedicated and shared networks.

NVRs fall into three general classes: embedded devices, recording servers, and portal or recording by an application service provider (ASP) or Internet portal.

The embedded NVR has an embedded operating system and is dedicated to the decoding of multiple video streams, recording of these video streams onto its internal or external hard disk drive media, and streaming either live or recorded video for display on remote computers or workstations.

 © 2012 BICSI®

Network Video Recorders (NVRs), continued

Network disk recorders do not require disk software or file maintenance by the user. Since the operating system is not accessible and foreign software may not be installed in the device, recording resources are dedicated to accepting the video streams, storing them on digital media, and permitting recording review access from end users.

Decoding video streams is a resource-intensive operation. One practice is to allow this to be done by an embedded device instead of a video server. These devices can be directly compatible with high-definition displays and have digital display format interfaces like digital video interface–integrated (DVI-I), digital video interface–digital (DVI-D), or high-definition multimedia interface (HDMI).

NVRs have to multitask—accepting the video stream, writing to hard disk, searching requests by users, decoding complex recordings or live video streams, and running a suite of programs to protect itself from exploits, viruses, and root kits.

This performance is variable and depends on the complexity of the video being decoded (H.264 decoding can be intensive), the number and complexity of user requests, and the number of incoming streams. Modeling server requirements with performance level indicators can help initially select the server, but this process needs to be revisited periodically and during upgrade planning.

NVRs accept the video stream from network cameras. There is nothing that will produce additional frames or pictures once the user has chosen to decrease the video streaming rate at the camera itself.

NVR setup and deployment are design dependent and require physical security professionals with both a knowledge of how their video devices will perform and capture the scene as well as how the NVR (e.g., embedded or server-based) should be programmed to accommodate their needs and help manage risk at their facility.

NVRs will accommodate images and streams sent from high-definition (HD) cameras that would be larger than what the analog input on a DVR can accommodate.

A denial of service (DoS) attack on the network with network cameras and NVRs can be inadvertently created if packets intended for unicast to a multicast address or to a router or network switch are sent that cannot understand them. This traffic will be broadcast to all members of a LAN, even though it was intended for multiple users or NVRs, known as a multicast group.

A protocol known as Internet Group Management Protocol (IGMP) snooping can be used to forward this traffic to a limited set of ports, but the infrastructure must support this. A Layer 3 switch can also get users to join a multicast group by using IGMP messages and reduce the possibility of this happening.

Hard drive storage capacity is always increasing. The higher storage hard drive will lower the cost per camera channel, but it will increase the liability of having so much storage on a single drive.

Network Video Recorders (NVRs), continued

Video Storage Design

The design of the NVR video storage is based upon the following criteria:

- Number of cameras
- Type of recording (e.g., continuous, scheduled, event, motion)
- Image quality
- Image frame rate
- Compression type
- Desired retention time period

Type of Recording

These settings can dramatically impact the required video storage requirements. Continuous recording is all cameras recording all the time. This setting is the most straightforward to calculate the retention time.

A scheduled recording is simply based upon the cameras recording continuously during a predefined time period. For example, a camera can be set to record only at night or during off-hours.

Event recording is based upon a system event or trigger to start the recording of video for a predetermined time or until the event clears. For example, a surveillance camera viewing a secure door can be triggered to record when an alarm is received from that door.

Motion recording is an analysis of the video image based upon a predefined threshold of the amount of change or area of motion in the image that would constitute a detection of motion in the scheme. This detection of motion triggers the video to be recorded with a predefined pre- and post-time period.

Image Quality, Frame Rate, and Compression Type

The image quality, frame rate, and compression type affect the size of the video file required for storage.

Desired Retention Time Period

Many customers will have operational requirements that dictate the required time period to save the recorded video. This period can range from several days to several months. A common design period is 30 days.

Many NVR-based solutions can also be configured in a last in, first out setting.The system basically fills the available storage to a predefined threshold (often 90%); it then deletes the oldest recorded video to free up space for newly recorded video.

 © 2012 BICSI®

Network Video Recorders (NVRs), continued

Video Storage Calculation

The amount of storage required for archiving video signals depends on:

- Number of cameras.
- Resolution (image size).
- Frames per second.
- Type of compression used.
- Percentage of time there is motion in the camera's field of view.
- Length of time the recorded video should be stored.

Number of Cameras

The storage requirement will increase linearly as the amount of cameras increase (e.g., four cameras will require more storage than two cameras if all the other storage parameters remain the same).

Resolution

Resolution determines how much information will need to be stored for each frame of video. The higher the resolution, the more storage it takes up. The ESS designer should first determine the resolution needed. For example, a higher resolution may be needed if identifying someone's face is required; however, a lower resolution may be used if recording that someone walking by is needed.

See Table 5.11 for estimates of frame size, which are based on resolution.

Table 5.11
Frame size estimates

Resolution in Pixels (W x H)	Frame Size in Bytes	Typical Source
352 x 240	10 kB	Internet low-resolution video
704 x 480 (4 CIF)	30 kB	Internet high-resolution video
1280 x 720	60 kB	HDTV 720p resolution
1920 x 1080	80 kB	HDTV 1080p resolution

CIF = Common intermediate format
H = Height
HDTV = High-definition TV
kB = Kilobyte
p = Pixel
W = Width

Network Video Recorders (NVRs), continued

Frame Rate

The number of f/s relates to how smooth the video appears. Video viewed at 30 f/s looks like TV-quality video, but it uses up a lot of storage. For example, if 100 kilobytes (kB) per frame are stored and the frame rate was 30 f/s, a total of 3000 kB per second (100 x 30) (using M-JPEG compression) would be stored. That is 180 megabytes (MB) per minute (3000 x 60) or 10.8 gigabytes (GB) per hour (180 x 60) or over 259 GB per day (10.8 x 24). If recorded at 1 f/s (instead of 30 f/s), only 8.64 GB/day is used. If only used to view people walking around, then 5 f/s or less is adequate. If viewing fast moving vehicles, then 15–20 f/s may be required.

Motion Detection

The storage requirement can be reduced by using motion detection. Motion detection can be enabled on the camera from the video management software. In this case, the video is recorded only when motion is detected. For example, if motion is not detected 25 percent of the time, the storage requirement is reduced by 25 percent.

Compression Used

The compression codec (e.g., MPEG, JPEG, MPEG4 [H.264]) will determine how the video images are compressed and transmitted between the camera and the recorded media. H.264 improves the compression by only transmitting the difference between one frame and another. For example, if a person is walking in a field, then the camera only sends a picture of the person walking and sends the complete picture only once in a while. This can significantly reduce the amount of data transmitted and stored.

Length of Time

The amount of storage required increases the longer video is saved. But video can be stored for a period of time and then recorded over, decreasing the overall storage amount. For example, if video is stored for two days, at the end of the second day new video would start, replacing the video that was 48 hours old.

Sample Storage Calculations

The following are sample calculations to determine estimated video storage requirements:

Number of cameras =1
Storage frame rate = 8 f/s
Storage resolution = 4 CIF (704x480), 30 kb/frame
Storage per sec= 8 f/s x 30 kb/frame = 240 kb/s
Storage per min = 240 kb/s x 60 sec/min = 14.4 Mb/min
Storage per hour = 14.4 Mb/min x 60 min/hr = 0.864 gigabit (Gb)/hr
Storage per day = 0.864 Gb/hr x 24 hr/day = 20.7 Gb/day

Storage requirements = 20.7 Gb/day or 20.7 Gb/8 bits per byte = 2.6 GB per day with 100% motion

The above storage represents 100 percent recording, reduced by the percentage of motion anticipated in the camera's field of view. The above example would require 1.3 GB per day if 50 percent motion is expected.

 © 2012 BICSI®

Monitoring Devices

Monitors used for surveillance are essentially TV monitors, typically without tuning or audio capabilities. These video-only displays accept various forms of video input from a camera, switcher, or recording device and convert it back into a visible picture on the monitor screen. The monitor is the human interface for the VSS.

The capability of the surveillance monitor to provide an accurate image clear to the human eye is the key to any VSS. The security guard's success is dependent on the ability to accurately observe images on the monitor.

Monitors may be divided into four groups:

- Monochrome
- Color
- Video graphics and text
- Audio and video

Each category of monitors is specially suited for one or more applications. Surveillance applications typically use monochrome or color monitors.

Monochrome monitors are designed to display a continuous range of light intensity, commonly referred to as halftones or gray scales. Computers use video graphics and text monitors and are designed to display color hues with a higher purity.

The size of the monitor does not necessarily indicate the quality of the image. Since in the United States all security monitors have 525 lines of resolution, the vertical resolution is essentially the same regardless of the screen size. Horizontal resolution may vary, but it is primarily determined by bandwidth.

IMPORTANT: The primary consideration when selecting a monitor is to ensure that it has a resolution equal to or greater than the output of the camera or of the transmission link.

Monitoring Devices, continued

For many years, the options for security monitors were limited to cathode ray tube (CRT). Advances in technology have generated a variety of displays to choose from, including:

- CRT.
- Plasma.
- Liquid crystal display (LCD).
- Digital light processor (DLP).
- Touch screens.
- LED.
- Organic light-emitting diode (OLED).
- Projection.

NOTE: See Chapter 8: Notification, Communication, and Display Devices for additional information.

Monitor Location Methodology

The elements that must be considered when planning to locate monitors associated with a surveillance system are:

- Number, type, and quality of monitors.
- Integration with other systems.
- Physical arrangement of monitors.
- Ability to view in multiple locations.
- Sequencing and matrix or multiplex switching.
- Virtual or manual matrix switching of video cameras.

The ESS designer must consider the number of locations where cameras are mounted and decide whether to dedicate one monitor to each camera or use sequencing or split screens. Other considerations include the monitor types and performance, the volume of pedestrian or vehicular activity, the history of criminal or undesirable activity, and the likelihood of future incidents.

These factors also will influence the selection of the size and design of the monitor array. A 125 millimeter (mm [5 inch (in)]) monitor placed 1.83 m (6 ft) from the monitoring station, sequencing through eight cameras per minute, may not provide adequate time and image quality to detect crime or other undesired events.

 © 2012 BICSI®

Monitor Location Methodology, continued

The following factors must be included in the monitor array design to address operator fatigue:

- Positioning of the monitors
- Distance between the monitor and the operator corresponding to the size of the monitor
- Height of the monitor's placement above the floor
- Monitor's position within the array

Considering the human factor in the monitor array design will result in a visualization system that is efficient and effective while meeting operators' ergonomic requirements.

Video Surveillance Systems (VSS) Layout and Distribution Concept

There are a number of different ways to distribute analog and IP video monitoring, recording, and control systems. The distribution concept can be either local or remote distribution:

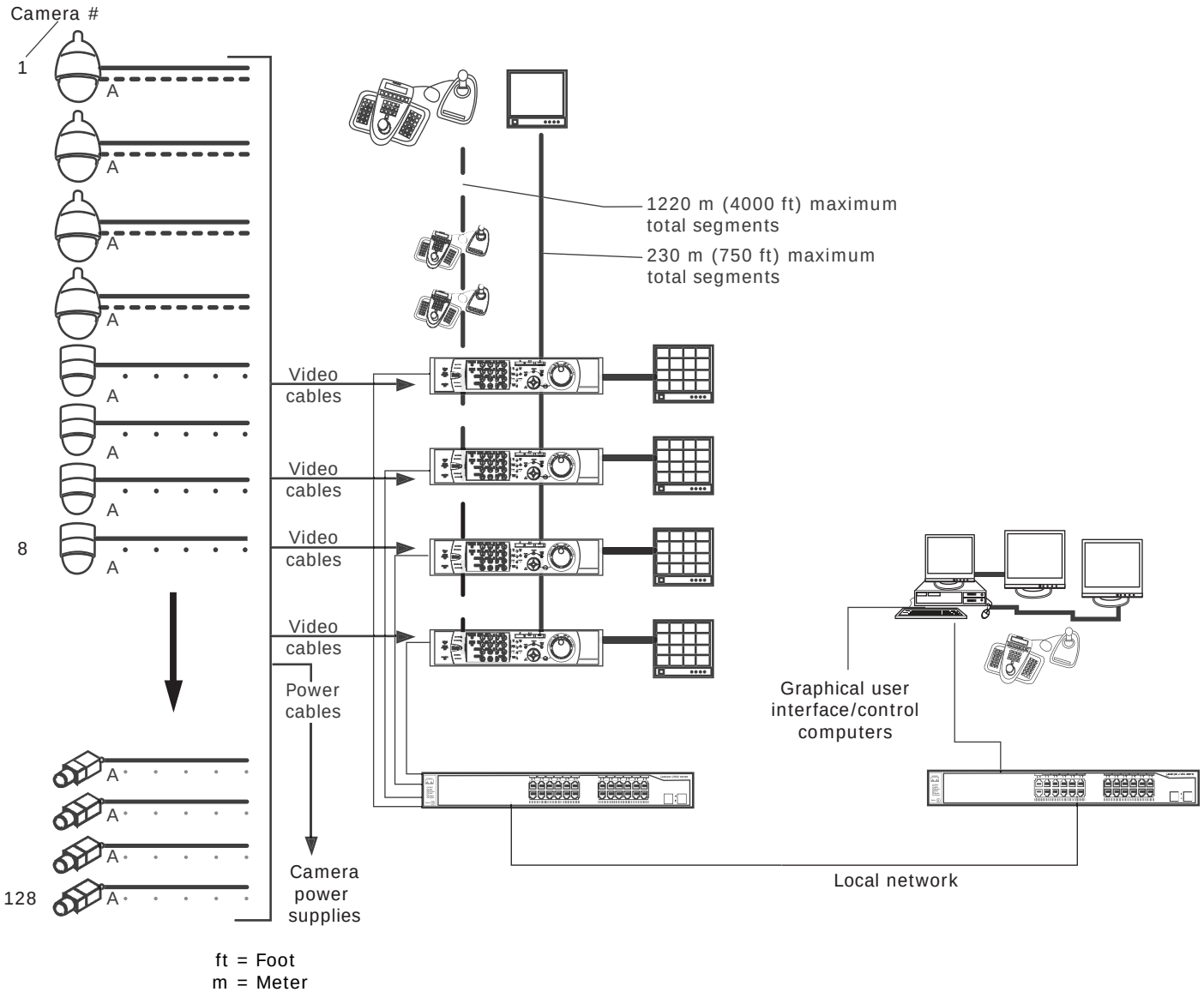
- Local distribution occurs when the monitor and control devices reside in the same space, such as an operation center. In this instance, the system can only be monitored from this single location.
- Remote distribution is when video is pushed from a control location to a remote area for viewing purposes, such as mounting monitors for viewing at a guard booth. It can also include monitoring from certain identified workstations and monitoring via IP from select locations.

These applications are based on the type of monitoring software and recording devices specified by the ESS designer.

Video Surveillance Systems (VSS) Layout and Distribution Concept, continued

Most applications that require access to monitored or recorded video by individual users may be handled by single or multiple DVR systems as shown in Figure 5.10.

Figure 5.10
Analog system without matrix switch

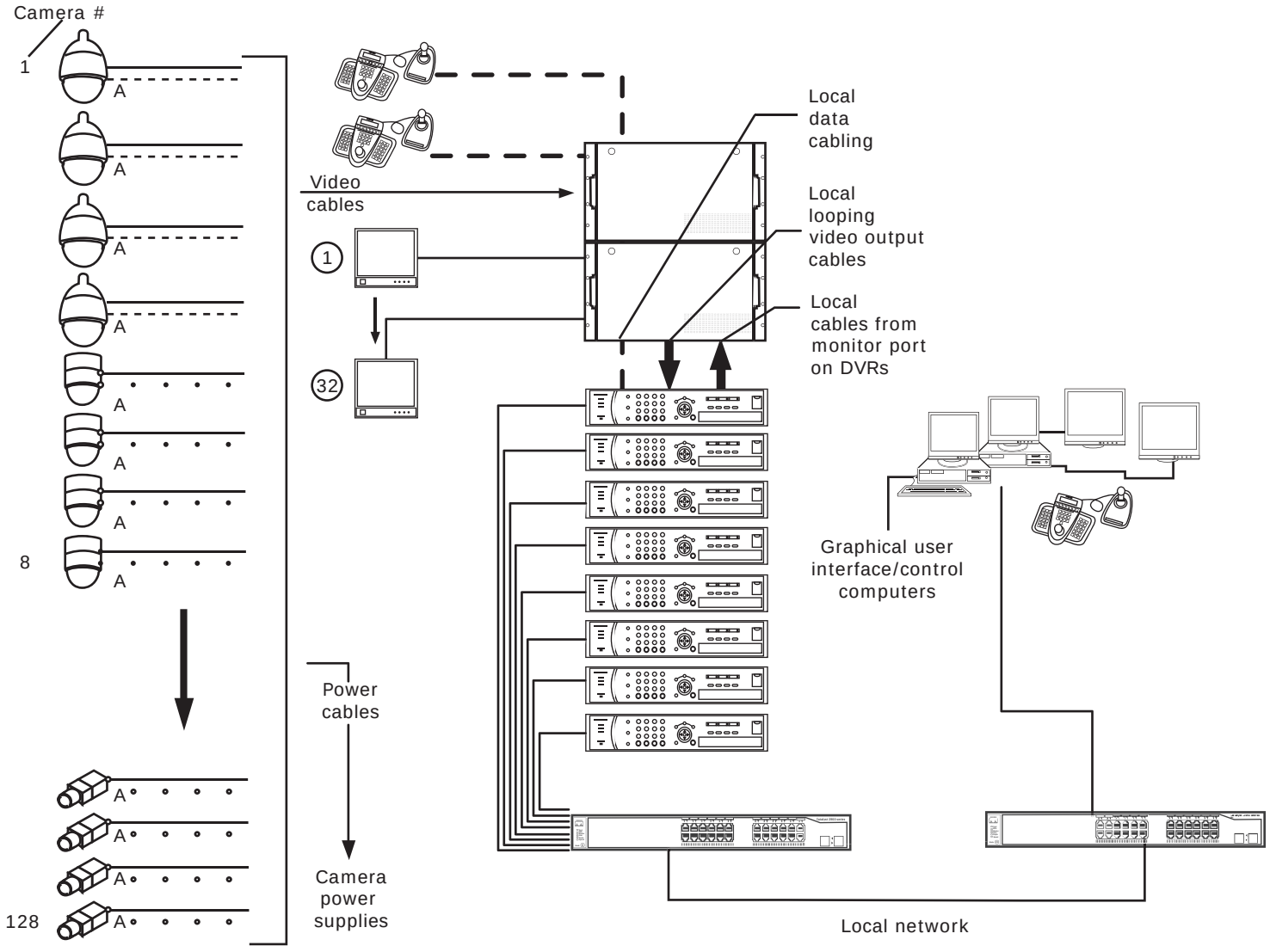


 © 2012 BICSI®

Video Surveillance Systems (VSS) Layout and Distribution Concept, continued

Should the system grow larger and require fixed multiuser locations, a matrix analog switching system may be used together with the DVRs as shown in Figure 5.11.

Figure 5.11
Analog system with matrix switch



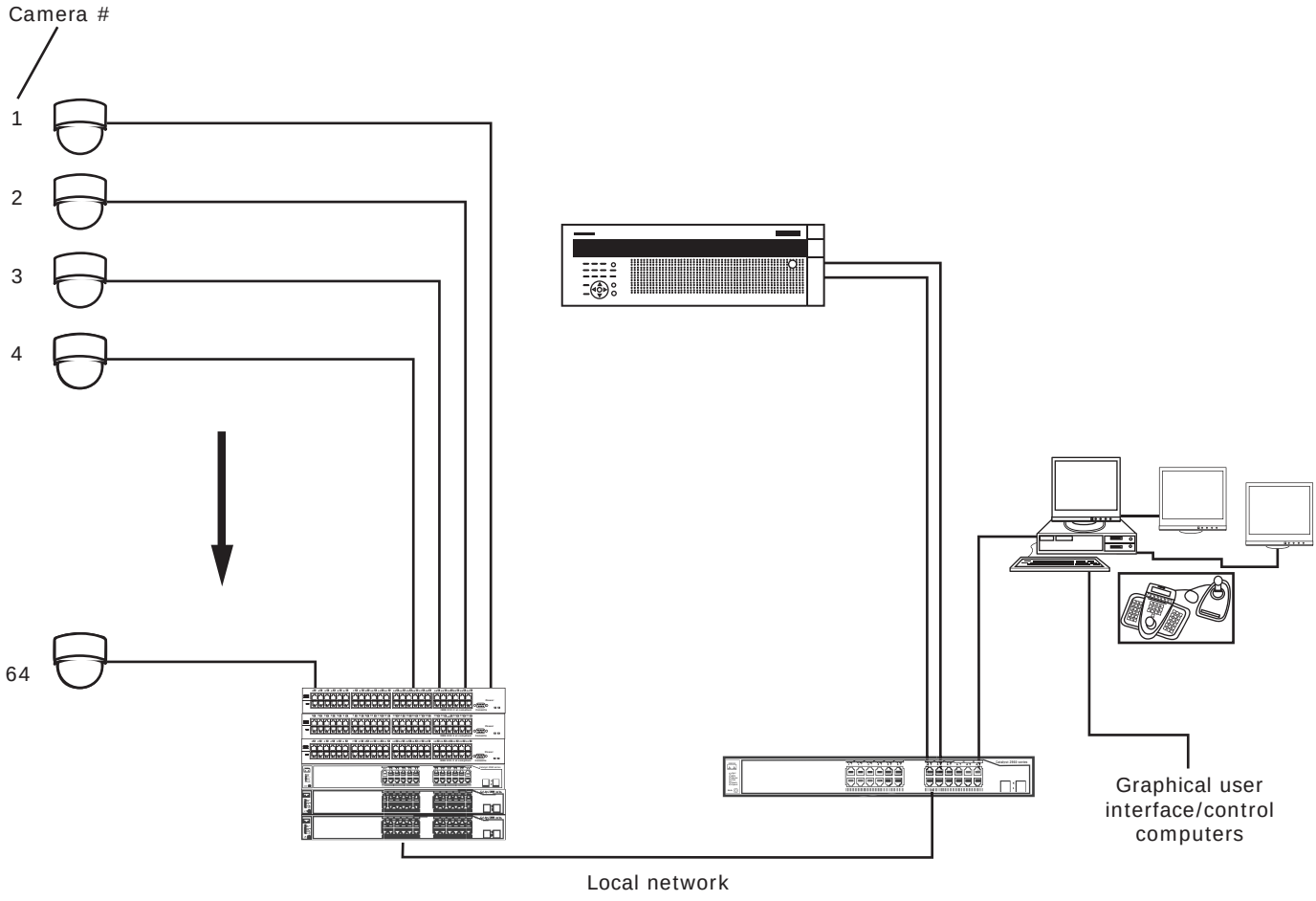
DVR = Digital video recorder

Video Surveillance Systems (VSS) Layout and Distribution Concept, continued

When multiple users require simultaneous access, a digital matrix system may be used to provide the most consistent means of delivering video feeds and access to recordings.

IP-based systems can use either embedded network video recording systems or recording servers (see Figure 5.12).

Figure 5.12
Internet protocol video system embedded recording

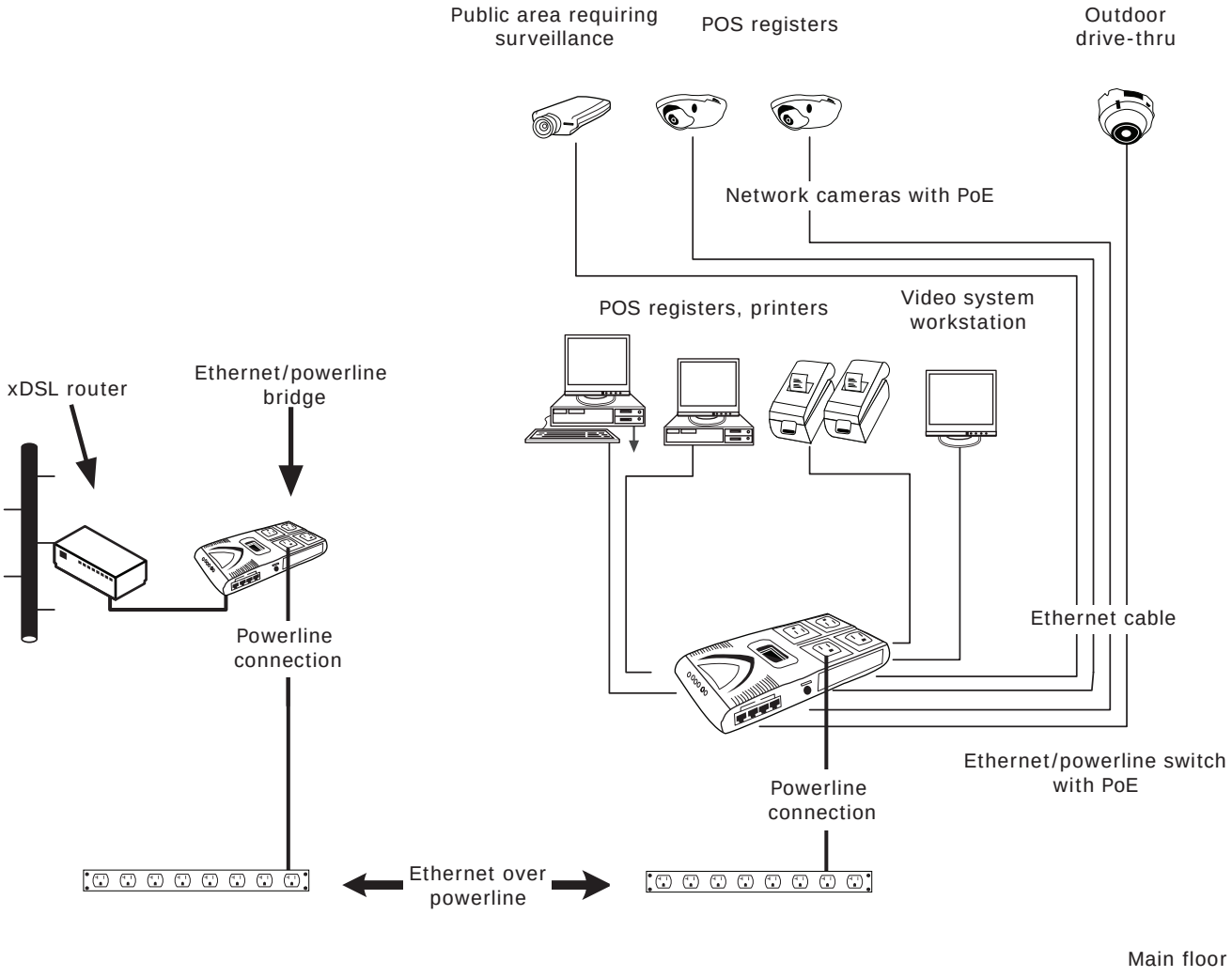


 © 2012 BICSI®

Video Surveillance Systems (VSS) Layout and Distribution Concept, continued

The hybrid system can support both analog and IP cameras on a single platform (Figure 5.13).

Figure 5.13
Network video system for point of sale applications

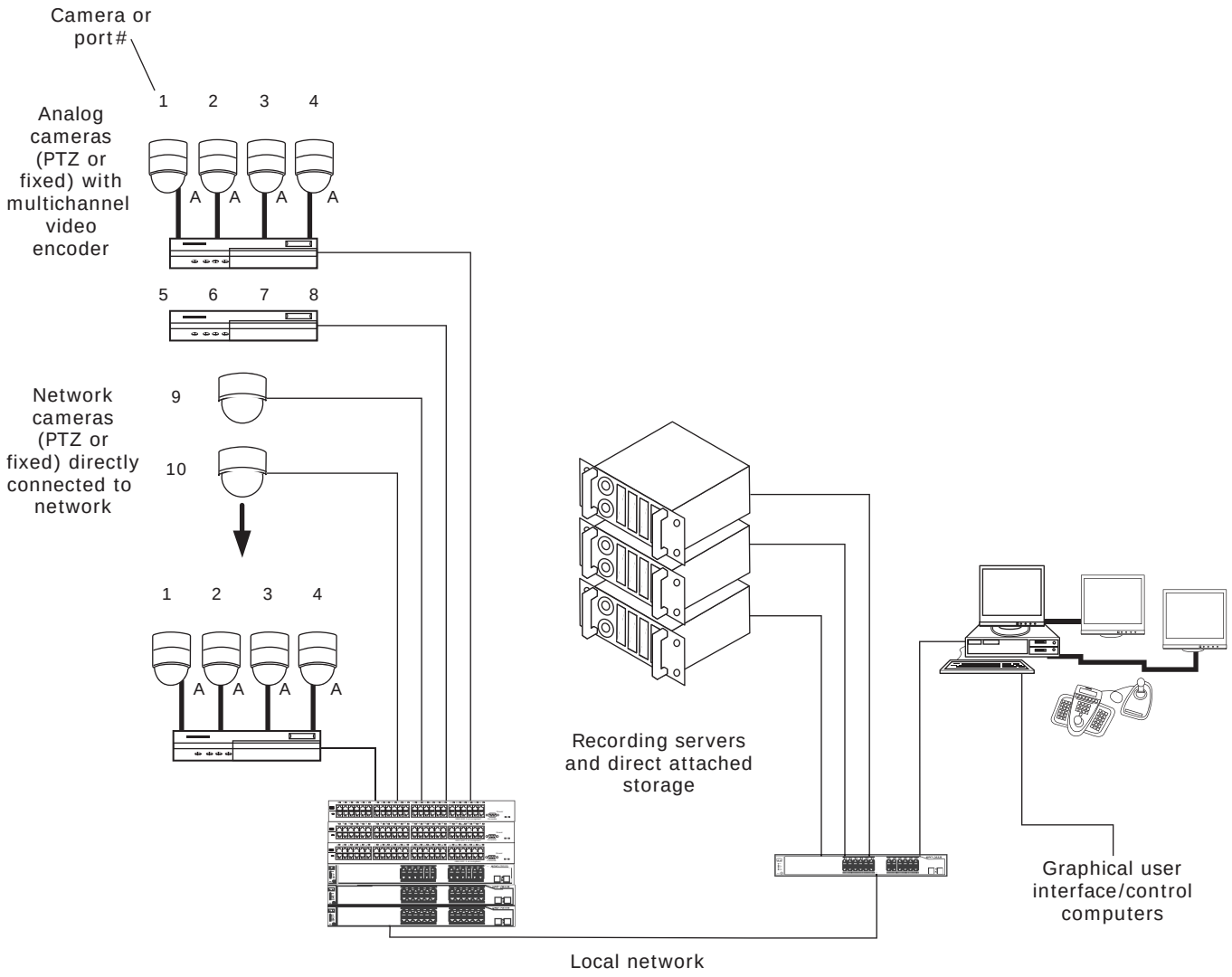


PoE = Power over Ethernet
POS = Point of sale
xDSL = X digital subscriber line

Video Surveillance Systems (VSS) Layout and Distribution Concept, continued

A hybrid IP video system with a recording server is shown in Figure 5.14.

Figure 5.14
Hybrid Internet protocol video system with recording server



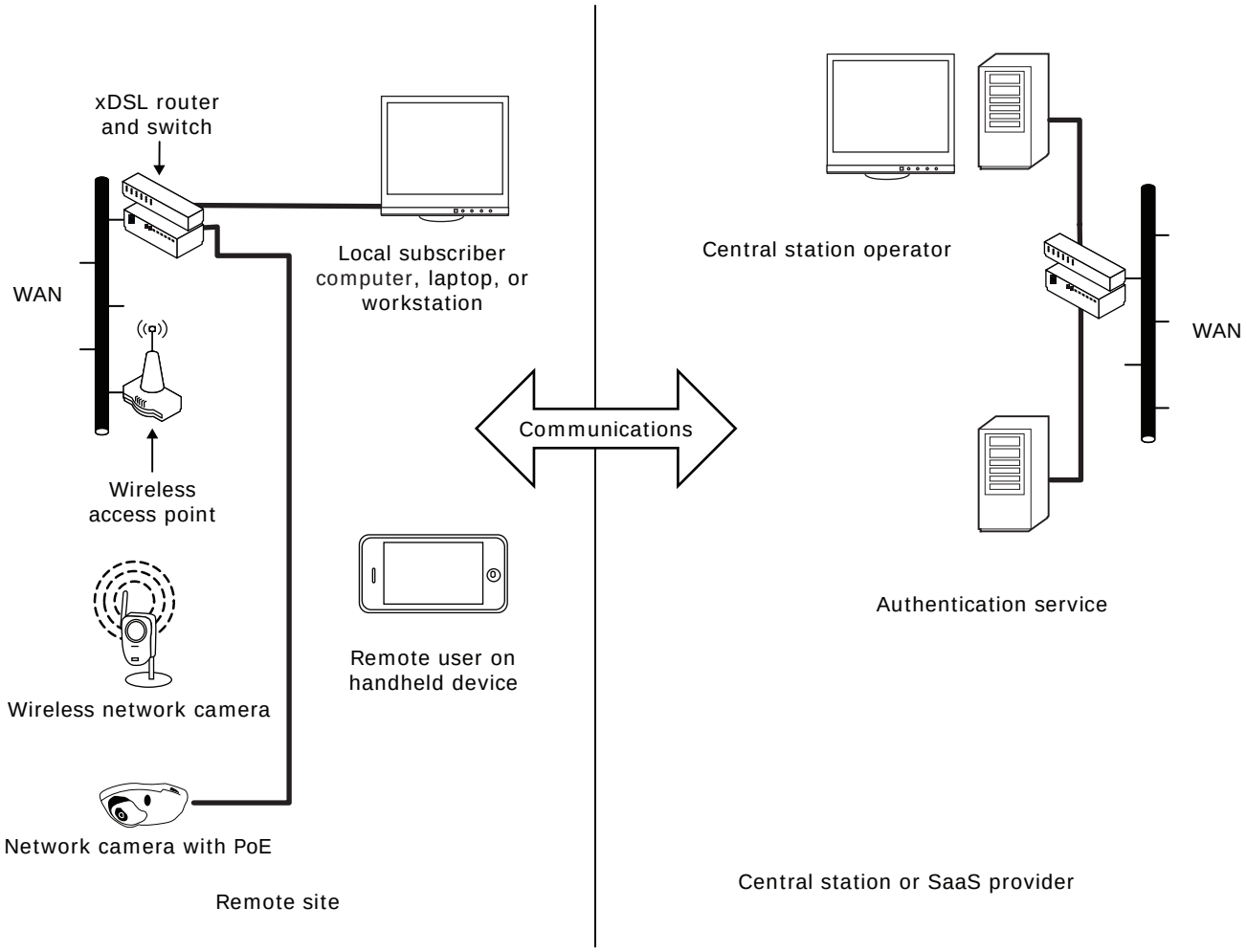
PTZ = Pan, tilt, and zoom

 © 2012 BICSI®

Video Surveillance Systems (VSS) Layout and Distribution Concept, continued

A remote network video monitoring system using a SaaS is displayed in Figure 5.15.

Figure 5.15
Remote network video monitoring system using software as a service



PoE = Power over Ethernet
SaaS = Software as a service
WAN = Wide area network
xDSL = X digital subscriber line

Software as a Service (SaaS) or Application Service Provider (ASP)

The ability to store and manage video content streamed from IP cameras at an online location has great advantages for certain multisite end users.

With a SaaS-based digital video management system (DVMS), the IP camera streams directly to an online storage location. The user then subscribes to an online, portal-based service to access the video content and run searches and various video analysis tools. The ESS designer should consider any privacy issues when considering the online SaaS.

The SaaS can represent a substantial cost savings over a conventional DVMS, both short and long term, as the product investment costs are greatly reduced.

A variant of the SaaS is the use of local storage and an online portal to process video searches and analysis.

Hardware Control System

Examples of hardware control systems include controller keyboard and mouse, modules with push-buttons and jog shuttles, and miniature displays and touch screens. These require no computers or servers to operate or program and are often desirable when simplicity of use and maintenance is a requirement.

Digital Matrix

A digital version of the previously described analog video matrix, this system class always uses some type of CPU to process the following types of typical transactions:

- Camera to monitor(s) call up
- Camera control
- Alarm process and acknowledge
- Recorder control and video playback
- Video event search
- Graphic map display

The main difference is that all commands may be processed over a network, and switch streams of video to workstations or monitors paired with decoders. This is analogous to the analog version of switching hardwired video feeds through a cross-point analog matrix.

Digital matrix systems depend on various protocols in order to minimize bandwidth use and allow for a minimum of delay for controlling cameras and switching video feeds. Some protocols include IP multicast and IGMP.

 © 2012 BICSI®

Digital Video Management System (DVMS)

This system class manages video content. One way to tell the difference between a digital matrix and DVMS is to see if the system can:

- Search for video independent of selecting the actual video source but relating the search to a common parameter such as a general area that might contain video cameras or that is within the video cameras' field of view.
- Process video searches containing multiple parameters and search criteria like start and end dates, video motion, removal of objects, and duration of object within a certain location.
- Perform analysis on video, such as on LPC devices through the use of LPR algorithms.
- Move and manage video content to and at various locations depending on the users' requirements.

Step-by-Step Approach to System Selection and Deployment

The ESS designer is encouraged to use the following framework for designing an analog or IP video system. Each of the individual tasks is presented as an overview and may require additional detail.

Step	System Selection and Deployment
1	Plan. • Consider where the site survey fits in the scheme of a physical security program. • Advantages of the assessment process: – Preassessment phase: • Identify what is to be assessed. • Protect this key information with procedures. • Identify and rank the critical assets. – Advantages of conducting the assessment and survey: • Increase awareness, not necessarily paranoia. • Establish a baseline. • Identify the vulnerabilities, and develop responses. • Identify the key assets that will drive the risk management process. • Promote an action to minimize risk. • Kick off a physical security program (in this case, a VSS). – Assessment: • Analyze the network architecture. • Assess the threat environment. • Test and try to defeat the system. • Assess the physical security (see the site survey). • Conduct a physical asset analysis. • Assess the operations security. • Examine the policies and procedures. • Conduct an impact analysis. • Assess the infrastructure interdependencies. • Conduct a risk characterization. • Identify risks: – Are there any physical vulnerabilities to infrastructure? – Can unauthorized users enter main wiring facilities? – Are there logical or user vulnerabilities to infrastructure? – Is there protection against system attacks from within facility?

 © 2012 BICSI®

Step-by-Step Approach to System Selection and Deployment, continued

Step	System Selection and Deployment

- Postassessment (after project deployment):
  - Prioritize recommendations.
  - Develop an action plan.
  - Capture the lessons learned and best practices.
  - Deploy a video system.
  - Conduct training.
- Identify the system types to match and minimize the risk types:
  - Classify video system by type:
    - Observation
    - Investigation and forensic review
    - Recognition of objects such as human faces and license plates
    - Prosecution
    - Loss prevention and deterrence
    - Intrusion detection and perimeter monitoring
    - Access control
    - Operations management and resource allocation
    - Safety
    - Security/video surveillance (monitoring function)
- Conduct site survey:
  - Assess lighting conditions.
  - Associate a function to a camera:
    - Monitoring
    - Detection
    - Identification
    - Recognition
    - Access control
  - Note the environmental conditions and possible vandalism:
    - Viewing angle
    - Environment
    - Lighting type, level
    - Reflectance/emissivity
    - Obstructions
    - Temperature
    - Humidity
    - Corrosives

Step-by-Step Approach to System Selection and Deployment, continued

Step	System Selection and Deployment

- Water
- Vandalism

– Note the mounting conditions:

- Cabling entry
- Requirements
- Accessibility

– Note the special objects/scenes:

- Vehicles
- License plates
- Shoreline/border
- Transit platforms

- Video site survey cycle:
  – Enter the site survey data (rough sketches, location notes).
  – Use a standard site survey sheet.
  – Normalize the devices by camera types.
  – Transfer to the floor plans.
  – Verify samples with actual site conditions (see below task).
- Verify all monitoring and recording functions using the ISO12233 I3A/ISO, Rotakin®, or other accepted standard:
  – Adjust the system as necessary for key areas, adding, or moving cameras as required.
  – Sample the equipment for video site survey and test:
    - Laptop computer
    - Fixed box type IP camera
    - Long Ethernet stranded crossover cable
    - Assortment of varifocal lenses
    - Tripod/ball head for camera
    - Light meter with gray card
    - ISO12233 I3A/ISO standard test target chart
    - LED IR illuminator/power supply

 © 2012 BICSI®

Step-by-Step Approach to System Selection and Deployment, continued

Step	System Selection and Deployment
2	Select camera types and imaging requirements. • Match camera function and desired resolution. • Assess difficult lighting conditions: – High contrast (dynamic imaging use) – Day/night switchover – Automatic back focus – Image stabilization requirement • Imager resolution size: – Match the resolution size also with required bandwidth allocation. – Megapixel IP cameras can require substantially more bandwidth. • Consider the use of certain technologies to aid identification: – Consideration in the site survey process. – Face location/face detection. – Automatic tracking/automatic zoom with PTZ cameras. – Use of dynamic imaging/backlight compensation for high-contrast lighting situations. • Deploy PTZ cameras to match the monitoring requirements, especially in larger coverage areas, for manual monitoring or to be activated by alarm conditions. • Deploy immersive imaging lenses for a virtual PTZ experience if applicable. • Select compression type by monitoring, user, bandwidth, and functional requirement: – MPEG-4 and H.264 for monitoring and multicast compatibility. – JPEG for higher resolution recording. • Use lens estimator to size lens: – Enter scene height, width, and distance for each camera. – As an alternate, note actual viewing angle on scaled diagram. – Determine object height on monitor to match functional requirement. – Determine focal length.
3	Determine initial system selection type. • Match number of cameras to recording system type: – An example of a small network or IP-based video system is one with eight or fewer network cameras connected to a small embedded type of NVR and monitored or reviewed at one or two workstations.

Step-by-Step Approach to System Selection and Deployment, continued

Step	System Selection and Deployment
	– A midsize IP video system with multiple NVRs capable of handling higher throughput, more users, and managed from a single or multiple workstations. – Should the need arise to connect existing or specialized analog cameras, use a hybrid analog and IP-based system. • Choose between embedded system and server-based system: – Embedded systems usually have no camera licensing costs, have a fixed network throughput, and offer exclusive file protection through a proprietary operating system. – Server-based recorders require camera or software licenses, have variable network throughput, require additional software to protect files, and require an advanced skill set to maintain. – Verify camera protocol compatibility if using server-based recorder. • Determine recorder capacity. • Match recorder type and quantity with number of users accessing the video information. • Match network switch type with unicast or multicast requirement and number of users.
4	Develop bandwidth/network/routing maps. • Develop bandwidth measurement scenarios. • Note individual camera bandwidth values, and use camera and recorder bandwidth calculators as required. • Accumulate to nearest network switch—apply totals. • Accumulate multiple network switch bandwidth—apply totals. • Accumulate total camera bandwidth for each network video recorder—apply totals. • Perform user identification by function. • Note individual user monitoring station bandwidth values. • Accumulate to nearest network switch—apply totals. • Accumulate typical multiple user monitoring station bandwidth values for each NVR—apply totals.
5	Verify infrastructure compatibility and protocol support. • Cable infrastructure needs to support bandwidth capacity requirement. • Cable installation and cable quality significantly impact data rate. • Wiring plant topology and network switches need to support placement of security and surveillance system devices. • Deploy PoE systems effectively to complement the system's requirements.

 © 2012 BICSI®

Step-by-Step Approach to System Selection and Deployment, continued

Step	System Selection and Deployment
6	Apply topology requirements.
7	Encourage convergence, and use professional imaging over networks using the most qualified and professional product possible. Make the video available to as many users as possible who have permission to view and control the video streams.
8	Make resolution adjustments as required to meet end user requirements; revise bandwidth allocation maps.
9	Verify recording, control, and management system design. • Verify recording system utilization with recording streams, monitoring users. • Make sure users have the live and recorded image quality they need. • Maintain the most favorable criteria for the project. • Maintain the lowest reasonable cost for system. • Increase the number of ways the video information can be accessed. • Strengthen and secure the network devices. • Do not have one device service, too many users, or perform many functions—improve system survivability. • Model all network-based systems prior to deployment, and correct the system design as required (see below).
10	Check common network usage scenarios. • Recording system utilization with recording streams, monitoring users. • Network switch functions to support bandwidth load and failure scenarios. • Provide recovery from the most common and reasonable infrastructure failures. • Simulate as many network conditions and loads as possible for components, edge devices, and infrastructure.
11	Develop a comprehensive performance specification for a video-based surveillance system, and verify inclusion of construction specification institute sections.
12	Publish a network video commissioning statement to specify the system deployment. • Step-by-step staging, programming, installing, and commissioning tasks. • Division of responsibilities. • Acceptance test criteria.

Step-by-Step Approach to System Selection and Deployment, continued

Step	System Selection and Deployment
13	Preproject diagram development. • Security block diagram. • Data closet design. • Camera schedule. • Camera detail. • Riser diagrams. • PTP diagrams. • Command center elevations and stretchout. • Command center sequence of operations by scenario are usually required for the planning and design phases of surveillance project; all other diagrams are required for installation and commissioning phases.
14	Develop master bill of material (BOM). • Camera BOM. • TR BOM. • Control system BOM. • Workstation BOM. • Command center BOM.
15	Project diagram development. • Security block diagram (update as required). • Data closet design (update as required). • Camera schedule (update as required). • Camera detail. • Riser diagrams. • PTP diagrams. • Command center elevations and stretchout (update as required). • Command center sequence of operations by scenario.
16	Project management.
17	Testing.
18	Video-based acceptance test.
19	Framework for continuous performance verification includes performance testing metric and positive influence against possible legal challenges to video evidence.
20	Training.

 © 2012 BICSI®

Support Infrastructure

VSS infrastructure requires:

- Conditioned space.
- Power source.
- Power distribution.
- Surge protection.
- Bonding and grounding (earthing).
- Alternate power source.
- Pathways (junction box and conduit).
- Other support elements.

The ESS designer should consult the AHJ to understand code implications during the design of surveillance and other ESS systems.

The following sections will cover the suggested requirements for a complete design.

Conditioned Space

The ESS designer should refer to the latest edition of BICSI's *TDMM* for details about the design of TRs and equipment rooms (ERs).

ESS systems require conditioned spaces related to:

- Dust and static electricity.
- Environmental control (heating, ventilating, and air conditioning [HVAC]).
- Fire protection.
- Floor loading.
- Grounding (earthing).
- Lighting.
- Location.
- Pathways.
- Power.
- Security.
- Size.
- Wall linings.

Power Source

The ESS designer should refer to the *TDMM* for design requirements concerning branch circuits for equipment power. These circuits must be dedicated, unswitched, and installed in accordance with the electrical codes.

With the help of other professionals, an ESS designer has to coordinate the interconnection between the power source and the equipment.

This might include:

- The location of hardwired connection points.
- Exterior cameras requiring local power.
- Quantity and configuration of receptacle connection points.

Power Distribution

Video surveillance cameras are typically powered by either 12 Vdc or 24 Vac power supplies. Voltage drop should be considered when determining the distance from the camera 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 surveillance cameras to multifused 12-24 Vac/dc power supply centralizes the power sources for multiple surveillance cameras and surveillance accessories. This is in lieu of having ac outlets installed near each camera device. Voltage drop and wire size must be considered for each individual camera 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 camera or accessory is ac powered individually, more uninterruptible power supply (UPS) circuits are required than a multifused power supply. A multifused power supply also simplifies placing a UPS circuit to one source for the multiple cameras or accessories.

PoE can be utilized as a powering source for IP cameras subject to:

- Distance from the power source.
- Capacity of the power source.
- Power requirements of the camera.
- Power requirements of the accessories (e.g., housing, heaters, blowers).

Surge Protection and Lightning Arrestors

The ESS designer should provide protection against spikes, surges, noise, and other line problems for all system equipment and components.

The ESS designer also should protect all exterior video, control, power, signal cables, and conductors against power surges and lightning. Video surge protectors must not attenuate or reduce video and sync signals under normal conditions. Each surge protector should be nationally recognized testing laboratory (NRTL) listed.

 © 2012 BICSI®

Bonding and Grounding (Earthing)

The ESS designer should refer to manufacturer's recommendations, the latest edition of the code adopted by the AHJ, and the latest version of the *TDMM* for more information.

Alternate Power Source

The ESS designer should evaluate power sources to ensure that they are reliable and capable of providing a degraded mode of operation in the event that primary utility service is lost. Such power sources may be:

- Internal UPS.
- External UPS.
- Local generation.

The evaluation should also review the alternate power source's capacity and system load to determine the operational run time while in the degraded mode. The ESS designer should assess and document the selection of the critical elements of the VSS provided with an alternate power source.

ESS systems that use an internal UPS have an integrated battery backup within the equipment enclosure. External UPS systems are stand-alone systems that may be either hardwired or cord-and-plug connected to the building's power distribution.

Pathways

The ESS designer should refer to the codes and standards for pathway considerations, including the latest edition of the code adopted by the AHJ, the *TDMM*, and the appropriate standards.

The ESS designer should consider installing devices and media in enclosures or conduit for security and protection based on the environment.

Other Support Elements

The *TDMM* lists several means and methods for supporting system components.

A number of elements may be introduced to increase the overall reliability and resiliency. Related design elements may include resilient and backup power, multiple and backup transmission paths, and multiple cameras that create overlap.

Video Surveillance Systems (VSS) Interoperability Methods and Practices

In the security industry, there are common practices for interoperability that apply to VSS. They involve various participants in the project process and are outlined below.

Security device manufacturers (e.g., video camera, recorder, application) participate in common video interoperability practices.

These practices allow IP video camera streams to be decoded by video recording systems. The video camera device manufacturer prepares an SDK, a common gateway interface (CGI) command set, and an API to allow for easier integration into NVR devices, DVMSs, ACS, building automation systems, and physical security information management (PSIM) systems.

Each manufacturer has a process of certification of an individual IP video camera device to ensure consistent interoperability for a specific device's firmware or software release. The system integrator has an approach to video integration that incorporates additional tasks in the project management process:

Consider the device to system interoperability task in the commissioning process:

- Standardize and freeze specific device and system versions for the life of the project and avoid untested device and system versions.
- Consider standardizing the selection of physical and logical network devices (e.g., network switches, midspans, routers).
- Verify physical and logical network device/system compatibility with each IP video device and system manufacturer.
- Consider deployment in dedicated and shared infrastructure.

Best Practices in Video Deployment

When considering the design and selection of a VSS, ESS designers need to consider the individual needs of each market they are working with. The following are intended as examples only, and each market's own requirements are to be verified on a project-by-project basis.

In-car and transit VSS often use wide view surveillance products for identification. This application can require ruggedized, removable digital media for video storage. Retail video and loss prevention video solutions incorporate point of sale (POS) transaction data (e.g., electronic journal) with digital video images of events for simultaneous viewing and proof of a given transaction.

In addition, these systems may incorporate:

- Input from one or multiple POS or ATM machines via RS-232 interface or Ethernet.
- Simultaneous viewing of time-linked transactions and multiple video cameras.
- Transaction searching and go to next or previous match.
- Print transaction reports of retail shrinkage events with linked video images.

 © 2012 BICSI®

Best Practices in Video Deployment, continued

A VSS deployed in an energy environment or power plant requires products that may be initially more expensive, but they have longer lives and low maintenance requirements. Maintenance and reliability are key drivers for product selection as the labor to maintain the video devices and infrastructure is expensive.

For retail and corporate banking video applications, flexibility, the lowest qualified cost, and the ability to produce excellent images for forensic purposes are key requirements. Specific video analytics for this market have been developed and may be considered where applicable. One such analytic includes the recognition of people loitering in the retail financial institution's lobby.

Urban and city center VSS have specific requirements that may include:

- Low-light capability for all outdoor public video surveillance devices.
- Cameras capable of producing high-resolution video images and the addition of a video analytics subsystem where required.
- Compatibility with optical fiber or wireless transport system.
- Consideration of privacy and any public surveillance restrictions by the AHJ.

For public arenas, the use of cameras capable of producing high-resolution video images and the addition of a video analytics subsystem may be useful.

For the purposes of identifying indoor and outdoor crowd disturbances, low-light and IR-compatible cameras offer a relatively low-cost alternative to providing enhanced lighting. Other system goals may be to minimize PTZ camera control delay and video switching delay and to provide ease of expansion to accommodate specialized surveillance of visiting dignitaries.

Residential video systems are generally low cost, WAN-friendly, and designed for periodic, not continuous, use. As in the case of urban and city center surveillance, the ESS designer is cautioned to consider privacy and any public surveillance restrictions by the AHJ.

Some gaming video surveillance solution devices and system highlights may include:

- Continuous duty video camera devices (e.g., PTZ drive motor reliability).
- High-resolution imaging, especially in high-ceiling areas.
- Accurate color reproduction under a variety of lighting conditions.
- A control system with minimal camera control and switching delay.
- A DVMS with instant replay capability for multiple operators and cameras.
- Redundancy of all operation and equipment capabilities required, especially in high-stakes areas.

Managing the Video System

The ESS designer should take into account the project management and physical security management process when considering a VSS.

Some issues to consider in convergence of physical security and IT in VSS include:

- The union of physical and IT resources has a significant effect on video systems.
- Preventing the end run around policies by organization partners:
  - Physical security perspective
  - IT perspective

In the upgrade choices for the ESS designer and user, consider these issues:

- Interoperate, integrate, and interface
- Postpone interoperability:
  - Ramifications
- Upgrade or choose interoperability:
  - Ramifications
  - Process
  - Running concurrent systems
  - Quality of service or fault tolerance
  - Logical and network security issues for integration

When and how to upgrade can have an impact on the design process. The ESS designer is encouraged to model the design in various situations the user is planning to experience or some situations that have not been considered.

Technology is continually evolving, and end users will continue to rely on the ESS designer to interpret which technologies are innovative and how they may be integrated into their VSS.

 © 2012 BICSI®

Common Terminology

Some of the terminology commonly used in the surveillance industry is defined below.

Internet Protocol (IP) or Network Video

Video over Internet Protocol (IP)

Video over IP is the deployment of video information over a network that conforms to the OSI layer model. This includes support of cameras and encoders transmitting using various protocols (e.g., TCP/IP, UDP, FTP).

Devices that stream video over IP networks transmit frames and packets of video data to a single location or multiple locations for different purposes. A device like a network video camera or multichannel video encoder can send a video stream to a single network video recorder or video decoder location or to multiple locations of the same type of equipment.

Network Video (Internet Protocol [IP]) Camera

This is a device that produces a video image and encodes it for streaming over a network. This device combines a lens, imager, digital signal processor, and D/A converter in a single package. The network video camera will, at a minimum, include an Ethernet connection for the network.

If this is a remotely positionable camera with PTZ lens capability, the camera's position is controlled via commands sent from a user's computer or network recording/control command center directly to the camera over the network. In addition, the network PTZ camera may have an input/output or serial connector for an additional means of positioning control.

If the device is IEEE 802.3at compliant, the power is sent over the Ethernet cable; otherwise, the low-voltage (usually 12 Vdc or 24 Vac or both) connections are used for power.

Multichannel Video Encoder

This device converts video from analog cameras into multiple video streams that may be accepted by the network recording/control command center. It is usually a four-channel device that may be placed near the analog camera or at some distance to accommodate placement in a TR.

Video Decoder

This device decodes video streams for direct connection to a composite analog monitor or for direct display within a software application. This device is usually located at the network recording/control command center. It can be a four-channel device where each output channel may represent a different incoming video stream.

Internet Protocol (IP) or Network Video, continued

Network Disk Recorder or Network Video Recorder

This device usually has an embedded operating system and is dedicated to the decoding of multiple video streams, recording of these video streams onto its internal or external hard disk drive media, and streaming either live or recorded video for display on remote computers or workstations. The device may have direct attached storage. Network disk recorders do not require disk software or file maintenance by the user.

Network Video Recording Server

This device usually has a distributable operating system (e.g., Windows XP, Windows Server) and is dedicated to the decoding of multiple video streams, recording of these video streams onto its internal or external hard disk drive media, and streaming either live or recorded video for display on remote computers or workstations. The device may have direct attached storage of variable capacity. Video recording servers require operating system, disk software, and file maintenance by the user.

Unicast versus Multicast Video Streams

This device sends frames or packets of video information directly to a single IP-based device for display or recording and does not involve a multiple distribution of packets in sending unicast streams. Some video encoding techniques (e.g., JPEG) use unicast streams. A network switch that is processing four unicast streams for each of four users monitoring a single network camera will use four times the bandwidth consumption that a single camera in unicast mode will produce. A camera capable of a multicast mode (usually using MPEG-4 Part 2 Video Compression) requires the use of network switches and infrastructure that is capable of sending the video packets to a group of users, known as an IP multicast group, without further increase in bandwidth consumption.

Structured Cabling and Ethernet Protocol

Layer 2 and Layer 3 Switches and Routers

Bridges and switches operate at the OSI Layer 2 and forward traffic among LANs and LAN segments with high throughput. Layer 2 is the layer that contains the physical address of a client or server station. It is also called the Data Link layer or medium access control layer and contains the address that is inspected by a bridge, switch, or computer network interface card. The Layer 2 address of every network device is unique, fixed in hardware by its manufacturer, much like a ZIP code or postal address.

Routers operate at OSI Layer 3 and provide multiple protocol support and WAN access. Layer 3 devices contain the logical address of a client or server station, which is also known as the network layer. Layer 3 contains the address that is inspected by a router that forwards the traffic through the network. The Layer 3 address of a network device is a software setting established by the user that can change dynamically and periodically. One protocol often used with Layer 3 switches in video over IP applications is IGMP.

 © 2012 BICSI®

Imaging and Compression Features

Progressive Scan Imaging

Progressive scan imaging provides a sequential, top-down scan of the video image for a smoother rendering. An interlaced image of a moving object often appears blurred and may include horizontal artifacts. This is due to the process of joining or interlacing the odd and even lines to form a single frame.

Megapixel Imaging

Imagers used by surveillance cameras often use about 330,000 pixels when compared with imagers having over 1 megapixel (e.g., 1.3 megapixel imager or 1,300,000 pixels). The 1.3 megapixel imager is able to produce a full scan image of 1280 x 960, or four times the 640 x 480 (VGA) image. Megapixel imaging offers a larger image that better retains detail after enlargement of a particular area.

Back Focus—Automatic

The automatic back focus function moves the camera imager back and forth to achieve optimal focus in the event of the imager's automatic or manual conversion from color to black and white and vice versa.



Chapter 6
Intrusion Detection Systems

Chapter 6 explores the basics of design and provides examples of the application of various types of sensors to provide intrusion detection.

Table of Contents

Intrusion Detection Systems (IDS) 6-1
Introduction 6-1
Principles of Operation 6-2
Overview 6-2
Detection Sensors 6-3
Notification 6-4
Communication Methods 6-5
Telephony 6-5
Internet Protocol (IP) Technology 6-5
Wireless Communications 6-6
Cellular Telephony 6-6
Electronic Security Components 6-7
Control Panel 6-7
Keypads and Annunciators 6-9
Initiating Devices 6-10
Motion Detection Devices 6-11
Window Detection Devices 6-12
Glass Break Detectors 6-12
Shock Sensors 6-13
Magnetic Switches 6-14
Security Screens 6-14
Door Status Monitoring Devices 6-15
High-Security, Balanced Magnetic Switch 6-17
Perimeter Detection Devices 6-17
Outdoor Motion Detectors 6-17
Photoelectric Beam Detectors 6-18
Passive Magnetic Field Sensor 6-19
Electric Field Sensor 6-19
Microphonic Sensor 6-19
Optical Fiber Cable Sensor 6-19
Radar Sensors 6-20
Specialty Detection Devices 6-20
Notification Devices 6-21

Audible Devices 6-22
Sirens 6-22
Speakers 6-23
Piezo (Buzzer) 6-23
Visual Devices 6-23
Wireless Devices 6-24
Optional Integrated Equipment 6-24

Intrusion System Cabling 6-25

End-of-Line Supervision 6-26

 © 2012 BICSI®

Figures

Figure 6.1 Logical intrusion detection systems diagram 6-2
Figure 6.2 Liquid crystal display keypad 6-10
Figure 6.3 Passive infrared detector 6-11
Figure 6.4 Two styles of acoustic glass break detectors 6-12
Figure 6.5 Window shock sensor 6-13
Figure 6.6 Surface-mounted magnetic switches 6-14
Figure 6.7 Examples of recessed magnetic switches 6-15
Figure 6.8 Roller ball switch 6-15
Figure 6.9 Plunger switch 6-16
Figure 6.10 Floor-mounted overhead door switch 6-16
Figure 6.11 Single beam photoelectric detector 6-18
Figure 6.12 Long-range dual beam photoelectric detector 6-18
Figure 6.13 Radar sensor controlling a pan, tilt, and zoom camera 6-20
Figure 6.14 Indoor speaker or siren 6-21
Figure 6.15 Outdoor speaker or siren 6-21
Figure 6.16 Types of line supervision 6-26
Figure 6.17 States of a magnetic switch 6-27
Figure 6.18 Resistor color code chart 6-28

Tables

Table 6.1 Detection sensor technology and application 6-3

Intrusion Detection Systems (IDS)

Introduction

Intrusion detection systems (IDS) come in many forms and with various features. Typically, the IDS panel will monitor door contacts 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).

When designing a security system, consider additional benefits to enhance the system. IDS panels should be monitored from a central monitoring station to provide the best security for a home or business. The IDS panel can be tied into an alerting system that not only annunciates audibly and visibly locally but also alerts police and private security personnel. These systems also can alert users via telephone, cell phone, e-mail, tablet, or pager.

The expanded capabilities of alarm notification can ensure that homeowners, business owners, and managers will be notified in the event of an emergency. The system can be integrated to achieve maximum effectiveness for the client's needs. The role of the electronic safety and security (ESS) designer is to coordinate and balance the needs with technical capabilities and the security plan.

IDS can be used to identify a security breach of unauthorized entry for the exterior building perimeter, interior building security boundaries, and exterior site perimeter by a local alarm monitoring station or remote monitoring station.

Electronic intrusion detection is designed to allow a timely response or deterrent to security breaches that may adversely affect people and property.

Video surveillance systems can be integrated into IDS and may serve as motion and intrusion detection devices, using video images to record and monitor the activity for prompt response and forensic analysis.

NOTE: Refer to Chapter 5: Video Surveillance Systems for additional information.

Principles of Operation

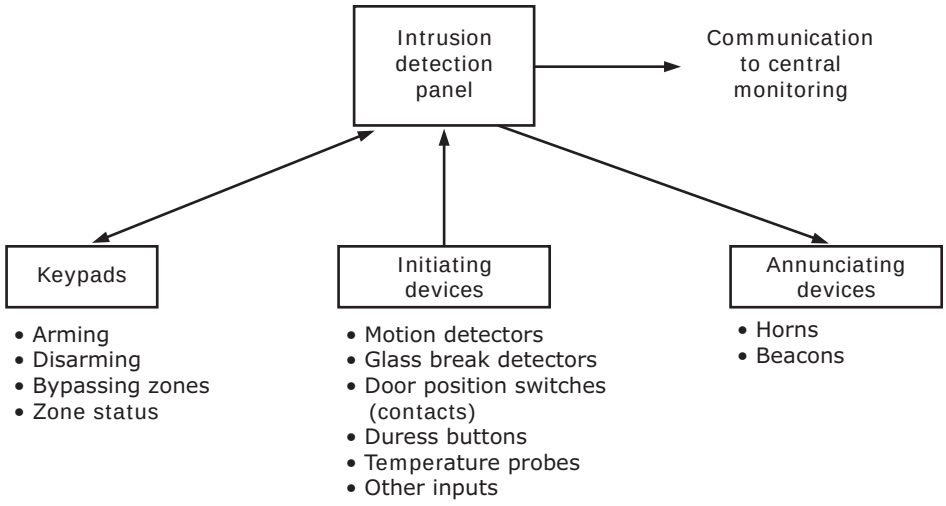
Overview

IDS generally detect 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 (see Figure 6.1).

IDS are an integration of the following components and devices:

- Detection sensors—Devices that monitor and detect forced and unauthorized entry into a protected area.
- 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.
- Notification console—Devices that monitor events and system alerts that operators can use to make informed decisions as to the operational status of the entire system.
- Power source—Low-voltage transformer and backup batteries.

Figure 6.1
Logical intrusion detection systems diagram



 © 2012 BICSI®

Detection Sensors

Detection sensors operate on the principle of sensing or detecting changes that occur to the operational conditions specified at the area under protection (see Table 6.1).

Detection sensors experience either a change or variation in:

- Voltage.
- Current.
- Resistance.
- Frequency.

This change or variation causes an on or off condition in digital signals or a regulated variation in analog signals that is then integrated into the processor controller to be analyzed and processed.

The detection sensors can be capable of initiating an alarm under any of the following conditions:

- Breaking an electrical circuit
- Interrupting a light beam
- Detecting a sound
- Detecting a vibration
- Detecting a change in capacitance because of the disturbance of an electrostatic field
- Tampering with the sensors or processing controller

IDS sensors are used to monitor:

- Perimeter—Doors, windows, fence, and wall.
- Area of space—Office space, hallways, cabinets, and lobbies.
- Point of object—Safes, paintings, and expensive artifacts.

Table 6.1
Detection sensor technology and application

Technology	Basis of Activation	Application
Audio	Sound	Interior areas, vaults, and other low sound level areas
Electromechanical	Breaking electrical circuit	Interior and exterior areas
Infrared	Movement	Interior and any areas where the temperature remains fairly constant
Microwave	Movement	Interior and exterior areas
Photoelectric	Interrupting light beams	Interior and exterior areas with line of sight between transmitter and receiver
Sonic/ultrasonic	Movement	Interior areas

Notification

Notification devices can be locally or remotely monitored (e.g., security office) for system activation or status on a schedule or real-time basis. A combination of the following notification methods can be found in most IDS:

- Keypads—Provide information on sensor status and operational conditions of the overall system.
- Speaker—May have a speaker over which audible alarm signals or synthesized/prerecorded/live voice messages are conveyed regarding the operations and status of the system.
- Sirens—May be installed inside and outside the facility, which sound various types of audible signals, depending on the detection sensor that has been activated.
- Bells—May be an electromechanical or electronic sounder that can be loud, providing notification over a wide area.
- Strobe lights—Frequently are required under the authority having jurisdiction (AHJ) for commercial systems to provide visual notification when specific detection sensors are activated (e.g., smoke detectors in fire alarm systems).
- Video monitor—Used to show system status and display graphics.
- Relays—Can be activated under certain programmed conditions to activate other functions (e.g., lights, pumps, video recorders, video transmission, sensor status).
- Recording devices—Can be activated from a detection sensor to record activities occurring in the vicinity of the activated sensor.
- Power-line carrier (PLC)—Can be used to activate components (e.g., lights, appliances, sound) throughout the protected facility or in close proximity to the activated sensor.

IDS can and 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.

 © 2012 BICSI®

Communication Methods

Telephony

IDS can use telephony as a means of communicating with a central reporting station. When an event occurs, the control panel through line seizure will dial a preprogrammed number over a dedicated telephone line and wait for a handshake tone upon answer.

Once the handshake has been established, the panel will transmit a four- to six-digit identifier and then the appropriate code for the event. The event code is a series of tones based on a programmed modem format.

The most common modem formats are:

- Contact identification.
- Radionics.
- Security Industry Association.
- 4/2.
- 3/2.

Internet Protocol (IP) Technology

Intrusion device manufacturers have Internet protocol (IP) modules that can expand the controller's communications capabilities to include Ethernet. These modules are typically hardwired into a terminal port located directly on the controller. IP allows the controller to communicate to a central reporting receiver or a server that can be located anywhere on the IP network. This method provides:

- Expedited supervisory response.
- Real-time transmission of events to the central monitoring station.
- Greater control of transmission through firewalls and network monitoring software.
- Ability to have more than one reporting point (time of day flexibility).
- Ability to integrate IDS in other security systems, providing full event logging and control.

Wireless Communications

In addition to carrier-provided networks, wireless communications systems can be used for alarm transmission. Many wireless solutions are available, ranging from short-range systems intended to transmit a single alarm point a few hundred feet to long-range systems designed to operate over hundreds of miles. In applications requiring high reliability (e.g., ESS systems), it is preferable to operate technologies that require a license or permit from a regulatory agency as licensed operation will provide some regulatory protection from interference from other users. Wireless communications can be the primary or secondary form of communication.

Generally, most wireless communications products will provide an IP-based transmission channel. In turn, IP-based reporting technologies will adapt most easily to wireless transmission.

If the ESS designer believes the use of wireless notification links would be of value to a project but is not well acquainted with wireless transmission systems and issues, then the advice of qualified personnel, such as a BICSI-certified Wireless Designer, should be sought.

For further detailed discussion of the applicable technologies, refer to the *Wireless Design Reference Manual*.

Cellular Telephony

A special cellular dialer is hardwired to the controller and utilizes a serial protocol to establish communications with the controller. This technology does require a service contract with a local cellular service provider.

It is the ESS designer's responsibility to factor in the added monthly charge into the total yearly cost of ownership.

 © 2012 BICSI®

Electronic Security Components

Control Panel

The control panel is the central processing unit (CPU), or main controller, of IDS. IDS controllers are microprocessor based and can operate in a stand-alone mode or networked in an enterprise architecture.

The controllers are 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. Controllers can send a coded message for service that needs to be performed on its own system (e.g., low battery, loss of power, hardware tamper, microprocessor failure). The control panel's reaction to an input is based upon the programming it has received from the installer or manufacturer.

Most control panels consist of a circuit board with screw terminals for connecting the wiring from inputs, outputs, power, keypads, and other devices. Generally, control panels have connections for power supplies, batteries, annunciation devices, external system interfaces, communication buses, and system detection devices.

Some control panels allow the connection of addressable devices (e.g., devices with unique addresses and processors that have the capability of providing more information than contact position) to the system. The communication bus is for the connection of devices that provide some form of control, expansion, or function (e.g., keypads, annunciators, zone expanders, building automation, intercom, access control).

Each output of the control panel (e.g., alarm, power) has a maximum current output value. This value is determined by the manufacturer. Each active device uses a certain amount of current, which is indicated on the device or its accompanying literature. Each time an active device is added to an output, the current draw is increased. The total current draw for an output should never exceed its rated value.

The same is true for the entire control panel. Each control panel has a maximum total current output, which is the total amount of current draw from all of the outputs combined. If the ESS designer finds that either the maximum value of an output or the total panel will be exceeded, an external power supply should be added to the system to power the additional load. For more information on properly selecting the correct type and size for a particular system, refer to the manufacturer's literature.

The battery backup for IDS is generally located in the control panel as well. It is the ESS designer's responsibility to correctly size the battery for the necessary runtime of the panel without external power.

Control Panel, continued

Backup batteries are rated in ampere-hour (Ah). An example is 8 Ah, which means the battery can output 8 amps for one hour. For any decrease in current draw, the amount of time the battery will operate will increase.

For example, this 8 Ah battery will operate for two hours if there is only a 4 amp draw or 8 hours if there is a 1 amp draw. The total current draw for a system is determined by adding all the current usage values for all of the attached devices and control panel.

Sizing the correct size battery can be accomplished with a simple formula once the required run time and current values are known:

$$B = T \times I$$

Where:

B = Battery size

T = Required battery run time

I = Current draw

For example, a system has a total draw of 800 milliamperes (mA) and needs to operate on standby power for 12 hours.

To determine the battery size required, use the following formula:

$$B = T \times I$$

$$T = 12 \text{ hours}$$

$$I = 800 \text{ mA } (.8 \text{ amp})$$

$$B = T \times I$$

$$B = 12 \text{ hours} \times .8 \text{ amp}$$

$$B = 9.6 \text{ Ah}$$

If a standard battery size for the total value calculated is not available, always size up. In this case, a 12 Ah battery would be installed.

In some cases, it may be necessary to have a required battery runtime while the panel is in alarm. More current can be used when a system is in alarm because of high-energy devices (e.g., siren, strobes). In this case, additional calculations will need to be performed.

 © 2012 BICSI®

Control Panel, continued

Control panels have a maximum size battery that can be charged and maintained. If the calculated battery is larger than the maximum battery rating of the control panel, an external power supply/battery charger will be required. For more information on selecting the correct external supply, refer to the manufacturer's literature.

Additionally, the ESS designer should consider backing up the panel's alternating current (ac) power input with an uninterruptible power supply (UPS).

In large facilities, IDS may be integrated into one unit with access control or life safety systems. In this type of system, IDS controllers are all integrated into a single platform: administered, commanded, and controlled from a local or remote computer server.

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.

Keypads and Annunciators

Keypads and annunciators provide a means for the users and installers to input commands to the control panel (e.g., user codes, silencing alarms, system programming). They also provide information to users and installers (e.g., violated devices or zones, trouble signals, programming feedback).

Keypads and annunciators come in three different styles—hard button, numeric keypad, and touch screen:

- Button functions are preprogrammed at the factory on hard button styles and cannot be changed by the installer. Examples include reset, silence, and test.
- Numeric keypads have a full numeric keypad (0–9) with # and * keys and may include predefined or programmable hard keys. The # and * keys may have special functions such as enter or cancel. If alpha characters are required in programming, the hexadecimal characters A–F are available where 1 is equivalent to A; 2 is equivalent to B; and so on.

NOTE: Refer to the keypad or system installation manual for the proper procedure for entering alpha characters on a particular system.

- The touch screen style provides a more intuitive interface for both the user and installer. Programmable icons, or soft keys, are used for user input. The touch screen also provides a soft, numeric, or full keyboard.

There are several different methods in which information is provided to the user from the keypad or annunciator. All keypads use some type of bell, chime, or buzzer to provide an audible notification locally of a change in state.

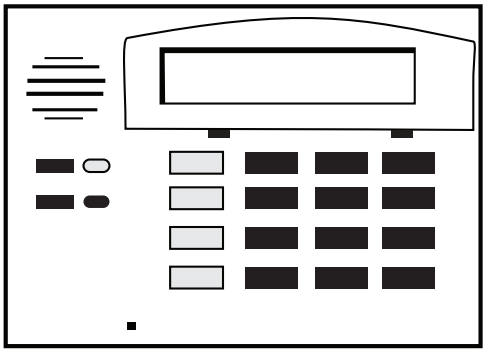
Visually, basic keypads use a light-emitting diode (LED) display that indicates the system status (e.g., armed, standby, bypass), trouble conditions, violated zones, and alarms. A legend is usually provided as a cross-reference for the LEDs. Mid-grade keypad units use a fixed message liquid crystal display (LCD) screen that provides the same information as the LED systems but in a different manner. Zone numbers are indicated by LCD numbers on the screen rather than LED indicators; a legend is still required to identify protected zones.

Keypads and Annunciators, continued

Most units have programmable LCD displays. These units allow the installer to program full words for zones and conditions either with a computer or by using the keypad. The user will see descriptive messages on the display, such as "reception area motion," instead of just a zone indication. Touch screens are similar to the programmable LCD display, but they can provide even more information and may use interactive icons instead of just text.

Keypads and annunciators should always be placed in an area that is readily accessible by the user (see Figure 6.2). The best location is usually by the primary entrance to a facility. Most systems will allow the installation of multiple units, so they may be placed at multiple entrances or where they can be monitored by security personnel.

Figure 6.2
Liquid crystal display keypad



Initiating Devices

Initiating devices are those used to send input signals to the panel such as a breach or a change in state of the device. Basic initiating devices use dry contacts to send signals to the control panel on two wires. These devices are either passive and do not require external power (2-wire) or active and require external power (4-wire). The contacts in these devices come in a range of configurations—normally open (NO), normally closed (NC), or form C (one NO and one NC connected to a common terminal on one side). The type that is used depends on the application and panel manufacturer.

Proprietary multiplexed addressable devices have unique addresses set by a small dial or dual in-line package (DIP) switches. The panel polls these devices at preset times (typically in milliseconds). If a device detects a problem, it sends this information to the panel along with its address. Addressable devices are passive but receive their power on the same pair of wires on which they send their signals, so two wires are generally all that is required.

 © 2012 BICSI®

Motion Detection Devices

Motion detection devices are used to detect motion in a room or area. Do not confuse motion detectors with photoelectric beam detectors that send out an invisible beam of light to a receiver or reflector. These are discussed later in this chapter.

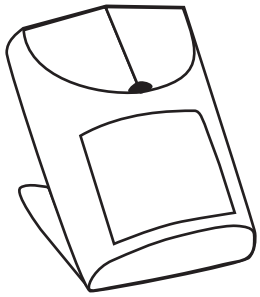
Motion detectors usually rely on three types of technology—passive infrared (PIR), ultrasonic, and microwave:

- PIR detectors have an optical sensor that is able to distinguish whether an infrared emitting object is present by first learning the ambient temperature of the monitored space and then detecting changes in the temperature caused by the presence of an object (see Figure 6.3).
- Ultrasonic sensors are active detectors that transmit ultrasonic sound waves that are inaudible to humans. The ultrasonic sensor's transmitter emits an ultrasonic signal into the protected area; the transmitted and received signals will be equal until an object enters the area that results in a change of frequency.
- Microwave devices emit microwaves from a transmitter that are detected by a corresponding and integrated receiver; an object entering and disrupting the microwave signal creates a reduction or reflection in the beam's intensity, thereby generating a change in the operational state of the sensor.

Combination detectors use two of the three technologies to try to prevent false alarms. Motion detectors have a fixed rated area that they will cover. It is important to refer to the manufacturer's instructions to determine the correct placement and the right device for the coverage area. Motion detectors are also active devices that require power.

Some motion detectors have a pet immunity rating, which helps to prevent false alarms caused by pets or animals. The motion detector is designed not to activate if any animal under the weight listed on the device passes in front of it. Motion detectors used outside usually have a pet alley. This is a set distance between the ground and the detection beam/area in which the motion detector will not detect.

Figure 6.3
Passive infrared detector



Motion detectors can be used alone for primary detection or as a secondary means for window and door protection. If motion detectors are used in areas that people may occupy while the system is armed, be certain that the motion detectors are on a zone that is programmable to be turned off when the building is occupied. Ensure that motion detectors are not pointed toward heat registers or items hanging from the ceiling to reduce false alarms.

Window Detection Devices

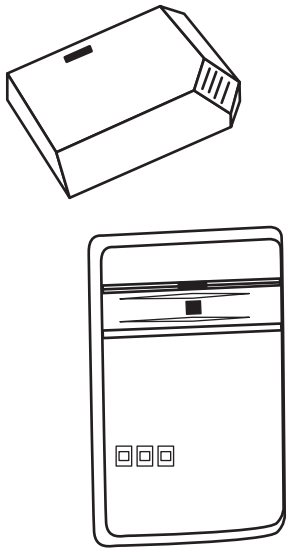
Window detection devices come in a variety of styles and use different methods to detect breaches. Some styles are acoustical and rely on sound to indicate a breach. These devices, also referred to as glass break detectors, can cover multiple windows within a manufacturer's defined area and detect the sound of breaking glass. Other styles mount directly to the window or the window frame and detect vibrations from the prying and forcing of a window or the breaking of glass.

Magnetic switches also can be mounted to window jams, whereas magnets are mounted to the actual window to signal a change in position of the window. Custom-made window security screens have alarm wires embedded in the screen and magnetic switches in their frames that signal a breech if the screen is cut or removed.

Glass Break Detectors

Glass break sensors may be used for internal perimeter building protection by detecting the unique frequencies produced from the breaking of glass to generate an alarm condition (see Figure 6.4). Glass break acoustic sensors are mounted in close proximity to glass panes and listen for sound frequencies associated with the breaking of glass.

Figure 6.4
Two styles of acoustic glass break detectors



Glass break detectors are an economical solution because one device can cover multiple windows, which reduces installation costs and time. The units can be mounted on a wall or ceiling with the internal microphone pointing toward the windows being protected.

 © 2012 BICSI®

Window Detection Devices, continued

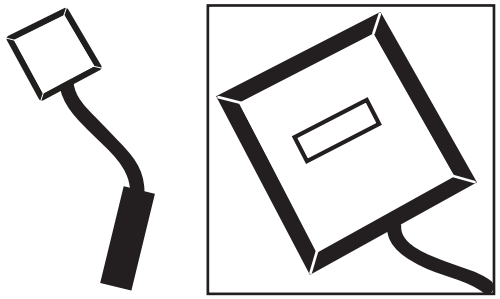
The major disadvantages to glass break detectors are they provide no protection to windows that are already open and will not detect the prying of windows. Glass break detectors are active devices and usually have a sensitivity adjustment to help in preventing false alarms.

When designing a glass break detection system, be certain that no window is outside the listed coverage area of the specified unit. A 7.5 meter (m [25 foot (ft)]) to 9 m (30 ft) radius is common, but some units only detect a radius no larger than 3 m (10 ft).

Shock Sensors

Shock sensors mount directly to the protected window or window jam and detect the vibrations of windows being opened or broken (see Figure 6.5). Many are stand-alone 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. Sensitivity usually can be adjusted on either type.

Figure 6.5
Window shock sensor



An improperly adjusted shock sensor can be easily activated by strong winds and rattling windows. Shock sensors have the advantage of detecting both glass breakage and the opening of a window. Shock sensors offer no protection if a window is already open unless the intruder is clumsy or creates a lot of vibrations.

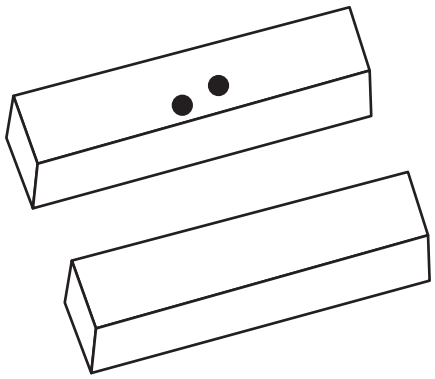
Shock sensors have higher installation costs since one unit is usually required for each protected window. It is sometimes acceptable to protect two windows with one device if the windows are side by side. Consult the manufacturer's installation instructions for further information.

Window Detection Devices, continued

Magnetic Switches

Magnetic switches can be mounted to window jams and their associated magnet mounted to the actual window (see Figure 6.6). If the window changes position, the magnetic switch changes state and sends an alarm signal to the control panel. Magnetic switches can be surface mounted or recessed into the frame and window.

Figure 6.6
Surface-mounted magnetic switches



Multiple switches can be used with one magnet so that the window can be protected whether closed or partially open. For example, a magnetic switch can be mounted in the window jam so that it aligns with the magnet in the window when the window is closed. A second switch can be installed in the jam so that it aligns with the magnet when the window is partially open. Both switches will be wired in series and be associated with the same zone. This gives the end user the option to keep some of the windows open and still feel protected.

Magnetic switches have a high installation cost because each window requires at least one switch. Magnetic switches provide no protection against breaking the glass.

Security Screens

Security screens replace the screens that come with some windows. They include a wire that is interwoven with the screen material. The wire is also installed in a series of magnetic switches that detect if the screen is in place. Each end of the wire is connected to loop wire coming from the panel. If the screen is cut or removed, it initiates an alarm.

Screens provide the greatest amount of protection, but they are the most expensive to install because each screen is custom made and each window requires one to be effective. Many commercial windows do not have provisions for window screens, so they cannot be used.

 © 2012 BICSI®

Door Status Monitoring Devices

Door status monitoring devices, commonly referred to as door switches, door contacts, or door position switches, are used to tell the control panel whether the door is open or closed. They do not have the ability to tell the control panel if the door is secure.

Hardwired door status monitoring devices 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 device.

Magnetic switches come in surface mount, recessed mount, and other models for specific doors (e.g., overhead or roll-up garage doors). See Figures 6.7–6.10 for examples. Magnetic switches consist of a magnet that is mounted in or on the door and a switch that is mounted in or on the door jam. Plunger and roller ball switches are recessed into the door jam, and the door physically changes the state of the switch as it is opened or closed. All models of switches come in different colors to match the finish of the door.

Figure 6.7
Examples of recessed magnetic switches

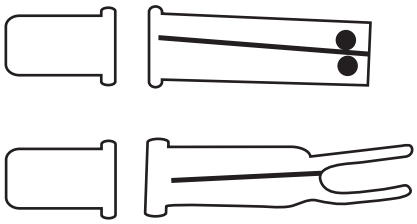
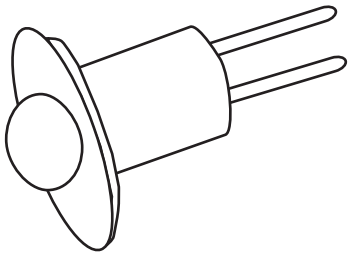


Figure 6.8
Roller ball switch



Door Status Monitoring Devices, continued

Figure 6.9
Plunger switch

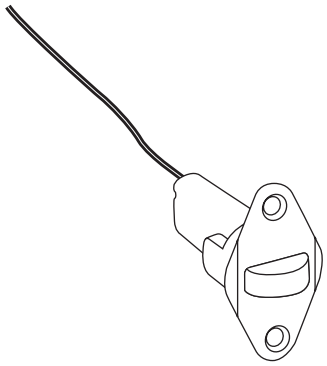
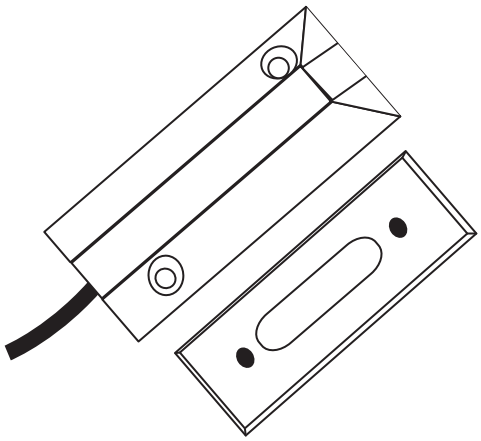


Figure 6.10
Floor-mounted overhead door switch



 © 2012 BICSI®

High-Security, Balanced Magnetic Switch

Defeating a recessed mounted magnetic door contact is possible. For high-risk areas, high-security biased door contacts often are used. The high-security contact uses a biasing magnet, mounted inside the reed switch part of the package. This biasing magnet pushes the contact's reed switch to the door open or alarm position when the external magnet is not present and trying to pull the reed switch the other way.

The contact's actuator magnet, which usually is installed in the door, has the perfect balance of magnetism and opposing polarity as the biasing magnet. When the actuator magnet is installed at the recommended distance from the switch, it balances out with the biasing magnet. The position of the switch's contact remains in the door closed position.

If an unfamiliar or secondary magnet is positioned near the switch, the opposing and balanced magnetism between the bias magnet and the actuator magnet may be disturbed. The reed switch changes to the door open state. This would then send an alarm to the systems connected to it.

To increase security, a triple-biased door contact may be used. This device has three reed switches with three biasing magnets in one half of the package. The other half of the door contact includes three balanced actuator magnets. Defeating this device is considered difficult.

Perimeter Detection Devices

Perimeter detection devices provide intrusion detection notification for the outer edge of an area or property (e.g., property line, fence line). These devices are intended to provide notification when unauthorized entry is gained onto the property.

Care should be used when designing perimeter detection because these devices can be susceptible to false alarms (e.g., animals, weather). Perimeter detection devices include outdoor motion detectors, photoelectric beam detectors, fence detectors, seismic detectors, and radar detectors.

Outdoor Motion Detectors

Outdoor motion detectors use the same PIR or microwave technologies as their indoor counterparts, but they are in an environmentally rated enclosure to protect the electronics from the elements. They also offer a selectable range of sensitivity so that they can be adjusted to prevent false alarms.

Outdoor motion detectors generally are mounted on the exterior of a building and have a detection range of 9 to 15.2 m (30 to 50 ft). These detectors are economical to install because they only require wiring to be installed in the building, so no trenching is usually required. Outdoor motion detectors are susceptible to false alarms because of animals or weather if they are not adjusted properly.

Perimeter Detection Devices, continued

Photoelectric Beam Detectors

Photoelectric beam detectors project an invisible beam of light between two points. When the beam of light is interrupted, an alarm is generated. These detectors can use single or multiple beams of light (see Figures 6.11 and 6.12).

Figure 6.11
Single beam photoelectric detector

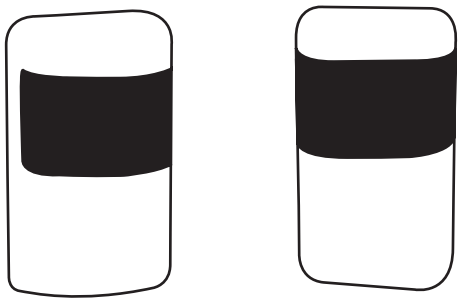
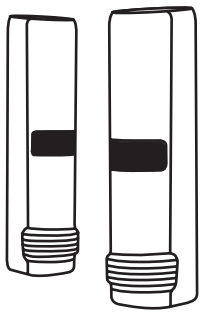


Figure 6.12
Long-range dual beam photoelectric detector



Photoelectric beam detectors utilize a transmitter that generates the beam of light and a receiver that receives the beam of a light. The receiver converts the received light energy into electrical energy and measures the amount of voltage generated in this conversion process. When the voltage amount drops below a specified level because of beam obstructions, an alarm is generated.

Both the transmitter and receiver require external power, so wiring will need to be installed to both units if they are separate. The alarm wires are connected at the receiver. Some short-range units have the transmitter and receiver built into the same unit. The transmitter projects the beam of light at a reflector, which reflects the light back to the receiver. In this type of design, power and alarm wiring would only need to be installed to the location of the transmitter receiver.

Photoelectric beam detectors require line of sight (LoS) between the transmitter and receiver with no obstructions that could interfere with the path of the beam. Depending on the type of detector and its sensitivity, a branch from a tree or bush could generate an alarm.

 © 2012 BICSI®

Perimeter Detection Devices, continued

Beam detectors are initially aligned manually by the installer and then fine-tuned with a multimeter to measure voltage. Some long-range devices have a sighting hole for the installer to look through for the initial alignment. It is imperative that both the transmitters and receivers be mounted on a solid surface that cannot move.

Beam detectors can be used along fence lines and at openings in fences or gates to detect human traffic, across driveways or roads to detect vehicle traffic, or in large buildings in place of conventional motion detectors as a cost-saving measure.

Some systems will allow one transmitter to serve multiple receivers. This can reduce the system installation time and cost as well as the power requirements.

Single beam detectors are generally designed for detecting a short distance along a perimeter. The transmitter projects one beam of light at the receiver. Interruption of this beam will generate an alarm.

Multibeam detectors project two or more beams at the same receiver. Each beam must be interrupted for an alarm to be generated. Multibeam detectors can help prevent false alarms that are due to animals or branches and are used in long-distance applications up to 305 m (1000 ft).

Passive Magnetic Field Sensor

This technology uses an electromagnetic field generator powering two wires running in parallel. The wires are connected to a signal processer that analyzes any change in the magnetic field that has been generated, such as that produced by a vehicle entering the field.

Electric Field Sensor

This sensor technology can be installed on walls, fences, or poles in a stand-alone mode. The signal processor generates a fixed electromagnetic field and analyzes the amplitude and rate change as well as the length of any disturbances of the field.

Microphonic Sensor

This sensor technology is based on coaxial sensor cable installed on fence fabric and then calibrated to differentiate between signals from the cable or the fence being cut, someone climbing the fence, or wind hitting the fence fabric. The sensors are designed to detect and analyze incoming electronic signals received from the sensor cable and then generate an alarm condition from signals exceeding the design threshold or preset conditions.

Optical Fiber Cable Sensor

An optical fiber cable can be used to generate an alarm condition by measuring the difference in the amount of light sent through the optical fiber core. Using signal processors, a disturbance in the cable will reduce the amount of light transmitted, which then generates an alarm condition.

Perimeter Detection Devices, continued

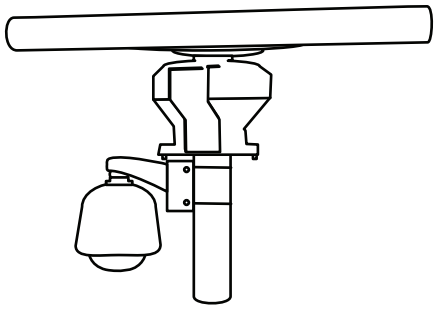
Radar Sensors

Radar sensors serve as wide area intrusion detection devices. They are adapted from an established technology conventionally used for tracking aircraft or vessels. The rotating antenna and microwave frequencies transmitted are similar to marine or aircraft radar equipment with the exception that the rotation rate of the antenna is often increased to provide the capability to track fast-moving objects at close range.

The familiar "green screen" with blips representing targets is overlaid on a geospatial map or other map of a facility. Detection zones and boundaries are drawn to alert the security console of a target entering a defined area of interest or exclude other areas. Objects detected also may alert the security console based on their speed and direction of travel. The size of the objects detected by the system is dependent on the frequency the antenna transmits. Detection of objects smaller than an average human is possible.

Because of their ability to geolocate a target, pan, tilt, and zoom (PTZ) cameras can be incorporated with a radar sensor and be automatically directed to track an object in real-time to provide visual verification of an intrusion event (see Figure 6.13). The limitations of this technology require that an LoS be established between the area of interest and the radar antenna.

Figure 6.13
Radar sensor controlling a pan, tilt, and zoom camera



Specialty Detection Devices

Specialty items are devices that either would not be used regularly on most IDS or provide detection from threats other than intrusion detection. These devices provide detection against environmental threats (e.g., high water, temperature) and life safety issues (e.g., gas leaks) or report medical emergencies (e.g., wireless alert pendants for the elderly or handicapped).

 © 2012 BICSI®

Notification Devices

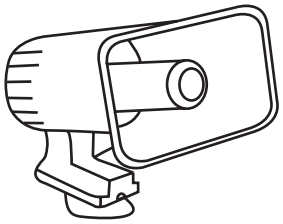
Notification devices are audible or visual indicator devices that are controlled by the alarm or auxiliary outputs on the control panel. These devices provide notification to building occupants that an alarm condition has occurred so that the necessary action can be taken (e.g., responding to or evacuating an area). A notification device also will let intruders know that unauthorized entry has been detected and can cause them to find some method of escape.

Notification devices can be installed inside or outside the protected premises (see Figures 6.14 and 6.15). Internal devices will alert the occupants and possibly the intruder. External devices are sometimes used to alert neighboring facilities of an alarm condition or to make it easier for responding authorities to identify the building with the active alarm.

Figure 6.14
Indoor speaker or siren



Figure 6.15
Outdoor speaker or siren



The ESS designer should discuss with the customer whether notification devices are wanted or needed by the customer. Some may prefer a silent alarm only. Local codes and ordinances should be checked to see if any restrictions are in place for audible or visible alarms. Many jurisdictions limit or prevent entirely the use of external audible alarms because of the nuisance they may cause neighbors.

Notification Devices, continued

Audible Devices

Audible devices can utilize voice notifications as well as whooping, whirring, beeping, or buzzing sounds, depending on the type of device. Some systems can be configured to produce different sounds based upon the type of alarm or location of the breach.

Sirens

Sirens are self-contained units that require external power to operate and produce the most commonly recognized whirring or whooping sounds.

When voltage is applied, a built-in siren driver will produce an amplified sound. The siren can have multiple inputs with each input producing a different audible notification. Sirens come in various styles, audible levels, and indoor/outdoor ratings. The ESS designer should identify the type of environment and ambient noise level at the location where the siren needs to be installed and pick the appropriate siren for the application.

For example, outdoor sirens are typically larger and louder than indoor sirens. Using this type of siren in an office environment not only may look out of place, but it may also cause hearing damage to those nearby. Sirens tend to use a fair amount of current, so they can easily overload the control panel. If additional devices are required and the limits of the panel are exceeded, external power supplies may be used.

NOTE: Refer to the system's installation documents to properly select and install any external power supply.

 © 2012 BICSI®

Notification Devices, continued

Speakers

Speakers are generally similar in design and style and can be easily confused with sirens. However, unlike sirens, the audible tone that speakers emit is generated externally rather than internally. Speakers will sound whatever signal is sent to them, which can be the same whooping and whirring of the siren, notification tones, or voice directions.

NOTE: Refer to the system's installation documents to ensure that the type and quantity of speaker specified will work with that particular system.

Piezo (Buzzer)

Piezos are small buzzers that sound a high-pitched noise. They are self-contained devices that require external voltage to internally produce sound.

Piezos are generally installed by the manufacturer in control panels, keypads, and annunciators to indicate off-normal conditions. They also can be installed at designated locations (e.g., security office) to provide advanced notification to authorized staff before a general alarm is sounded.

Visual Devices

Visual notification can be through the use of strobe, flashing light, or LED to indicate an alarm or trouble condition. Like piezos, LEDs are generally used on control panels, keypads, and annunciators to indicate off-normal conditions. They can also be used as visual indicators at other areas.

Strobe lights or flashing lights come in multiple colors and can be mounted indoors or outdoors. Control panels can send signals via the premises' power wiring to turn on or flash interior or exterior lighting to indicate an alarm.

Wireless Devices

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

IDS may utilize wireless technology to transmit:

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

Wireless IDS can be used in place of most wired devices, including:

- Surface mount door contacts.
- Recessed window contacts.
- Short-range PIR motion sensors.
- Glass break detectors.
- System keypads.
- System key fobs.

Optional Integrated Equipment

While IDS can operate as stand-alone systems, most will allow the incorporation of other systems into the control panel with built-in expansion modules. It is quite common for residential IDS to have fire detection incorporated into the system design.

Most commercial IDS will allow the addition of access control and video surveillance.

NOTE: For more information on fire detection, refer to Chapter 7: Fire Detection and Alarm Systems. For more information on access control systems, refer to Chapter 4: Access Control Systems.

 © 2012 BICSI®

Intrusion System Cabling

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

- Panel to keypad: 4-conductor stranded 18 American wire gauge (AWG) (nonshielded)
- Panel to addressable devices: 1-pair twisted 18 AWG (nonshielded)
- Panel to powered device: 1-pair 18 AWG
- Conventional device to addressable module: 1-pair 22 AWG

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

- Panel to keypad: 4-conductor nontwisted 18 AWG (nonshielded)
- Panel to device: 2-conductor 22 AWG (nonshielded)
- Communication bus: 4-conductor 18 AWG (nonshielded)
- Panel to powered device: 2-conductor 18 AWG

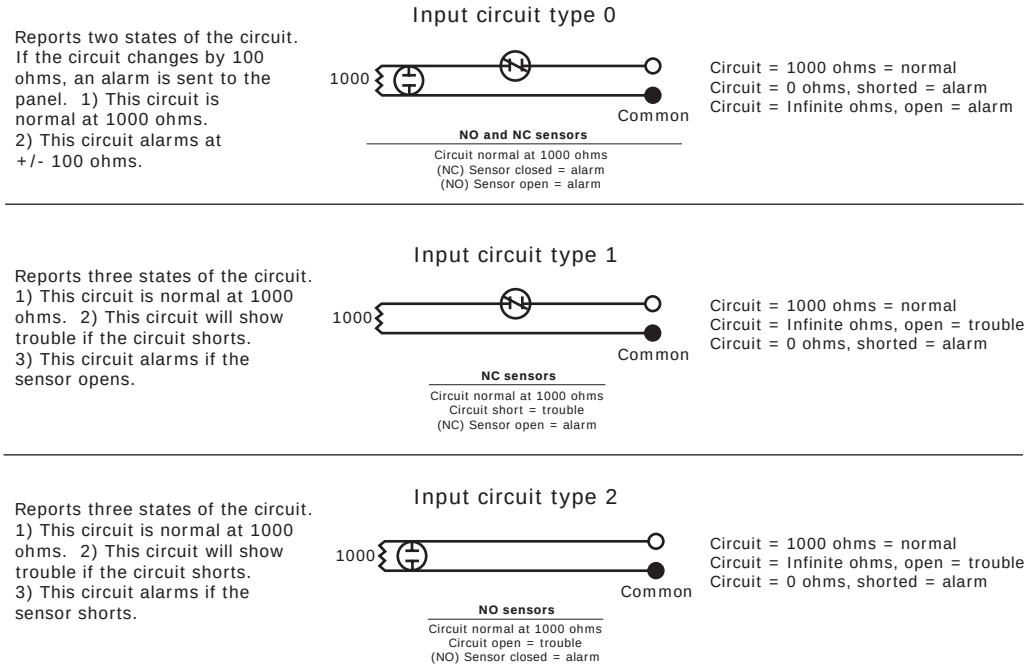
Refer to the details in Chapter 4 on Ohm's law and voltage drop to properly calculate and determine the acceptable cabling distance for each device.

End-of-Line Supervision

End-of-line (EOL) supervision is required for IDS devices to provide detection of failure or tampering of the device or the cabling to the device. The supervision of the circuit is accomplished by installing an EOL resistor (EOLR) at the device (see Figure 6.16).

NOTE: This resistor must be installed at the device and not at the panel.

Figure 6.16
Types of line supervision



NC = Normally closed
NO = Normally open

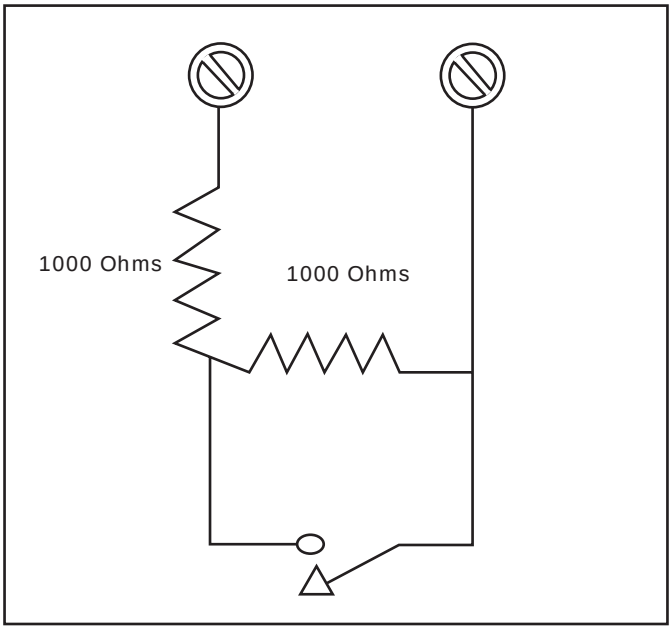
 © 2012 BICSI®

End-of-Line Supervision, continued

The voltage sensing terminal of the intrusion detection panel measures the voltage across the EOLR to ground. Figure 6.17 shows the use of 1000 ohm resistors to show four possible states of the magnetic switch. Magnetic switches can be used in NC series or in NO parallel circuits:

- With the circuit closed, the resistance reading will be 1000 ohms (e.g., door secure).
- With the circuit open, the resistance reading will be 500 ohms (e.g., door unsecure).
- With a cut circuit, the resistance will be open (e.g., wire cut).
- With a shorted circuit, the resistance will be at or near 0 ohm (e.g., bypassed or jumpered contact).

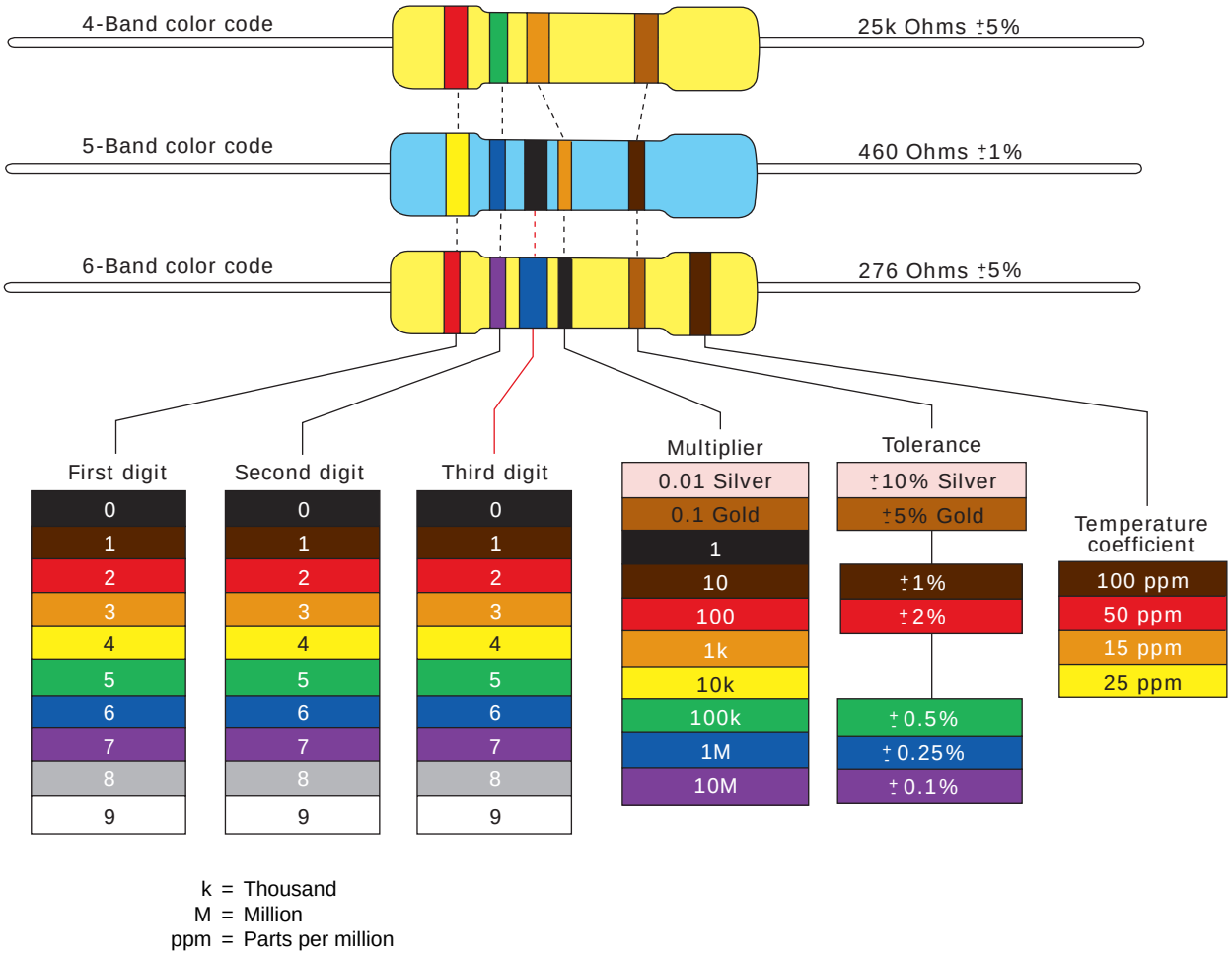
Figure 6.17
States of a magnetic switch



End-of-Line Supervision, continued

Figure 6.18 details the band color schemes on resistors that provide the resistance value/rating in ohms of the resistor. Similar schemes are also used on other electronic circuit elements such as capacitors and inductors.

Figure 6.18
Resistor color code chart



 © 2012 BICSI®

Chapter 7
Fire Detection and Alarm Systems

Chapter 7 provides an overview of the complex subject of fire detection and alarm systems, including classes of fire alarm and detection systems, components that initiate a fire alarm condition, detectors and systems currently available, fire suppression systems and their related initiation devices, and notification appliances.

Table of Contents

Fire Detection and Alarm Systems 7-1
Introduction 7-1
Classes of Fire Alarm Systems 7-3
Overview 7-3
Protected Premises System 7-3
Local Monitoring 7-3
Remote Monitoring 7-3
Supervising Station System 7-4
Central Station Service 7-5
Proprietary Supervising Station System 7-7
Remote Supervising Station System 7-7
Public Fire Alarm Reporting System 7-8
Requirements of a Public Fire Alarm Reporting System 7-8
Requirements of Alarm Transmission Equipment 7-8
Requirements of Publicly Accessible Fire Service Boxes 7-9
Initiation Devices 7-10
Overview 7-10
Detection 7-10
Smoke Detectors 7-11
Ionization Detectors 7-12
Advantages 7-12
Disadvantages 7-13
Typical Uses 7-13
Photoelectric Detectors 7-13
Advantages 7-15
Disadvantages 7-15
Typical Uses 7-15
Beam Detectors 7-16
Advantages 7-16
Disadvantages 7-16
Typical Uses 7-17
Duct Smoke Detectors 7-17

Air-Sampling (Aspirating) Fire Detection Systems. 7-18
Overview 7-18
Functionality of an Air-Sampling Fire Detection System 7-18
Applications 7-19
Sampling Pipe. 7-20
Heat Detectors 7-21
Fixed Temperature Spot Heat Detectors. 7-22
Advantages 7-23
Disadvantages 7-23
Rate-of-Rise Spot Heat Detectors 7-24
Combination Rate-of-Rise and Fixed Temperature Heat Detectors 7-25
Advantages 7-25
Disadvantages 7-25
Rate-Compensated Heat Detectors 7-26
Advantages 7-26
Disadvantages 7-26
Typical Uses 7-26
Flame Detectors 7-27
Advantages 7-27
Disadvantages 7-27
Typical Uses 7-27
Gas Detectors. 7-28
Advantages 7-28
Disadvantages 7-28
Typical Uses 7-28
Coverage for Smoke and Heat Detectors 7-29

Other Fire Detection System Devices 7-31
Pull Stations 7-31

Fire Suppression Systems and Supervision Devices. 7-32
Overview 7-32
Monitoring Devices 7-32
Water Flow Detectors 7-32
Vane. 7-32
Pressure 7-33
Valve Tamper Switches 7-33
Pressure Switches 7-34

 © 2012 BICSI®

Notification Appliances 7-35
Overview 7-35
Types of Notification Appliances 7-35
Bells 7-36
Chimes 7-37
Horns 7-38
Speakers 7-39
Strobes 7-41
Factors Affecting Performance 7-42
Audibility 7-42
Intelligibility 7-44
Visibility 7-44
Circuits and Pathways 7-50

Control Units 7-52
Overview 7-52
Central Control Panels 7-52
Zoned Systems 7-53
Addressable Systems 7-54
Supervision 7-55

Trouble Conditions 7-56
Overview 7-56
Supervisory Trouble Signal 7-56
Power Supplies 7-57
System Inputs and Outputs 7-57
Remote Monitoring and Control Modules 7-58
Remote Control (Annunciator) Panels 7-59
Graphical Displays 7-60
Signaling 7-60
Zones 7-60

Digital Alarm Communicator System (DACS) 7-61
Overview 7-61

Transmitters 7-62
Digital Alarm Communicator Transmitter (DACT) Dialers 7-62
Transmission Means 7-62
Transmission Channels 7-63
Long Distance 7-64
Call Forwarding 7-64
Protocol 7-64
Digital Alarm Radio Transmitter (DART) 7-65
Transmission Means 7-65
Testing 7-65
Receivers 7-66
Digital Alarm Communicator Receiver (DACR) 7-66
Reception Requirements 7-66
Testing 7-66
Digital Alarm Radio Receiver (DARR) 7-66
Internet Protocol (IP) Alarm Communicator System 7-67
Overview 7-67
Internet Protocol (IP) Alarm Communicator System Transmitter 7-67
Internet Protocol (IP) Alarm Communicator System Receiver 7-68
Internet Protocol (IP)-Based Solution 7-68

 © 2012 BICSI®

Figures

Figure 7.1 Larger central station retransmit chain 7-6
Figure 7.2 Typical ionization smoke detector 7-12
Figure 7.3 Photoelectric smoke detector using principle of light obscuration 7-14
Figure 7.4 Typical photoelectric smoke detector using principle of light scattering 7-14
Figure 7.5 Typical photoelectric beam-type detector 7-16
Figure 7.6 Typical duct smoke-type detector 7-17
Figure 7.7 Air-sampling system 7-21
Figure 7.8 Typical fixed temperature heat detector 7-22
Figure 7.9 Typical rate-of-rise heat detector 7-24
Figure 7.10 Principle of operation of typical combination rate-of-rise and fixed temperature heat detector 7-25
Figure 7.11 Typical infrared flame detector 7-27
Figure 7.12 Typical detector coverage areas 7-30
Figure 7.13 Typical fire alarm pull station 7-31
Figure 7.14 Typical water flow detector 7-32
Figure 7.15 Typical valve tamper switch 7-33
Figure 7.16 Typical pressure switch 7-34
Figure 7.17 Typical fire alarm bell 7-36
Figure 7.18 Typical fire alarm chime 7-37
Figure 7.19 Typical fire alarm chime with integrated strobe 7-37
Figure 7.20 Typical fire alarm horn 7-38
Figure 7.21 Typical fire alarm horn with integrated strobe 7-38
Figure 7.22 Typical fire alarm speaker 7-40
Figure 7.23 Typical fire alarm speaker with integrated strobe 7-40
Figure 7.24 Typical fire alarm strobe 7-41
Figure 7.25 Typical visible notification appliance coverage pattern 7-45
Figure 7.26 Visible notification appliance placement 7-46

Tables

Table 7.1 Temperature classification for heat-sensing fire detectors 7-23
Table 7.2 Typical ambient sound levels by location 7-43
Table 7.3 Room spacing for wall-mounted visible appliances 7-47
Table 7.4 Room spacing for ceiling-mounted visible appliances. 7-48

 © 2012 BICSI®

Fire Detection and Alarm Systems

Introduction

This chapter provides a brief overview of the complex subject of fire detection and alarm systems, including:

- Classes of fire alarm and detection systems, including the protected premises, local and remote types of fire alarm systems, and supervising station types of systems that are continuously monitored by a nationally recognized testing laboratory (NRTL) certified central fire alarm station.
- Components that initiate a fire alarm condition by the detection of smoke and heat with the various types of detectors and systems currently available.
- Various fire suppression systems and their related initiation devices that are supervisory in nature to ensure that the active suppression of a fire condition will occur. These supervisory devices monitor such items as the open and closed position of valves and the pressures and flow within a fire suppression system; the devices 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.
- Notification appliances that alert the occupants of a building to safely evacuate the area when a fire condition is detected.
- Fire alarm and detection control units and annunciators. These comprise the intelligence of the systems and perform various functions, including monitoring the system's reliability. Signals are used to alert facilities personnel that a component requires replacement or maintenance or that an alarm condition exists. These discussions include power requirements and the control unit's ability to communicate with the annunciator and with off-site facilities through various transmitters and receivers.

The information presented here should be considered as reference material for the design and implementation of such systems. Serious consequences can result from the inadequate or substandard design and installation of fire detection and alarm systems, including loss of life and property.

NOTE: For more information on legal liabilities, refer to Appendix B: Legal Aspects of Electronic Safety and Security Design.

Introduction, continued

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

Installers also are trained in the latest codes and standards and are certified under professional development programs (e.g., National Institute for Certification in Engineering Technologies [NICET]) as well as by the equipment manufacturers who conduct installation seminars. Continuing education related to changes in products, codes, and regulations is recommended to maintain proficiency in design and installation skills.

Electronic safety and security (ESS) designers should be familiar with the terms used in this chapter. ESS designers also need to be aware of the organizations that regulate, define, and govern the various codes and standards that must be followed by the fire alarm component manufacturers and the designers and installers of fire alarm and detection control units and annunciators. Another important aspect is the type of occupancy (occupancy classification) that is being designed.

ESS designers must understand their relationship with the authority having jurisdiction (AHJ) and the importance of this individual in coordination with the design and installation of the various fire alarm and detection control units and annunciators. Without the involvement of and final approval by the AHJ, a building cannot be occupied or insured.

The final aspect of fire prevention relies on the containment portion of a fire protection scenario. A firestopping method that seals fire and smoke barrier penetrations and prevents the passage of fire or smoke from one containment area to another is part of the ESS designer's and installer's responsibilities.

NOTE: Refer to the latest edition of BICSI's *Telecommunications Distribution Methods Manual* for firestopping requirements.

 © 2012 BICSI®

Classes of Fire Alarm Systems

Overview

This section will discuss two classes of fire alarm and detection systems:

- The first and most common class is a protected premises system. This system is a closed protected system in that 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. This type of system can be locally or remotely monitored by the client or maintenance personnel, but it is not a supervised station class of system.
- The second class of system is a supervising station system. This type of system embellishes a protected premises system. The difference is that the protected premises system is continuously monitored by a central monitoring company for any abnormal events. These personnel are responsible for dispatching, reporting, or similar functions resulting from events generated by the protected premises system.

Protected Premises System

Local Monitoring

Fire alarm systems are categorized by their detection and alarm transmission abilities. A local fire alarm does what its name implies. When activated, it announces an alarm to the occupants in the area it protects.

Alarm-initiating devices (e.g., smoke detectors, heat detectors, manual pull stations) are installed throughout the protected premises to monitor the area and signal the control panel upon activation. A local audible (e.g., bell, horn, speaker tone) or visual (e.g., high-intensity strobe light) alarm is then activated to notify the occupants. The occupants or building's facility personnel will then notify the local fire department or public safety agency.

Local fire alarms may have the capability to transmit a presignal alarm to occupants before sending a general alarm. The presignal feature is a component of alarm systems that protect environments such as correctional facilities, hospitals, and nursing homes. It enables those responsible for special occupants to check the area and determine whether additional alarms, evacuation, or fire department response is warranted. Presignal alarms also should be automatically transmitted to a central fire alarm system after a specified time period.

Remote Monitoring

Ethernet Compatible Fire Alarm System

An Ethernet compatible fire alarm system can be established as part of a new installation or as a card-based upgrade to certain alarm control panels installed in an existing facility. The card-based configuration offers significant cost savings over a dedicated workstation and introduces significant system flexibility for collecting and managing information.

Protected Premises System, continued

Each panel interface card within the fire and safety network is assigned a unique Internet protocol (IP) address that allows view and communication with individual elements of the system rather than simply providing zone-by-zone status.

The fire and safety network then interfaces with a corporate data network in the same manner any other computer appliance would be added. This means software upgrades can be accomplished as the system is expanded or enhanced. This system must be listed by an NRTL.

Network-Based Monitoring

Network-based monitoring defines each component as a node. The nodes can be:

- A fire alarm panel.
- A transponder.
- Another network-level communication device.

All devices on this network communicate via peer-to-peer network communications.

Digital Alarm Communicator Transmitter (DACT)

Digital alarm communicator transmitters (DACTs) are used for fire alarm control panels (FACPs) that are not network compatible or that may be too remote for a network connection. These devices typically communicate through a serial port and require vendor-specific software. FACPs equipped with a DACT can communicate their local event status or individual point status to the digital alarm communicator receiver (DACR) using a dial-up telephone connection.

NOTE: See the control units section in this chapter for further information.

Additional remote monitoring systems for central and remote stations are addressed in the next section on supervising station systems.

Supervising Station System

The concept of supervising station systems first appeared in the 1960s in the National Fire Protection Association (*NFPA*) *72®, National Fire Alarm and Signaling Code®*.

Supervising station systems will continue to evolve as new technologies emerge to address the needs of property owners (and the companies that insure the property owners) to provide the best protection possible of life and property. The role of the ESS designer is to blend the needs of the client with the requirements of codes and standards to provide a design that the AHJ will approve.

Supervising station systems differ from protected premises systems by reporting the signals provided to the supervising station system from the protected premises system for retransmission to the designated fire protection authorities.

 © 2012 BICSI®

Supervising Station System, continued

Central Station Service

Central station monitoring companies do not own the properties they monitor, and such services are typically fee based. They generally monitor fire detection systems for many separate property owners.

The fire alarm is typically transmitted over telephone lines to the central station monitoring company, which then calls the local fire department for mitigation.

Requirements for Central Station Service

Central station service is a system or group of systems in which the operations of circuits and devices at a protected property are signaled to, recorded in, and supervised from a listed central station. This central station has competent and experienced operators who, upon receipt of a signal, take action as required by *NFPA 72*.

Central station service has six elements to meet the certification requirement:

- Installation of fire alarm transmitters
- Alarm, guard, supervisory, and trouble signal monitoring
- Retransmission of received signals
- Recordkeeping
- Testing and maintenance
- Runner service

The listed central station may provide all six elements to the contracted subscriber. It may provide only the services available at the listed central station location and subcontract the protected premises portion to a listed local fire alarm service provider.

An example of this arrangement would be a local technician who may be subcontracted by the central station service to install a transmitter and test and maintain an automatic fire protection (sprinkler) system at the protected premises.

The central station would be responsible for the signal monitoring, retransmission, and runner service. Both parties would share the recordkeeping obligations. The contractor would provide the record of completion and maintain the testing reports, and the central station would track and record all signals received from the transmitter.

Installation

The central station must provide or subcontract the installation of the transmitter to fully comply with the requirements of listing. An installation of a fire alarm system with a built-in transmitter or dialer by a nonlisted local fire alarm installation company does not meet the requirements of a listed central station system. It does, however, meet the requirements of a remote supervising station system as discussed later in this chapter.

Supervising Station System, continued

Alarm, Guard, Supervisory, and Trouble Signal Monitoring

The central station is required to monitor the protected premises fire alarm signals and retransmit them to the public fire communications center immediately upon receipt. In contrast, guard, supervisory, and trouble signals can be retransmitted to designated personnel specified in the subscriber contract. Records of all signals transmitted to the central station must be automatically logged.

Testing and Maintenance

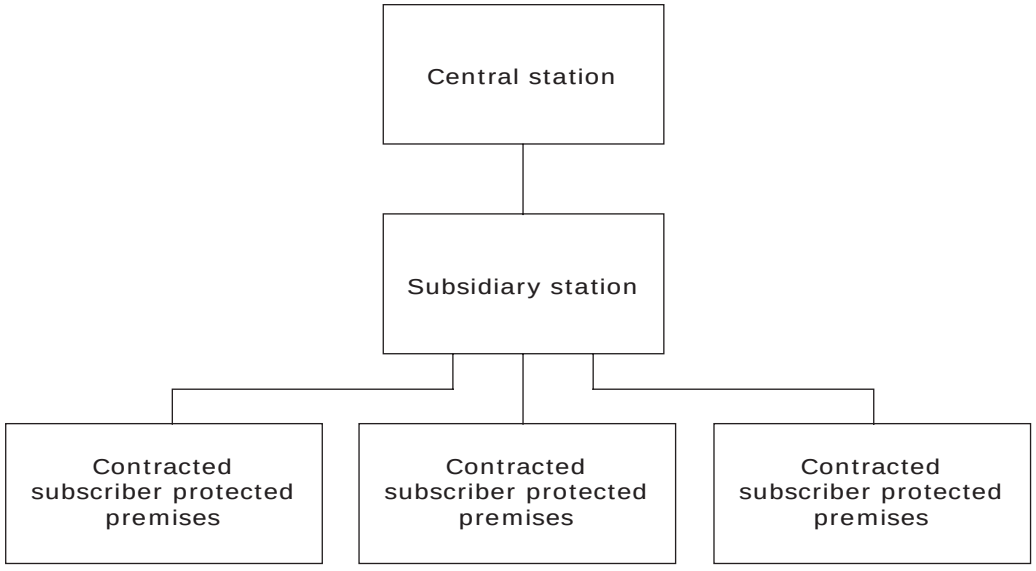
Testing and maintenance requirements are addressed in *NFPA 72*. For central station service systems, a pass code must be provided to place the system into test mode.

Runner Service

The central station service must provide a runner service within two hours to respond to the protected premises in the event of an alarm or supervisory condition where equipment may need to be reset. Trouble signals must be addressed by a runner within four hours.

Central stations also may retransmit to a larger central station in a daisy-chain configuration as long as all stations in the chain adhere to UL 827, *Standard for Central-Station Alarm Services* (see Figure 7.1).

Figure 7.1
Larger central station retransmit chain



 © 2012 BICSI®

Supervising Station System, continued

Proprietary Supervising Station System

A proprietary supervising station system is required to meet nearly all of the elements of a central station service system. The major difference is that it is typically owned and operated by the protected premises owner. The staffing requirements are two operators, one of which may be the runner. When the runner is not in attendance at the station, contact with the station operator must be maintained every 15 minutes.

The building or room housing the station must be:

- Fire resistive.
- Detached or cut off.
- Equipped with a 26-hour emergency lighting system.

Access to the building or room must be restricted. If the proprietary supervising station houses the protected premises fire alarm system master control unit, the installation of a transmitter is not required.

Examples of this type of service are:

- College campuses.
- Multibuilding hotels and motels.
- Casinos.
- Industrial complexes.

Remote Supervising Station System

Central station monitoring service is not available in all areas, in which case remote station fire alarm monitoring may be used. This system uses the local fire department or public safety facility as its central station. When fire alarm calls are received directly from various occupancies, fire service personnel are self-dispatched to answer the calls.

Remote supervising station systems give protected premises owners and management an alternative to the strict level of service of a central station system or proprietary supervising station system.

The addition of a remote supervising station to the code permits the protected premises fire alarm system to report alarms to a supervising station where a minimum of two people are on duty at all times. One major difference is those two people may have duties other than the supervision and operation of the supervising station when allowed by the AHJ. Runner service is eliminated for this type of supervising station, and the requirement for automated recordkeeping is reduced to manually written or typed logs.

Public Fire Alarm Reporting System

NOTE: The following section contains information about public fire alarm reporting systems only. Chapter 27 of the *NFPA 72* 2010 edition details requirements of these systems but uses the terminology "public emergency alarm reporting system" since it applies to all types of public emergency alarm reporting systems, not just those used exclusively for fire alarm reporting.

Requirements of a Public Fire Alarm Reporting System

A public fire alarm reporting system is a type of remote station. In this instance, various geographical areas, instead of particular occupancies, are monitored. A public fire alarm reporting system allows the general public to initiate a fire alarm from openly accessible manual pull types of fire alarm boxes at street level. These boxes transmit emergency alarm signals directly to the fire department.

Public fire alarm reporting systems may also be called municipal fire alarm systems. These systems often are seen in rural communities that have unique facilities (e.g., college campus, hospital) to provide faster fire department response to alarm conditions.

The two types of public fire alarm reporting systems are Type A and Type B:

- The Type A public fire alarm reporting system is a system where an alarm from a fire alarm box is received then retransmitted to fire stations either manually or automatically. The signals from a fire alarm box are received at the public fire service communications center then selectively retransmitted to the proper fire station(s). If the number of alarms needing retransmission exceeds 2500 per year, a Type B system is required.
- The Type B public fire alarm reporting system is a system where an alarm from a fire alarm box is transmitted automatically to all municipal fire stations and, if used, a supplementary alerting device (e.g., siren).

Requirements of Alarm Transmission Equipment

Public fire alarm transmission equipment, including master boxes, auxiliary boxes, and street boxes, must meet the following operational and design requirements:

- Concurrent operation of at least four boxes must not result in the loss of alarm.
- Boxes, when in an abnormal condition, must leave the circuit usable.
- Boxes must be designed so that recycling does not occur if the actuating handle is held in the actuated position.
- Boxes must give visible or audible indication that the device has been actuated.
- Box cases and parts accessible to the public must be made of insulating materials or effectively grounded per *NFPA 70®, National Electrical Code®*.

These requirements must be met for all types of public fire alarm reporting boxes being installed.

 © 2012 BICSI®

Requirements of Publicly Accessible Fire Service Boxes

The concept of a public fire alarm reporting system is to make alarm initiation available to the public. With that in mind, *NFPA 72* has included the following requirements to make the initiating device accessible and safe to operate for the public:

- Boxes shall be located where conspicuous and accessible.
- Box housings shall protect internal components from the weather.
- Doors on boxes shall remain operable in adverse weather conditions.
- Boxes shall be recognizable as such and shall have instructions for use plainly marked on their exterior surfaces.
- Boxes shall be securely mounted as directed by the AHJ.
- Box locations shall be designated by the AHJ.
- Where the intent is for complete coverage, boxes should be located within 305 meters (m [1000 feet (ft)]) of each other. In residential areas, this distance can be increased to 488 m (1600 ft).
- Schools, hospitals, nursing homes, and places of public assembly shall have a box located at the main entrance as directed by the AHJ.
- Boxes shall be conspicuously visible and highlighted with a distinctive color.
- Boxes mounted on poles shall be identified by a wide band of distinctive colors or signs placed 2.4 m (8 ft) above the ground and visible from all directions wherever possible.
- Location-designating lights of a distinctive color, visible for at least 457 m (1500 ft) in all directions, shall be installed over boxes.

Protected premises located within the area covered by the public fire alarm reporting system may have their fire alarm systems connected to a master box where the AHJ approves such connection. This type of arrangement is defined as an auxiliary fire alarm system.

NOTE: It is not the goal of this manual to cover all aspects of the codes and standards for these station types. The intention is to provide an overview of what is required by standards organizations across the globe. Driven by the escalating costs of insurance, methods will continue to be developed to reduce the risk of owning and operating something of value.

Initiation Devices

Overview

This section focuses on the components essential to various configurations of fire alarm system initiation devices. While there are multiple component manufacturers, the basics or fundamentals of the devices generally remain the same.

This section will expound on the following categories of initiation devices:

- Smoke detection
- Heat detection
- Flame detection
- Fire–gas detection
- Human detection—fire alarm pull stations
- Water flow detection
- Supervisory switches—tamper and pressure type

Detection

The components of a fire are:

- Smoke (particulate and aerosol).
- Heat.
- Light radiation.

Fire detection devices are built to detect one or a combination of these components. While all components are necessary for a fire to exist, all components may not exist at a detectable threshold. Detectors will be selected to detect the elements that may exist in a fire for the ambient conditions that are present. It also should be realized that similar nonfire components might exist in the same ambient conditions, which could cause unfavorable false alarm conditions.

Devices used for fire detection include:

- Smoke detectors that sense visible or invisible particles of combustion generated by burning, smoldering, or the incipient stage of combustion. These devices fall into two categories: photoelectric and ionization.
- Heat detectors that sense the high temperature or the temperature rise caused by a fire.
- Flame detectors that sense the radiation produced by a fire, such as visible light, or invisible radiation such as infrared (IR) or ultraviolet (UV) radiation.
- Fire–gas detectors that sense the gases produced by a fire.
- Beam detectors that sense obscuration.

 © 2012 BICSI®

Detection, continued

Each type of detector is further divided into line, spot, and air sampling:

- Line detectors are where detection takes place along a continuous path and may consist of linear rate-of-rise detectors, beam-type smoke detectors, and heat-sensitive cable detectors.
- Spot detectors have a sensing mechanism or element within an enclosure. These can be bimetallic heat detectors, fusible alloy, rate-of-rise, or a combination type of the above detector.
- Air-sampling (aspirating) detectors consist of a sampling tube routed through a location requiring protection. Pressure differential created by venturi effect or vacuum pump draws air from the protected space into a detection chamber.

Detectors may be further classified as restorable and nonrestorable types:

- Restorable detectors usually are not destroyed during the detection process. They return to a normal state when conditions return to normal.
- Nonrestorable detectors (e.g., fusible links) are destroyed during the detection process.

Smoke Detectors

Smoke is produced as a component of a fire that is either actually burning or in the incipient (beginning) stage. These smoke particles may be:

- Visible (burning or smoldering fire).
- Invisible (incipient fire).

Smoke detectors are designed to detect these components of combustion; however, the proper smoke detection device must be selected to detect the smoke type that will exist within the ambient condition or for the fire stage to be detected.

Smoke detectors are classified by type of detection as:

- Ionization.
- Photoelectric.
- Combination (ionization/photoelectric).

These are further classified for circuitry sophistication as standard, analog, and intelligent:

- Single station smoke detectors contain no special circuitry other than what is required to power the detector circuitry, monitor the alarm status of the detector, and provide trouble indication if a fault occurs within the detector. This is the least costly smoke detector unit.
- Analog-type detectors contain all the circuitry of the standard detector plus special circuitry that monitors, reports on sensitivity of the detector, and allows the FACP to adjust the sensitivity as the detector sensitivity declines because of accumulated dust and increased age.
- Intelligent-type detectors contain logic circuitry that allows the detector to recognize and respond to the actual combustion profile of various types of fires. This special feature allows the smoke detector to respond faster and minimize false alarms. Typically, this is the most expensive smoke detector unit.

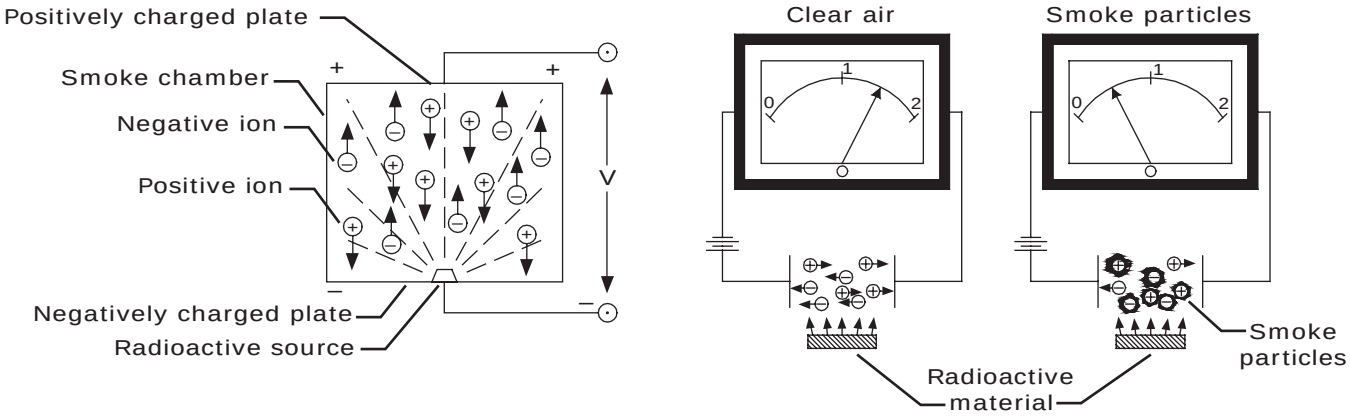
Ionization Detectors

The ionization fire alarm initiation device is also widely used. Its capability to detect smoke originating from fire is best utilized for clean-burning fires that produce small particles during combustion.

The typical ionization type of smoke detector consists of an alpha particle producing a radioactive source, a smoke chamber, and charged detector plates (see Figure 7.2):

- The alpha source causes the air within the smoke chamber to become ionized and conductive.
- As smoke particles enter the smoke chamber, the smoke particles attach themselves to the ionized air molecules, and the air in the chamber becomes less conductive.
- When the air conductivity within the chamber drops below a predetermined level, the alarm is triggered.

Figure 7.2
Typical ionization smoke detector



Advantages

Advantages of an ionization smoke detector include:

- Detects invisible products of combustion—Detects fires that are in the incipient stage or detects other aerosol-type smoke products.
- Acts quickly—Provides for earlier detection than other types of smoke detectors or heat detectors.

 © 2012 BICSI®

Ionization Detectors, continued

Disadvantages

An ionization detector:

- May provide false detection if used where volatile solvents, conductive material dusts, or high humidity are present.
- Detects the presence of smoke only, not toxicity.
- Has a potential for a high false alarm rate.

Typical Uses

Some of the more common uses for an ionization device are:

- Clean rooms.
- Computer rooms.
- Mechanical air ducts.
- Locations where sensitive detection methods are needed.

Photoelectric Detectors

Photoelectric-type smoke detectors are widely used and detect smoke by either the principle of light obscuration or light scattering. Its capability to detect smoke originating from fire is best utilized for fires that produce large particles during combustion.

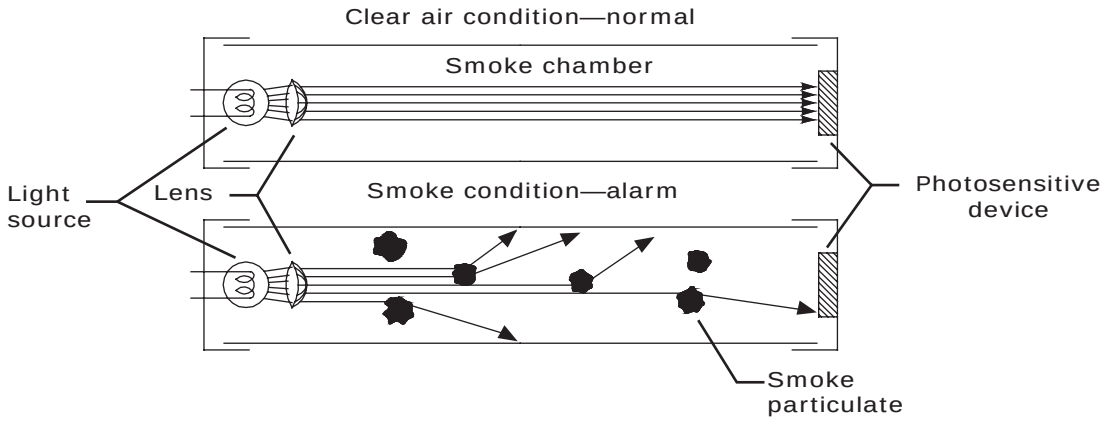
The fuel for a fire and, subsequently, the fire alarm actuation trigger, is dependent on the by-products of combustion. This requires the ESS designer to adequately take into consideration what materials a built environment is composed of and the purpose of the built.

Spot-type photoelectric smoke detectors using the light obscuration principle have a light emitting device, usually a light-emitting diode (LED), a smoke chamber, and a photosensitive device that receives the light directly from the light source and produces a monitored current (see Figure 7.3).

Smoke that enters the smoke chamber reduces the intensity of the light reaching the photosensitive device, which reduces the monitored current. When the intensity drops below a certain level, the sensor control circuitry detects a drop in the current produced by the photosensitive device. When the current falls below a preset threshold, the smoke alarm is triggered.

Photoelectric Detectors, continued

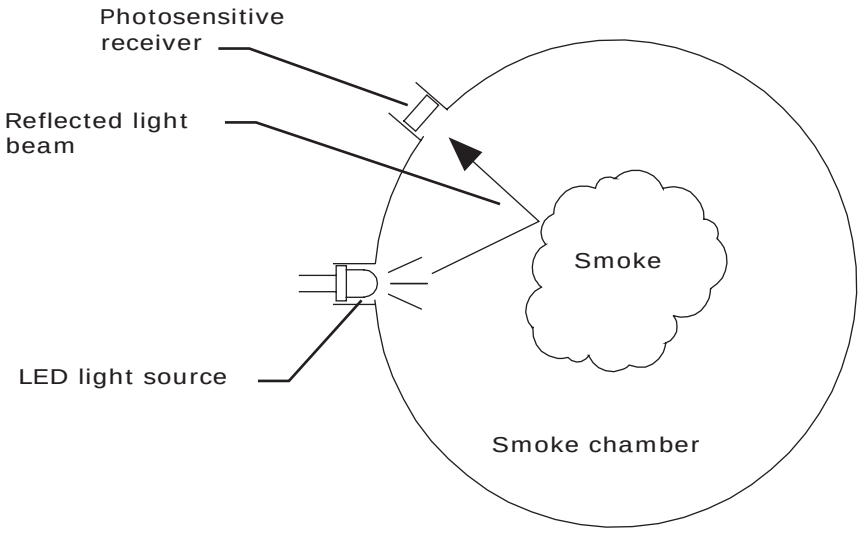
Figure 7.3
Photoelectric smoke detector using principle of light obscuration



Spot-type photoelectric smoke detectors that use the light scattering principle are constructed similar to the detectors that use the light obscuration principle except that the photosensitive device is set so that it cannot see the light source directly (see Figure 7.4).

When smoke enters the chamber, the smoke particles reflect the light from the source into the photosensitive receiver. When sufficient light intensity is detected, the alarm is triggered.

Figure 7.4
Typical photoelectric smoke detector using principle of light scattering



LED = Light-emitting diode

 © 2012 BICSI®

Photoelectric Detectors, continued

Advantages

Advantages of photoelectric smoke detectors include:

- Considered to be a life-saving device
- Sensitive to visual particles of smoke
- Detect smoldering low-heat fires
- More sensitive than heat detectors
- Provide early warning

Disadvantages

Disadvantages of photoelectric smoke detectors include:

- Easily contaminated by dust, causing reduced sensitivity
- Have the potential for a high false alarm rate
- Must be cleaned on a regular basis
- Detect the presence of smoke, not toxicity
- Have false alarms caused by insects attracted to light sources

Typical Uses

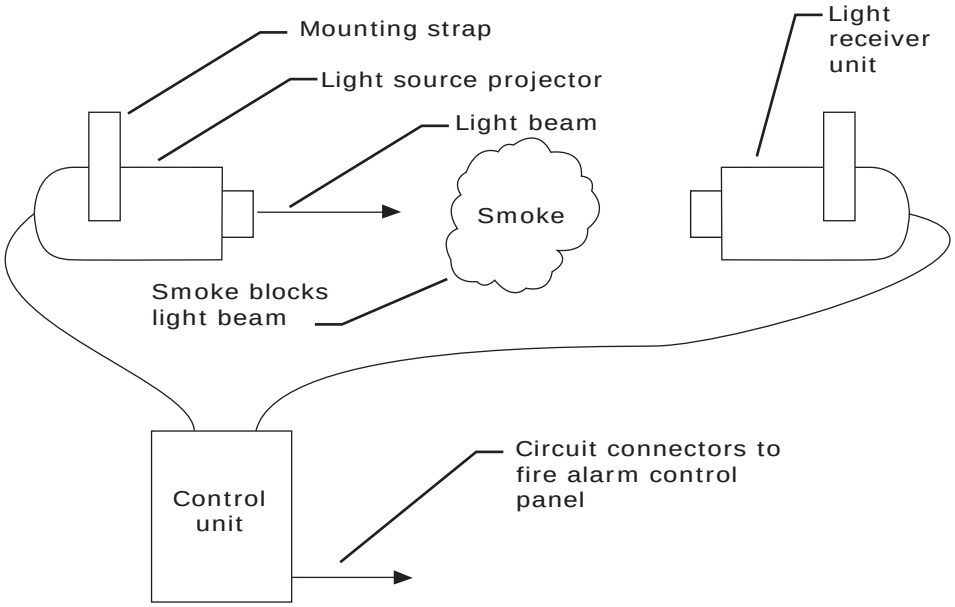
Photoelectric smoke detectors typically are used in:

- Office areas.
- Clean rooms.
- Raised floor spaces.
- Atriums and corridors.
- Meeting rooms.
- Data centers.
- Telecommunications rooms (TRs).
- Electrical equipment rooms (ERs).
- Sleeping rooms.
- Storage closets.

Beam Detectors

Beam smoke detectors are line-type photoelectric detectors, consisting of a separate light source and photosensitive receiver (see Figure 7.5). These devices are usually installed in large open areas where there is an unobstructed line of sight (LoS) between the light source and the receiver and where the use of spot-type detectors would be economically unfeasible because of the number of spot-type detectors required. These detectors operate on the principle of light obscuration.

Figure 7.5
Typical photoelectric beam-type detector



Advantages

Advantages of beam smoke detectors include:

- Cover a large area economically
- Quick acting

Disadvantages

Disadvantages of beam detectors are that they require:

- Unobstructed LoS between the light source and the receiver.
- Correct alignment to be maintained.

 © 2012 BICSI®

Beam Detectors, continued

Typical Uses

Beam smoke detectors are used in large:

- High atriums.
- Manufacturing spaces.
- Churches.
- Chapels.
- Stairwells.

Duct Smoke Detectors

Duct smoke detectors (see Figure 7.6) consist of:

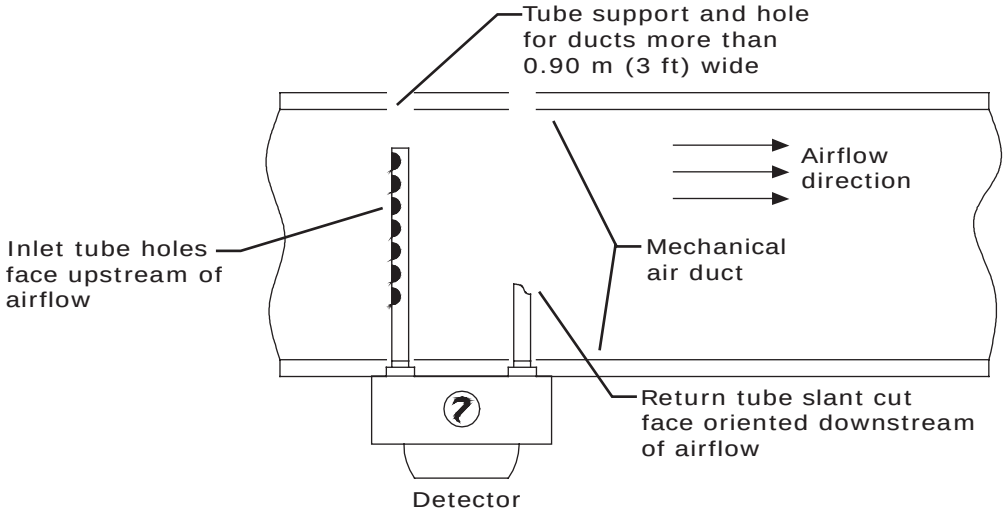
- An air-sampling tube.
- A smoke detector chamber.
- A photoelectric smoke detector device or ionization type of detector.

The air-sampling tube directs samples of the air in the space into the smoke detector chamber where it passes into the smoke detector for processing.

These types of smoke detectors typically are used to sense smoke in air conditioning ducts prior to entering (return air side) or leaving (supply air side) the air handling devices or fan unit.

These detectors are not accepted or recognized by code as an alternative for area detection for life safety applications as smoke particles entering the duct system will be dispersed in the air stream and will not be detected until smoke concentration reaches detectable levels. Another air-sampling type of duct smoke detector is the air-sampling aspirating fire detection unit.

Figure 7.6
Typical duct smoke-type detector



ft = Foot
m = Meter

Air-Sampling (Aspirating) Fire Detection Systems

Overview

For environments where detection of smoke is most critical, an air-sampling system provides the earliest possible detection. A number of applicable codes must be adhered to regarding air-sampling systems, including local codes. In every case, legalities pertaining to the selection, installation, approval, and integration of components in a fire alarm system must be adhered to strictly. This conformance protects life and property.

Where fire and smoke detection is critical (e.g., telephone central offices, data and voice communication centers, museums, high-value properties), an air-sampling (aspirating) fire detection system should be considered. These are the most sensitive detection systems currently available. They detect a fire before smoke or flame is apparent.

The typical system consists of a series of inconspicuous tubes, which carry samples of air from a protected space to a high-sensitivity detector. Air sampling works by continually drawing air into the tubes via a high-efficiency aspirator. A sample of this air is transported through a filter to the detection chamber.

The systems can detect invisible particles generated during the precombustion stage of a fire at levels of obscuration as low as 0.003 percent per foot compared with 3 percent per foot sensitivity for a typical spot-type photoelectric smoke detector. Manufacturers' literature claims they are up to 1000 times more sensitive than conventional ionization or photoelectric types of smoke detectors.

Functionality of an Air-Sampling Fire Detection System

An air-sampling or aspirating-type fire detection system is a self-contained smoke detection package consisting of five primary components:

- Air-sampling system
- Aspiration system
- Filter assembly
- Detector
- Control system

The fire detection system uses a network of pipes to continuously draw air samples and direct them to a central smoke detector.

The system operates with a network of sampling pipes that extend into the protected area. The pipes have various diameters and usually are made of a thermoplastic material. An internal aspirator continuously draws air into the piping network. The systems use either a filter assembly or laser particle counting technology to filter out airborne dust and debris particles, which helps to eliminate false readings.

 © 2012 BICSI®

Functionality of an Air-Sampling Fire Detection System, continued

The air samples then pass into the detection chamber for analysis. The detector uses the principle of light scattering as its method of detection. In this chamber, the sampled air is illuminated by a light source such as a laser or broad-spectrum xenon lamp. This light bounces off the small particles released by the combustion materials.

Sensitive receivers detect the light scattered by these particles. The receivers detect this light energy, representing the level of smoke in the air sample. This level is then sent to the control system for processing.

The control system receives and processes the information. At the control panel, smoke obscuration levels are presented graphically on a display, indicating three or more typical smoke level thresholds:

- Alert
- Action
- Fire

This display is programmable, enabling sensitivity and alarm level settings to be selected by the user. The control system reports trouble and activates the alarm. Like other systems, alarms can be reported locally or to an off-site location. This system also stores a historical log of smoke levels and events.

Applications

Some environments where air-sampling systems are most appropriate include the following high reliability:

- Telecommunications areas
- Data centers
- Hospitals
- Clean room environments

Air-sampling systems also are used in the following areas where smoke is difficult to detect because of the large size or where there are great air volume changes:

- Warehouses
- Atriums
- Aircraft hangars
- Cold storage areas
- Indoor stadiums

Applications, continued

Air-sampling systems can also provide enhanced protection in harsh environments. Environments with a higher degree of pollution or with extreme environmental characteristics have posed a problem for conventional smoke detection systems because of their inability to detect a fire event versus normal operating conditions. Air-sampling systems are able to provide a superior level of detection in these hostile applications.

These areas include:

- Power stations.
- Mines.
- Public transport automotive operations.
- Paper and timber mills.
- Manufacturing operations.

Other areas where air-sampling systems are used include places where appearance is important. The aesthetic requirements of some buildings pose a challenge for the conventional smoke detection systems. Air-sampling provides concealed smoke detection for these applications.

Some examples are:

- Historical buildings.
- Cathedrals.
- Museums.
- Archives.
- Art galleries.

In this type of application, a small hole is made in the ceiling for a detection tube to be inserted so that an air sample can be taken and analyzed.

Sampling Pipe

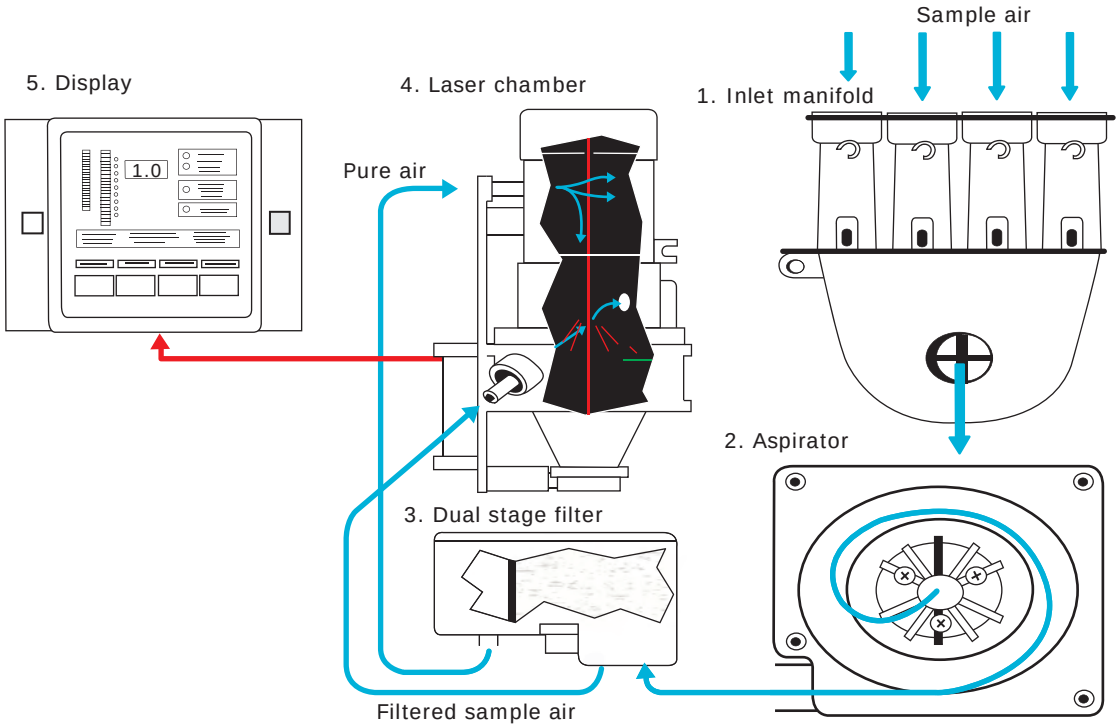
The sampling pipe often consists of plastic tubing with various diameters. The material must be suitable for the environment in which it is installed. Certain types of material must be used as specified by applicable codes, standards, and the AHJ. All joints in the pipe must be air tight and made using solvent cement, except at entry to the detector.

 © 2012 BICSI®

Sampling Pipe, continued

This pipe is identified at regular intervals along its entire length as aspirating smoke detector pipe. Typically, applicable codes dictate the interval for this identification. The systems are air balanced, much like a mechanical air distribution system, by varying the sampling head hole size of the individual tube. For example, the sample head holes farther away from the detector module are larger than the ones close to the module so that air is sampled at a uniform rate from all areas. See Figure 7.7 for an example of how an air-sampling system works.

Figure 7.7
Air-sampling system



Heat Detectors

As the name implies, heat detectors detect the heat produced by a fire. Heat detectors can respond to a:

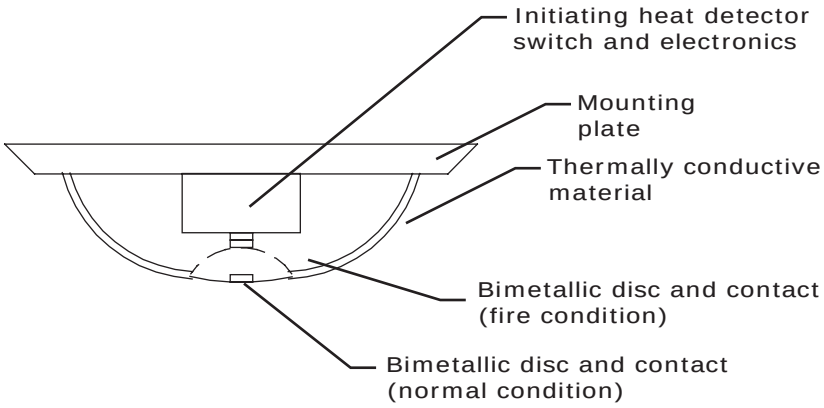
- Fixed temperature limit.
- Rapid rate of change of the temperature in the protected area.
- Combination of these types of detection.

These devices, while slow to respond and having been largely replaced by the smoke detector, still have limited uses in the detection of fires. These are the least expensive and most reliable of the detecting devices.

Fixed Temperature Spot Heat Detectors

Typical fixed temperature spot-type smoke detectors contain a bimetallic switch element that closes at a specified temperature limit (see Figure 7.8). This switch is composed of two metals, each having a different temperature coefficient of expansion. As this bimetallic element heats, the metal with the higher coefficient of expansion causes the switch to bend or curve, closing the switch contacts, thus indicating an alarm condition.

Figure 7.8
Typical fixed temperature heat detector



Another type of heat detector mechanism consists of a fusible link holding spring-loaded contacts apart. When the temperature reaches a predetermined level, the metal holding the link together melts, allowing the contacts to close.

Line-type heat detectors are cables that detect heat along their entire length. A line-type heat detector may consist of two wires that are separated by an insulator. After the heat builds to a certain level, the insulation melts, allowing the wires to touch and current to flow, initiating an alarm.

Another type of line-type heat detector consists of a central conductor and an outer metal conduit or tube assembled coaxially and separated by semiconductor material. As the temperature rises, the semiconductor allows more current to flow until the current reaches a predefined threshold, at which time the alarm is initiated. After the temperature returns to normal, the detector returns to its normal nonfire state.

Bimetallic spot and coaxial line types of heat detectors are self-restoring. Fusible link and melting insulation types of line heat detectors are not self-restoring.

 © 2012 BICSI®

Fixed Temperature Spot Heat Detectors, continued

Table 7.1 indicates the classifications, operating temperature ranges, and related color codes of fixed temperature heat detectors according to *NFPA 72*.

Table 7.1
Temperature classification for heat-sensing fire detectors

Temperature Classification	Temperature Rating Range °C	Temperature Rating Range °F	Maximum Ceiling °C	Maximum Ceiling °F	Color Code Temperature
Low*	39–57	100–134	28	80	Uncolored
Ordinary	58–79	135–174	47	115	Uncolored
Intermediate	80–121	175–249	69	155	White
High	122–162	250–324	111	230	Blue
Extra high	163–204	325–399	152	305	Red
Very extra high	205–259	400–499	194	380	Green
Ultra high	260–302	500–575	249	480	Orange

* Intended only for installation in controlled ambient areas. Units must be marked to indicate maximum ambient installation temperature.

°C = Degree Celsius
°F = Degree Fahrenheit

Advantages

Advantages of heat detectors include:

- Lower cost than smoke detector units
- More reliable than smoke detector units
- Not affected by dusty or dirty environments
- Minimal maintenance

Disadvantages

Disadvantages of heat detectors include:

- Slower to respond than smoke detectors
- Will not detect products of combustion
- Only suitable for protection of property

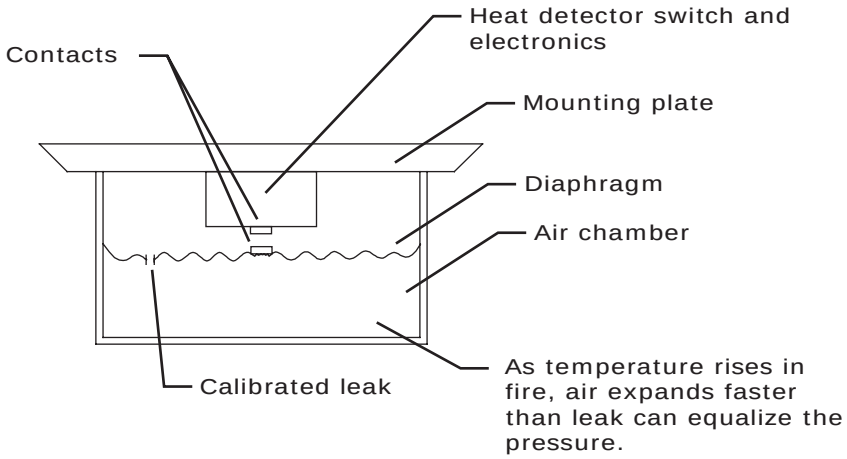
Rate-of-Rise Spot Heat Detectors

While fixed temperature detectors respond slowly to a certain temperature level in a space, the air temperature may take several minutes for the volume of air in the space to increase to the temperature needed to trigger an alarm. In contrast, the rate at which the air temperature changes during an event is quite rapid. Measuring this change provides a faster alarm response than measuring the temperature level in a space.

The rate-of-rise detector measures the change in the temperature of the space through the use of a differential pressure switch (see Figure 7.9). This switch contains an air chamber separated from the air in the ambient space by a flexible diaphragm. As air in the ambient space changes temperature, the air pressure increases, creating a differential pressure across the diaphragm.

The air chamber is constructed with a calibrated leak so that normal temperature and pressure fluctuations within the room space adjust across both sides of the diaphragm and will not cause the alarm contacts to close. During a fire, the air temperature rises at a rate faster than normal, causing an increase in pressure on the room side of the diaphragm. The leak cannot compensate; therefore, the diaphragm moves and closes the detector contacts.

Figure 7.9
Typical rate-of-rise heat detector

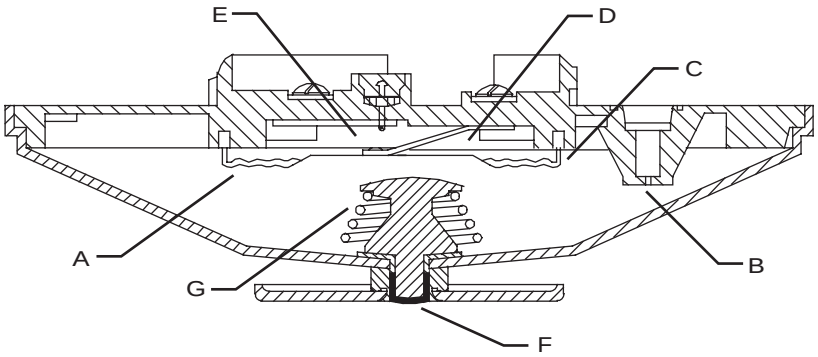


 © 2012 BICSI®

Combination Rate-of-Rise and Fixed Temperature Heat Detectors

This detector provides the best of both principles of the rate-of-rise and fixed temperature heat detectors to prevent false alarms (see Figure 7.10).

Figure 7.10
Principle of operation of typical combination rate-of-rise and fixed temperature heat detector



A = Air chamber
B = Vent
C = Diaphragm
D = Electrical contacts
E = Contact screws
F = Fusible alloy
G = Spring

A spot-type combination rate-of-rise, fixed temperature device. The air in chamber (A) expands more rapidly than it can escape from vent (B). This causes pressure to close electrical contact (D) between diaphragm (C) and contact screw (E). Fixed temperature operation occurs when fusible alloy (F) melts releasing spring (G), which depresses the diaphragm closing contact points.

Advantages

Advantages of a combination rate-of-rise and fixed temperature heat detector include:

- Responds faster than the fixed temperature detector
- Not affected by dust and dirt
- More reliable than smoke detector units
- Less expensive than smoke detector units
- Minimal maintenance

Disadvantages

The disadvantages include:

- Slower to respond than smoke detectors
- Will not detect products of combustion
- Only suitable for protection of property

Rate-Compensated Heat Detectors

Rate-compensated heat detectors are devices that are designed to activate at a predetermined temperature in a space regardless of the rate at which the temperature in the space increases. This is accomplished by compensating for the thermal lag between the room temperature and the interior of the device.

Construction consists of an outer metal tube that expands at a fixed rate. Within this tube, alarm contacts close when a certain expansion distance is reached, but this expansion is opposed by another metal device.

At a slow rate-of-rise in temperature, the outer tube expands, drawing the contacts closer together. The inner metal device exerts a counter force, keeping the contacts separated until the entire device has been heated to its rated temperature.

At a rapid rate-of-rise in temperature, the outer tube expands faster than the inner device can compensate. Therefore, the alarm contacts close when the entire device has been heated to a lower level, thus compensating for thermal lag.

Advantages

Advantages of a rate-compensated heat detector include:

- Responds accurately and positively to fire threats
- Virtually eliminates false alarms
- Available in a wide range of temperature settings
- Not affected by dust and dirt
- More reliable than smoke detector units
- Less expensive than smoke detector units
- Can be obtained with hazardous area rating
- Minimal maintenance

Disadvantages

The disadvantages include:

- Responds more slowly than smoke detectors
- Will not detect products of combustion
- Only suitable for protection of property

Typical Uses

Rate-compensated heat detectors can be used in:

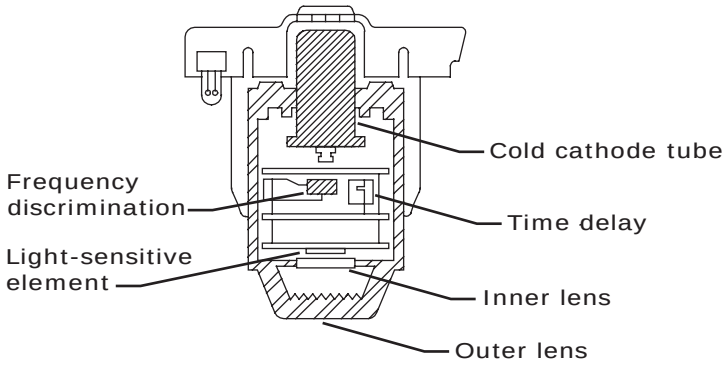
- Mechanical rooms.
- Boiler rooms.
- Electrical rooms.
- Areas under stairs.
- Locations having dirty or dusty environments.
- Elevator machine rooms.

 © 2012 BICSI®

Flame Detectors

Flame detectors are used to detect the light radiation component of a fire (see Figure 7.11). Typical detectors of this type detect the wavelength of IR, UV, or a combination of these two. These detectors are fast acting and are used in areas where rapidly occurring fires or explosions could occur.

Figure 7.11
Typical infrared flame detector



Advantages

An advantage of flame detectors is that they are fast acting.

Disadvantages

The disadvantages include:

- Narrow field of vision
- Expensive
- Unobstructed field of view required
- Difficult to maintain
- Lighting for UV

Typical Uses

Flame detectors can be used in:

- Fuel loading docks.
- Industrial process spaces.
- Other hazardous areas where a fast developing fire could occur.

Gas Detectors

These detectors respond to the various gases produced during the combustion process. These gases may be various concentrations of:

- Carbon monoxide (CO).
- Carbon dioxide (CO_2).
- Steam (H_2O).

One method of construction uses a semiconductor material. Under normal conditions, oxygen is absorbed by the material. Under a fire condition, combustion gases are absorbed by the semiconductor material. This changes the material's electrical conducting characteristics and causes an alarm condition. This type of detector is prone to false alarms because of the nonspecific nature of its alarm.

Another method of detection uses a catalytic element (usually platinum) encased in an alumina bead. As the gases produced by the combustion process are deposited on the catalytic element, its temperature increases, and the electrical resistance of the element changes. The element is connected into a Wheatstone bridge circuit with an identical element to provide long-term stability.

Advantages

Advantages of a gas detector include:

- Detects products of combustion
- Detects levels of gases produced between the occurrence of detectable particulate levels and detectable heat levels because of its sensitivity
- Detects gases prior to reaching lethal levels

Disadvantages

The disadvantages include:

- Can be prone to false alarms
- Must be mounted at a low level and is prone to damage
- Can be compromised
- Not suitable for areas where CO and CO_2 are produced as part of the functions within the area
- Cannot be considered as a universal replacement for smoke and heat detectors
- Expensive

Typical Uses

Gas detectors are most suitable for use as a supplement for smoke and heat detectors in small volume sleeping areas (e.g., hotel rooms, residential bedrooms).

 © 2012 BICSI®

Coverage for Smoke and Heat Detectors

NFPA 72 defines three types of coverage for smoke and heat detectors:

- Total coverage—"...shall include all rooms, halls, storage areas, basements, attics, lofts, spaces above suspended ceilings, and other subdivisions and accessible spaces as well as the inside of all closets, elevator shafts, enclosed stairways, dumbwaiter shafts, and chutes."
- Partial or Selective coverage—"Where codes, standards, laws, or authorities having jurisdiction require the protection of selected areas only, the specified areas shall be protected in accordance with this Code."
- Nonrequired coverage—"Detectors installed for reasons of achieving specific fire safety objectives, but not required by any laws, codes, or standards, shall meet all of the requirements of this Code."

NOTE: Types of coverage also are specified in various global fire codes such as the *International Fire Code*® and *Uniform Fire Code*. It also is governed by the AHJ for the locality in which the building resides. The coverage required depends upon the occupancy type of the building.

NFPA 72 specifies installation requirements for smoke and heat detectors of all types. Smoke and heat detectors should be installed in accordance with the manufacturer's instructions and the requirements of *NFPA 72*.

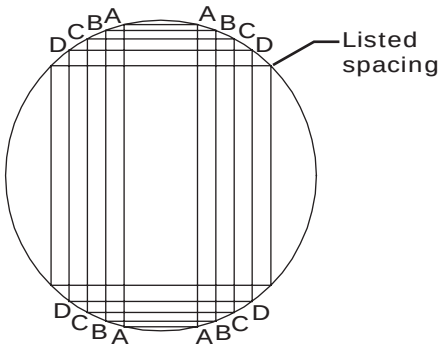
Typically, spot-type smoke detectors should be installed on ceilings not less than 100 millimeters (mm [3.9 inches (in)]) from a sidewall or on walls not less than 100 mm (3.9 in) from the ceiling (see Figure 7.12).

With regard to detector spacing, consideration also should be given to the:

- Type of construction.
- Locations of beams and columns.
- Ceiling slopes.
- Location of air supply ducts.

Coverage for Smoke and Heat Detectors, continued

Figure 7.12
Typical detector coverage areas



Rectangles
A = 3.0 m (10 ft) x 12.5 m (41 ft) = 38.1 m^2 (410 ft^2)
B = 4.6 m (15 ft) x 11.9 m (39 ft) = 54.3 m^2 (585 ft^2)
C = 6.0 m (20 ft) x 11.3 m (37 ft) = 68.8 m^2 (740 ft^2)
D = 7.5 m (25 ft) x 10.4 m (34 ft) = 78.9 m^2 (850 ft^2)
Listed spacing = 9.0 m (30 ft) x 9.0 m (30 ft) = 84.0 m^2 (900 ft^2)

ft = Foot
m = Meter

Spot-type heat detectors should be located on the ceiling. The height of the installation will determine the detector spacing. Detector spacing will be reduced for ceiling heights above 3.1 m (10 ft) by the percentage dictated by the table listed in *NFPA 72*. Fixed temperature and rate-compensated detectors should be selected based on the lowest operating temperature rating that will provide the earliest possible detection without causing nuisance false alarms.

With regard to detector spacing, consideration should be given to the:

- Ceiling construction.
- Location of beams and columns.
- Ceiling slopes.
- Proximity of supplies to smoke detectors.

 © 2012 BICSI®

Other Fire Detection System Devices

Pull Stations

Humans are excellent detectors of fires. When fire is detected by humans, an alarm can be initiated by the use of strategically placed pull stations. Pull stations are simple switches that, when pulled, turn on the fire alarm notification appliances.

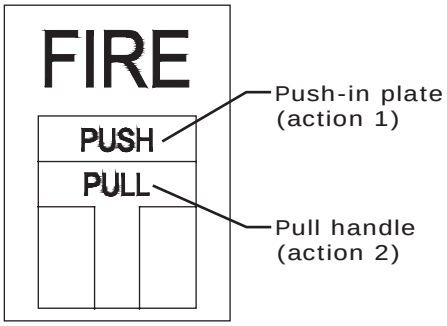
Pull stations come in two types:

- Single action.
- Double action.

Single action pull stations are so named because they require one action, such as pulling a lever, to initiate the alarm. Double action pull stations require two actions, such as lifting an access door or breaking a glass rod or glass pane and then pulling the lever to initiate the alarm. This provides a physiological barrier to prevent false alarms. Sometimes, the double action stations are provided with a telltale to indicate a prealarm or trouble condition if the first action is completed without the following of the lever pull.

Pull stations are located at each door that is a point of egress and are strategically placed so that the linear travel distance between pull stations does not exceed 61 m (200 ft). Typical mounting heights of pull stations should be 1220–1370 mm (48–54 in) above the floor (depending on the side or front reach rule) to comply with the Americans with Disabilities Act (ADA) and other states' handicapped codes. See Figure 7.13 for a typical pull station.

Figure 7.13
Typical fire alarm pull station



Fire Suppression Systems and Supervision Devices

Overview

The ESS designer should understand the relationship between the fire detection and alarm system and the fire suppression system. While each serves a similar purpose in the protection of life and property, the fire detection system is required to interface with the fire suppression system by using devices designed to monitor (supervise) the status of this system.

Supervisory devices are the monitoring equipment required for fire suppression (sprinkler or clean agent) systems. These devices monitor abnormal conditions in the suppression system. Their duties include the supervision of the open or closed position of control valves supplying water or agent to the system, fluctuation in system air pressure and fire pump status, and temperature/level of water or agent in gravity and pressure tanks (when used).

Monitoring Devices

Water Flow Detectors

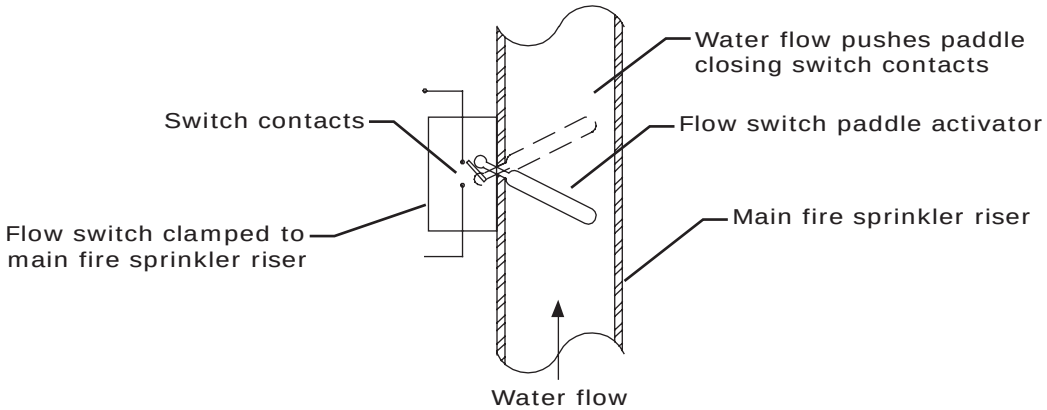
Water flow detectors are used in conjunction with automatic sprinkler systems and indicate the action of the fire suppression system. Vane and pressure are the two types of detectors used in these systems.

Vane

Vane-type water flow detection devices are equipped with a paddle that is inserted directly into the sprinkler riser.

The water flow switch consists of a simple two-position switch that is actuated by the paddle within the sprinkler pipe (see Figure 7.14). The paddle will respond to a flow of 37.85 liters (10 gallons) per minute in the system and indicate an alarm condition at the fire alarm panel. These devices may also be equipped with a time delay to guard against false alarms that may be caused by normal water pressure fluctuations. These delays are adjustable from approximately 0 to 120 seconds.

Figure 7.14
Typical water flow detector



 © 2012 BICSI®

Monitoring Devices, continued

Pressure

Pressure-type water flow detectors are recommended for dry pipe systems or wet pipe systems equipped with an alarm check valve. For wet systems, these devices are connected to the alarm port of the alarm check valve. The pressure water flow indicators are factory adjusted to activate at 28 to 55 kilopascal (kPa [4 to 8 (pound-force per square inch [psi])]) of rising pressure and will indicate an alarm condition as additional water enters the system.

A pressure sensing device containing a time delay is recommended to avoid false alarms because of pressure fluctuations in the system. These delays are adjustable from approximately 0 to 120 seconds.

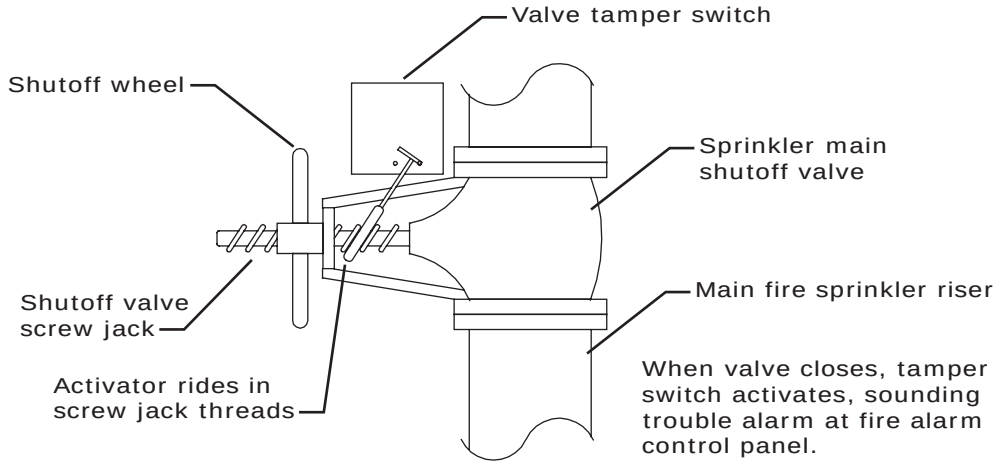
Valve Tamper Switches

Valve tamper switches are simple single throw switches interlocked with the automatic sprinkler system shutoff valve or zone valve (see Figure 7.15). Each valve in an automatic sprinkler system is required to have a tamper switch installed. When a sprinkler system valve is closed, the switch closes and sends a trouble signal to the FACP and its companion annunciator panel, if installed.

Tamper monitoring devices are used to monitor the open position of valves, such as outside stem and yoke (OS&Y) valves. These devices are mounted directly on the valve stem and signal an off and normal position within two revolutions of the hand wheel.

Post indicator, butterfly, and other similar devices are used to monitor the open position of valves and are connected directly to the valve stem. Each unit contains various configurations of contacts for connection to the supervisory circuit at the FACP.

Figure 7.15
Typical valve tamper switch



Monitoring Devices, continued

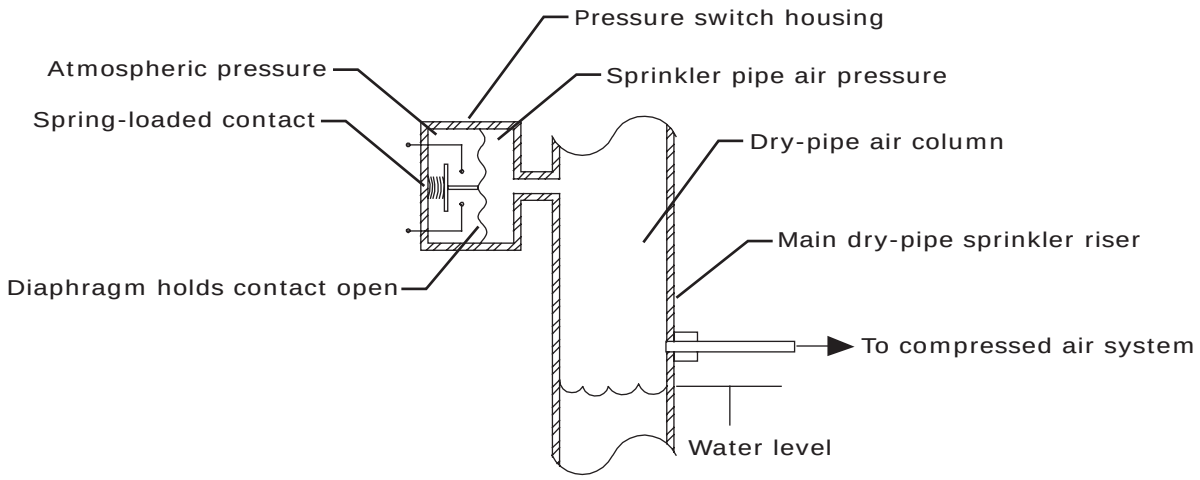
Pressure Switches

Pressure switches are used to monitor high and low pressures in a dry sprinkler system. For a wet system, other types of air or water pressures are monitored such as supply pressure or fire pump positive pressure (indicating operation of the fire pump).

If the air operating pressure is increased or decreased by 69 kPa (10 psi), the pressure switch will close and initiate a trouble alarm on the fire alarm panel and its associated annunciator panel, if one is installed. A separate signal is relayed when the system is restored to its normal operating pressure.

For dry-pipe-type automatic sprinkler systems, pressure switches monitor the pressure in the air column (see Figure 7.16). The pressure switch is installed in the main dry-pipe sprinkler riser just above the water column within the air filled dry area.

Figure 7.16
Typical pressure switch



 © 2012 BICSI®

Notification Appliances

Overview

In addition to reliable alarm initiation, effective fire alarm notification is the critical element of fire life safety systems. Fire alarm notification and signaling appliances protect life by automatically warning occupants of a fire condition and signaling the need to evacuate the building or area. To achieve its intended purpose, fire alarm notification needs to function in a way that ensures that the signal is correctly perceived and interpreted by building occupants.

The following design goals are necessary considerations when designing effective notification:

- Signal audibility
- Intelligibility
- Visibility

To ensure that good practice is followed, there are codes, standards, and regulations that govern the design of compliant fire alarm notification. Some examples of governing organizations and documents that define notification requirements are the NFPA, American National Standards Institute (ANSI), and AHJ. This section will not discuss standards affecting design practice. Instead, the section will address the components that constitute fire alarm notification.

Types of Notification Appliances

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 they are generally classified in the following categories:

- Bells
- Chimes
- Horns
- Speakers
- Strobes
- Chime/strobes, horn/strobes, speaker/strobes

When used for fire alarm signaling, notification appliances are required to carry a NRTL listing consistent with their intended use. Similarly, notification appliances used for fire alarm signaling are almost exclusively designed to operate on 24 volt direct current (Vdc) power so that they will continue to function normally on battery backup power in the event of a loss of primary power from the fire alarm system.

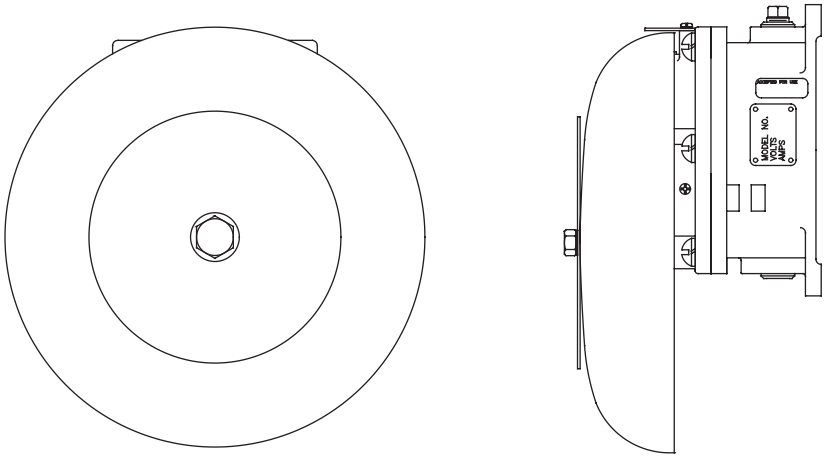
Types of Notification Appliances, continued

Bells

Fire alarm bells are one of the oldest types of fire alarm notification appliances and are still widely used (see Figure 7.17). Bells are usually electromechanical in nature, using magnetic activation to mechanically strike a gong, thereby generating the audible tone. Because they do not utilize integrated circuitry, bells can be an attractive choice for harsh environments or exterior applications.

Bell sizes vary, with larger gong radii generally producing more decibel output. Manufacturer documentation should be consulted for bell output decibel ratings.

Figure 7.17
Typical fire alarm bell



 © 2012 BICSI®

Types of Notification Appliances, continued

Chimes

Like fire alarm bells, chimes originated as electromechanical devices, using magnetic fields to move internal mechanical parts. Electromechanical chimes can still be obtained, but they are no longer in common use. Instead, modern chime appliances are usually electronic, solid-state devices using electronic tone generators to simulate the chime tone (see Figure 7.18) and can include visual notification devices such as strobes (see Figure 7.19).

Chime appliances are characterized by a soft and pleasing tone, which makes them a natural choice for many private mode signaling applications (e.g., hospitals, other institutional occupancies). The muted tone of the chime device reduces the likelihood of panic, which is favorable in institutional environments.

Chime appliances often have field-selectable output settings, located under the cover plate, and can be adjusted by a qualified technician. Manufacturer documentation should be consulted for chime output decibel ratings.

Figure 7.18
Typical fire alarm chime

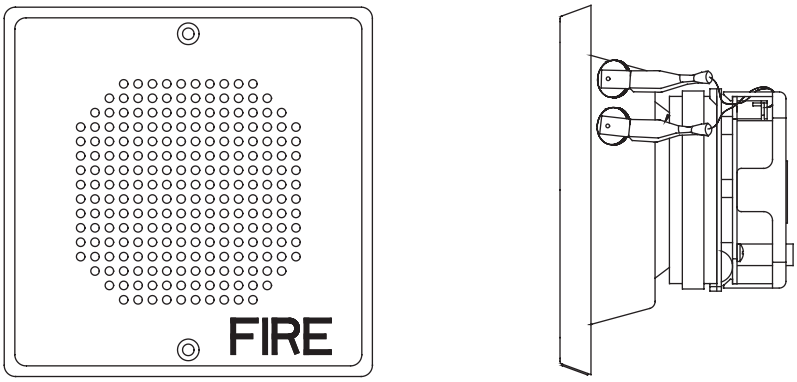
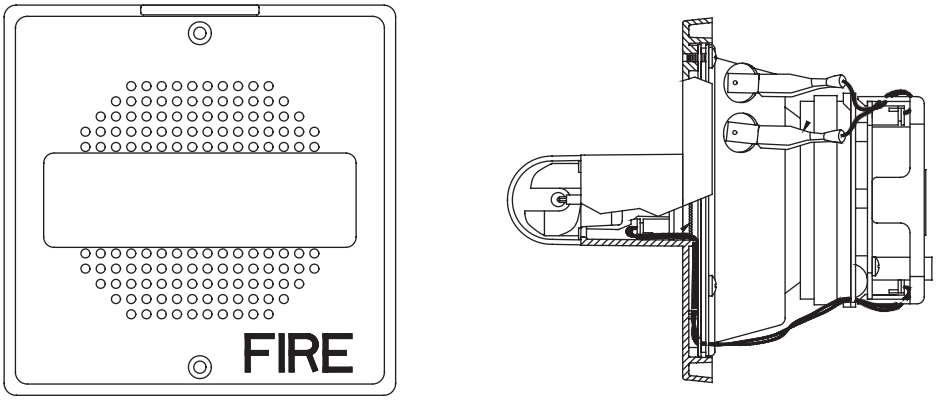


Figure 7.19
Typical fire alarm chime with integrated strobe



Types of Notification Appliances, continued

Horns

Horns are likely the most commonly used fire alarm notification appliance (see Figure 7.20) and, like chimes, can contain integrated strobes (see Figure 7.21). They are almost exclusively electronic and are characterized by high output and piercing tonality.

Horns are ideal for high ambient noise environments and applications where high and penetrating output is required. Horns are common in public mode signaling applications. Like chimes, horn appliances also usually have field-selectable output settings located under the cover plate.

Manufacturer documentation should be consulted for horn output decibel ratings. High-output horns with ratings as high as 110–120 decibels (dB) are available, but they should be used only with caution since they can damage hearing.

Figure 7.20
Typical fire alarm horn

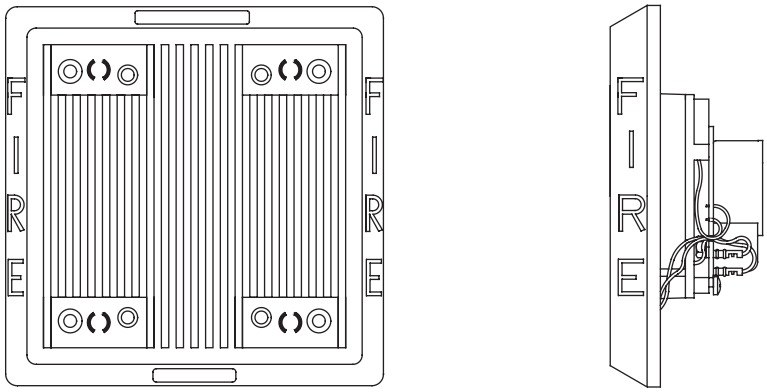
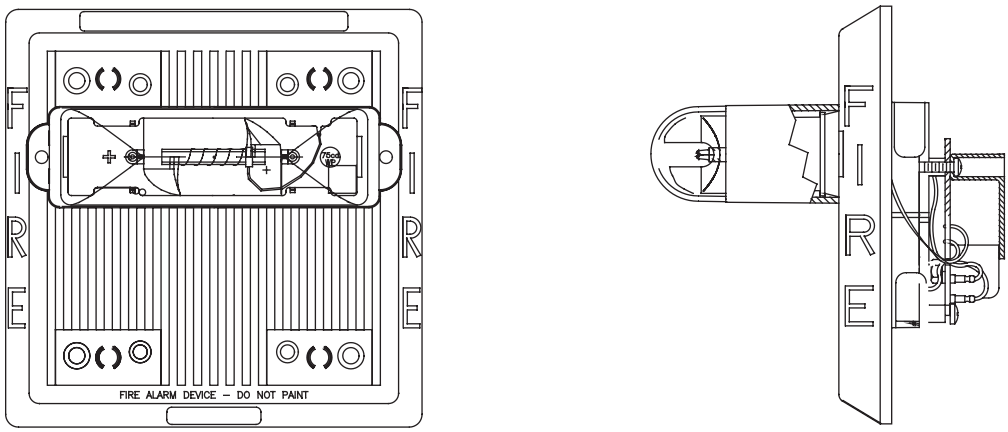


Figure 7.21
Typical fire alarm horn with integrated strobe



 © 2012 BICSI®

Types of Notification Appliances, continued

Speakers

Speaker appliances are commonly used with emergency voice evacuation systems and in applications that require the reproduction of multiple or varied tones or signals. They operate on a different principle than horns, utilizing an internal magnet, voice coil, and cone to generate a wide variety of tones and pitches, including spoken announcements. Because of this, speakers are not powered by standard 24 Vdc. Instead, speakers used in voice evacuation applications require audio circuiting, which originates at the voice evacuation system's headend amplifiers. This circuiting generally carries speaker level audio signal to
the distributed speaker appliances.

Some speaker types are designed with integral amplifiers and require only line level input from the voice evacuation system headend. Typical fire alarm speakers are shown in Figures 7.22 and 7.23.

Speakers have not been used in fire alarm signaling applications for as long as horns or bells. However, they are becoming more favored by code officials and jurisdictions because of their intelligibility and ability to give specific instructions to building occupants. Speakers are required in high-rise building applications and widely used in assembly-type occupancies. Speakers can also be utilized for mass notification.

Speaker appliances contain internal transformers to convert electrical signals to acoustical output. Output level depends on the transformer setting, which generally is accomplished with adjustable tap settings. Fire alarm speaker types are available with selectable taps ranging anywhere from 1/8 watt (W) to 16 W. Manufacturer's documentation lists the appliance tap settings with corresponding output decibel ratings.

Types of Notification Appliances, continued

Figure 7.22
Typical fire alarm speaker

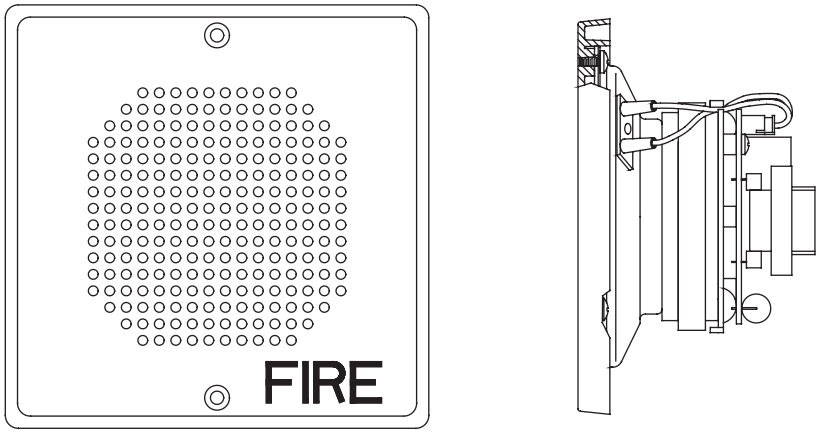
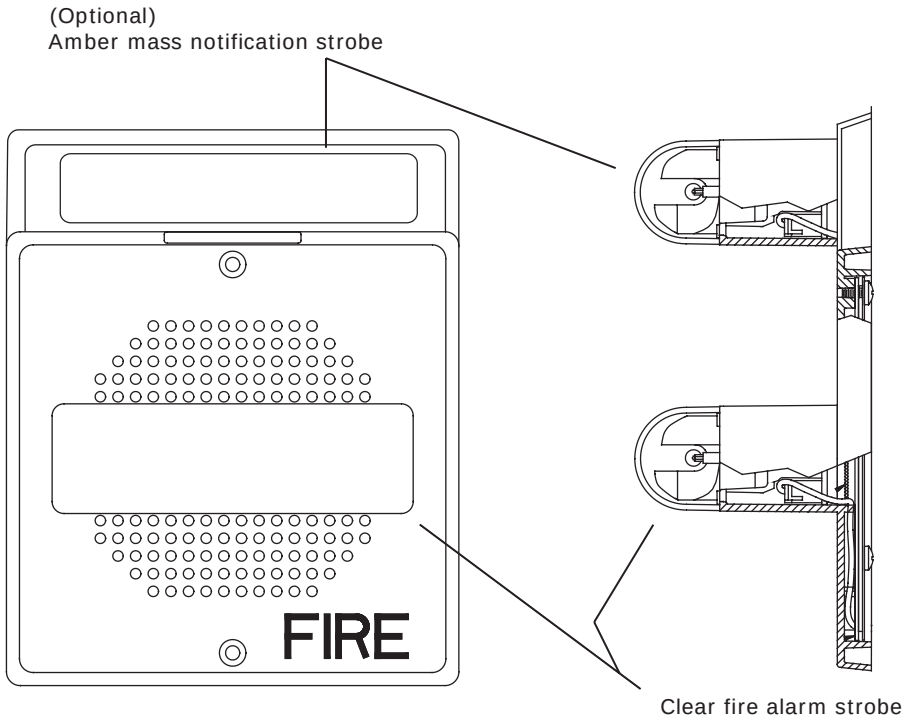


Figure 7.23
Typical fire alarm speaker with integrated strobe



 © 2012 BICSI®

Types of Notification Appliances, continued

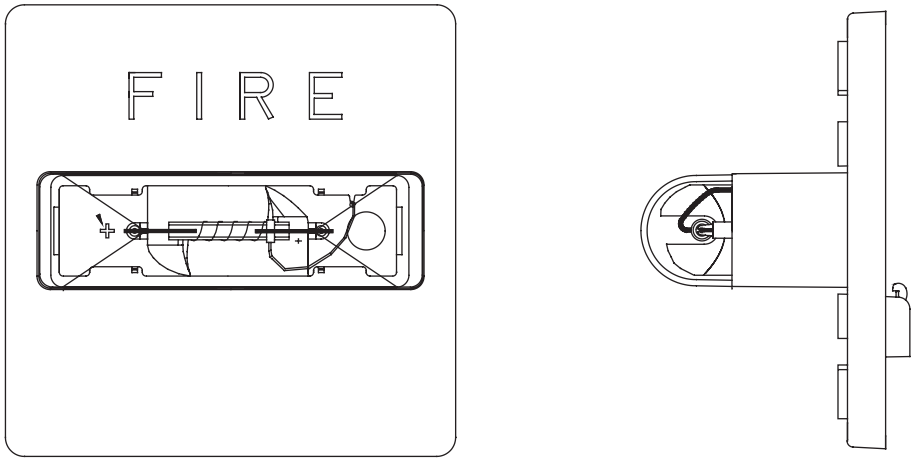
Strobes

Fire alarm strobe appliances are the preferred devices for achieving fire alarm signaling to individuals with hearing disabilities. Strobe appliances emit visible light pulses to alert occupants to a fire alarm event (see Figure 7.24). Strobe appliances are rated at different output levels, depending on the intended area of coverage. Strobe output is measured in candelas, a measure of luminous intensity.

Strobes flash at a preset frequency, or flash rate of 1–2 hertz (Hz) as required by the ADA, synchronized where two or more are within LoS. They are required to achieve this flash rate when operating anywhere in their listed voltage range. Like horn and chime units, strobes generally operate on 24 Vdc input power. For this reason, strobes can be easily integrated into chime, horn, and even speaker units.

An optional amber mass notification strobe can be incorporated such that a single notification device can serve two purposes.

Figure 7.24
Typical fire alarm strobe



Factors Affecting Performance

To fulfill the goals of protection of life and property, it is absolutely essential that notification appliances function as intended. The most comprehensive and extensive systems will be rendered useless if the alarm signal is not clearly perceived and understood by the occupants of the protected premises. In recognition of this fact, code writing authorities are giving increased attention to factors that affect system performance and effectiveness.

Audibility

Perhaps the most important aspect of fire alarm signaling is audibility. Hearing is still the most common mode of alarm perception. However, effective audibility can be compromised in many ways, such as the following:

- Alarm level—If output levels are not sufficient, occupants will be unaware of alarm events.
- Alarm clarity—If alarm tones and patterns are not clearly recognizable, occupants may misinterpret the nature of the alarm.
- Alarm reliability—Excessive false alarms can create mistrust and doubt, which can lead to the ignoring of alarm events.

Codes and standards contain extensive rules and guidelines to address these issues. To ensure general audibility, *NFPA 72* requires that public mode signaling achieve output levels of 15 dB over ambient decibel adjusted for frequency (dBA) levels or 5 dB over the maximum dBA level having duration of at least 60 seconds in all areas of protected premises.

Table 7.2 summarizes some typical average ambient sound levels by occupancy type. The values in the table are presented as a reference guideline only. In all cases, systems must be designed based on actual measurements of ambient conditions.

 © 2012 BICSI®

Factors Affecting Performance, continued

Table 7.2
Typical ambient sound levels by location

Location	Average Ambient Sound Level (dBA)
Business occupancies	55
Educational occupancies	45
Industrial occupancies	80
Institutional occupancies	50
Mechanical rooms	85
Mercantile occupancies	40
Piers and water-surrounded structures	40
Places of assembly	55
Residential occupancies	35
Storage occupancies	30
Thoroughfares, high-density urban	70
Thoroughfares, medium-density urban	55
Thoroughfares, rural and suburban	40
Tower occupancies	35
Underground structures and windowless buildings	40
Vehicles and vessels	50

dBA = Decibel adjusted for frequency

To achieve effective audible signaling in an area with an average ambient sound level of 65 dBA, the ESS designer must design the system to attain an alarm level of 80 dBA throughout the area. Manufacturer documentation will list the rated output for the notification appliance, usually measured at 3 m (10 ft) from the appliance.

A best practice is that the rated output will be decreased by 6 dB each time the distance from the device is doubled. Therefore, if the most remote location in a protected area is 12 m (39 ft) from an appliance that is rated for 92 dBA at 3 m (10 ft), the sound level at the remote area will be:

92 dBA – 6 dB {distance doubled from 3 to 6 m (10 to 20 ft)} – 6 dB {distance doubled from 6 to 12 m (20 to 39 ft)} = 80 dBA

In general, the preceding example is an effective design method. However, the calculation can be impacted by environmental elements (e.g., barriers, acoustical treatments). To account for such elements, the ESS designer should follow up with field testing to verify the effectiveness of the design.

Factors Affecting Performance, continued

Alarm clarity is also addressed in *NFPA 72*, which requires that audible alarms used for evacuation comply with ANSI S3.41, *Audible Emergency Evacuation Signal*. This standard establishes a pattern for evacuation signals called Temporal Code-3, which is characterized by an "on" phase lasting 0.5 s +/– 10 percent, followed by an "off" phase lasting 0.5 s +/– 10 percent, for three successive "on" periods, which is then followed by an "off" phase lasting 1.5 s +/– 10 percent.

If there are multiple notification appliances in a given area, they must be synchronized to avoid overlapping, which would obscure the temporal pattern. Temporal Code-3 was devised in an effort to make fire alarm evacuation signals universally recognized and understood.

Intelligibility

With the growing support and preference for voice evacuation systems, audibility is no longer the sole consideration for system performance. Where voice messages are concerned, it is not at all uncommon for messages to be audible, but not intelligible. Crowded subway stations, large auditoriums, and houses of worship are all examples of areas that may have sufficient audible output but poor intelligibility.

Fire codes and standards require that audible messages be intelligible but do not expressly define required levels of intelligibility. Annex D of *NFPA 72* addresses this concept by referencing the following standards:

- IEC 60268-16, *Sound System Equipment—Part 16; Objective Rating of Speech Intelligibility by Speech Transmission Index*
- ISO 7240-19, *Fire Detection and Alarm Systems—Part 19; Design, Installation, Commissioning and Service of Sound Systems for Emergency Purposes*
- NEMA SB 50, *Emergency Communications Audio Intelligibility Applications Guide*

Annex D utilizes the Speech Transmission Index (STI) method for measuring speech intelligibility as defined in IEC-60268-16.

Visibility

Audibility and intelligibility are worthy design goals, but they alone do not comprise an effective notification or signaling system. Since the advent of the ADA and the concept of equivalent facilitation, it has become equally important for systems to be visible as it is for systems to be audible.

Just as audibility can be compromised by environmental factors, visibility can be impacted by factors such as the:

- Area of coverage.
- Mounting location.
- Ceiling height.

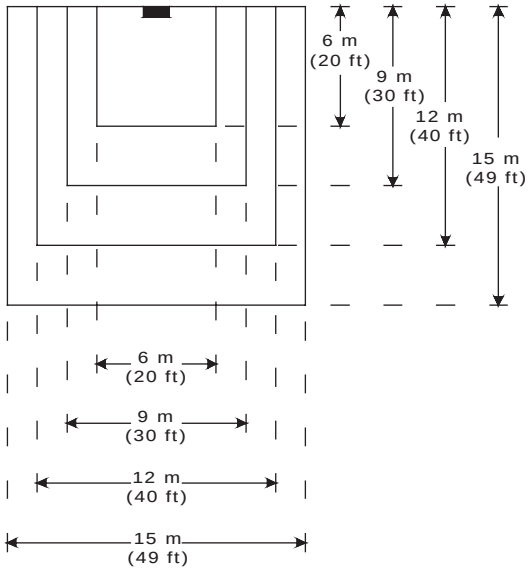
Fortunately for the system designer, codes and standards have taken a prescriptive approach in describing visible requirements, which makes the design of visible notification appliances a straightforward procedure.

 © 2012 BICSI®

Factors Affecting Performance, continued

A visible notification appliance is considered by the codes to project its luminance outward evenly in all directions. Therefore, a wall- or ceiling-mounted appliance will have a coverage pattern that extends an equal distance on either side of the device. Figure 7.25 illustrates this concept. Tables 7.3 and 7.4 can be used to determine the number of devices and candela ratings for a given space.

Figure 7.25
Typical visible notification appliance coverage pattern



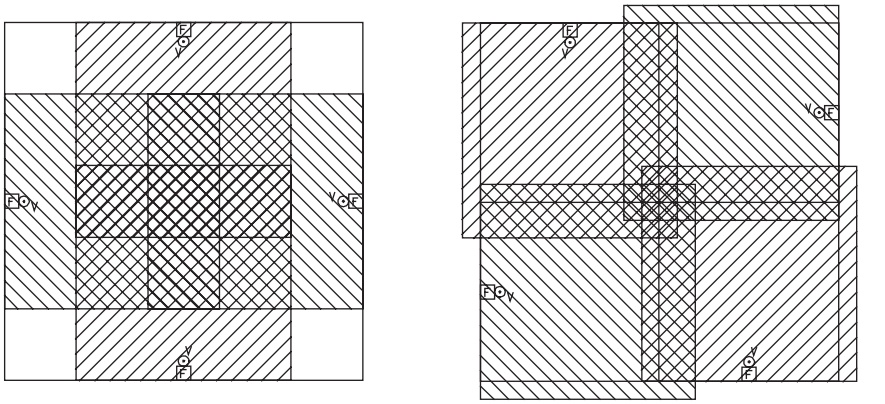
ft = Foot
m = Meter

The coverage pattern distances left and right of the appliance should be the same front to back from the appliance.

Factors Affecting Performance, continued

It follows from the preceding figure that if multiple appliances are used in a single room or area, they may need to be offset to attain proper coverage. This is illustrated in Figure 7.26.

Figure 7.26
Visible notification appliance placement



15 m (49 ft) x 15 m (49 ft) room
30 candela strobes
Unacceptable placement

15 m (49 ft) x 15 m (49 ft) room
30 candela strobes
Acceptable placement

ft = Foot
m = Meter

 © 2012 BICSI®

Factors Affecting Performance, continued

Finally, actual coverage areas based on intensity are defined in *NFPA 72* and summarized in Tables 7.3 and 7.4. The requirements take into consideration the potential use of multiple devices per area as well as ceiling height.

Table 7.3
Room spacing for wall-mounted visible appliances

Maximum Room Size		Minimum Required Light Output (Effective Intensity [cd])		
ft	m	One light per room	Two lights per room (located on opposite walls)	Four lights per room (one light per wall)
20 × 20	6.10 × 6.10	15	NA	NA
28 × 28	8.53 × 8.53	30	Unknown	NA
30 × 30	9.14 × 9.14	34	15	NA
40 × 40	12.2 × 12.2	60	30	15
45 × 45	13.7 × 13.7	75	Unknown	19
50 × 50	15.2 × 15.2	94	60	30
54 × 54	16.5 × 16.5	110	Unknown	30
55 × 55	16.8 × 16.8	115	Unknown	28
60 × 60	18.3 × 18.3	135	95	30
63 × 63	19.2 × 19.2	150	Unknown	37
68 × 68	20.7 × 20.7	177	Unknown	43
70 × 70	21.3 × 21.3	184	95	60
80 × 80	24.4 × 24.4	240	135	60
90 × 90	27.4 × 27.4	304	185	95
100 × 100	30.5 × 30.5	375	240	95
110 × 110	33.5 × 33.5	455	240	135
120 × 120	36.6 × 36.6	540	305	135
130 × 130	39.6 × 39.6	635	375	185

cd = Candela
ft = Foot
m = Meter
NA = Not allowable

Factors Affecting Performance, continued

Table 7.4
Room spacing for ceiling-mounted visible appliances

Maximum Room Size		Maximum Lens Height		Minimum Required Light Output (Effective Intensity); One Light (cd)
ft	m	ft	m	
20 × 20	6.1 × 6.1	10	3.0	15
30 × 30	9.1 × 9.1	10	3.0	30
40 × 40	12.2 × 12.2	10	3.0	60
44 × 44	13.4 × 13.4	10	3.0	75
50 × 50	15.2 × 15.2	10	3.0	95
53 × 53	16.2 × 16.2	10	3.0	110
55 × 55	16.8 × 16.8	10	3.0	115
59 × 59	18.0 × 18.0	10	3.0	135
63 × 63	19.2 × 19.2	10	3.0	150
68 × 68	20.7 × 20.7	10	3.0	177
70 × 70	21.3 × 21.3	10	3.0	185
20 × 20	6.1 × 6.1	20	6.1	30
30 × 30	9.1 × 9.1	20	6.1	45
44 × 44	13.4 × 13.4	20	6.1	75
46 × 46	14.0 × 14.0	20	6.1	80
50 × 50	15.2 × 15.2	20	6.1	95
53 × 53	16.2 × 16.2	20	6.1	110
55 × 55	16.8 × 16.8	20	6.1	115
59 × 59	18.0 × 18.0	20	6.1	135
63 × 63	19.2 × 19.2	20	6.1	150
68 × 68	20.7 × 20.7	20	6.1	177
70 × 70	21.3 × 21.3	20	6.1	185
20 × 20	6.1 × 6.1	30	9.1	55
30 × 30	9.1 × 9.1	30	9.1	75
50 × 50	15.2 × 15.2	30	9.1	95
53 × 53	16.2 × 16.2	30	9.1	110

 © 2012 BICSI®

Factors Affecting Performance, continued

Table 7.4, continued
Room spacing for ceiling-mounted visible appliances

Maximum Room Size		Maximum Lens Height		Minimum Required Light Output (Effective Intensity); One Light (cd)
ft	m	ft	m	
55 × 55	16.8 × 16.8	30	9.1	115
59 × 59	18.0 × 18.0	30	9.1	135
63 × 63	19.2 × 19.2	30	9.1	150
68 × 68	20.7 × 20.7	30	9.1	177
70 × 70	21.3 × 21.3	30	9.1	185

cd = Candela
ft = Foot
m = Meter

As with audible Temporal Code-3, effective visible signaling requires that multiple appliances in a given area be synchronized to avoid confusion as well as to protect against the possibility of seizures in persons affected by photosensitive epilepsy. When visible notification appliances are correctly sized and properly synchronized, they are readily apparent, even in the complete absence of audible signaling.

Circuits and Pathways

NFPA 72 defines circuit and pathway requirements based on performance and survivability characteristics. These designations apply to circuits and pathways (e.g., signaling line circuits [SLCs], initiating device circuits [IDCs], notification appliance circuits [NACs], auxiliary and power circuits) utilized in fire alarm systems.

Circuit and pathway performance characteristics are defined by class designations in *NFPA 72* as follows:

- Class A
  - Includes a redundant path
  - Operational capability continues past a single open
  - Conditions that affect the intended operation of the path are annunciated
- Class B
  - Does not include a redundant path
  - Operational capability stops at a single open
  - Conditions that affect the intended operation of the path are annunciated
- Class C
  - Includes one or more pathways where operational capability is verified via end-to-end communication, but the integrity of individual paths is not monitored
  - A loss of end-to-end communication is annunciated
- Class D
  - Has fail-safe operation, where no fault is annunciated, but the intended operation is performed in the event of a pathway failure
- Class E
  - No monitoring for integrity
- Class X
  - Includes a redundant path
  - Operational capability continues past a single open or short-circuit
  - Conditions that affect the intended operation of the path are annunciated

 © 2012 BICSI®

Circuits and Pathways, continued

Circuit and pathway survivability characteristics are defined by level designations in *NFPA 72* as follows:

- Level 0
  - Not required to have any provisions for pathway survivability
- Level 1
  - Shall consist of pathways in buildings that are fully protected by an automatic sprinkler system in accordance with *NFPA 13, Standard for the Installation of Sprinkler Systems,* with any interconnecting conductors, cables, or other physical pathways installed in metal raceways
- Level 2
  - Shall consist of one or more of the following:
    - 2-hour fire-rated circuit integrity (CI) cable
    - 2-hour fire-rated cable system (electrical circuit protective system)
    - 2-hour fire-rated enclosure or protected area
    - 2-hour performance alternatives approved by the AHJ
- Level 3
  - Shall consist of pathways in building that are fully protected by an automatic sprinkler system in accordance with *NFPA 13* and one or more of the following:
    - 2-hour fire-rated CI cable
    - 2-hour fire-rated cable system (electrical circuit protective system)
    - 2-hour fire-rated enclosure or protected area
    - 2-hour performance alternatives approved by the AHJ

Control Units

Overview

In commercial, educational, and institutional facilities, fire detection and alarm devices usually function as components of a system rather than as discrete devices. Fire detection and alarm control panels provide the central logic and control features necessary for a unified system of various types of devices capable of providing essential life safety functions.

Control units are capable of two-way communications. 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.

In addition to monitoring and controlling devices specific to the fire detection system, control units provide interfaces with auxiliary building components (e.g., environmental air handling equipment, smoke dampers, elevators, fire-rated doors) whose proper operation is essential to the integrity of a building's life safety system. Fire detection and alarm systems can be configured with a single, central control unit or with distributed control units as the size of the facility dictates.

Central Control Panels

In single-family residences, smoke detectors are often unitary, self-contained devices. Fire alarm devices are part of a larger fire detection system in:

- Commercial facilities.
- Educational facilities.
- Institutional facilities.
- Some large residential complexes.

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

FACPs 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.

 © 2012 BICSI®

Central Control Panels, continued

The connection between detection (initiation) and alarm (notification) devices and the central control panel is usually provided by wired circuits. Multiple devices can be connected to a common set of wires, creating a zone. Alternatively, devices can be addressed individually and connected to a common data bus to allow them to communicate with the central control panel through multiplexed data streams.

FACPs typically support at least four types of circuits:

- Alarm-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 provide circuit paths between any combination of addressable appliances or devices, circuit interfaces, control units, or transmitters over which multiple input or output signals are carried.
- Auxiliary monitoring and control circuits—These circuits connect remote input and output devices to the central control panel. These circuits are used for remote monitoring and control of auxiliary building equipment.

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 detection and alarm network (e.g., serial bus [SBUS] or IP/Ethernet).

Zoned Systems

Traditional FACPs are designed to accommodate a zone wiring scheme. In a zoned system, fire alarm devices in a common area of a facility are connected to the same alarm-initiating circuit. Each zone requires its own circuit conductors. This arrangement allows alarm annunciation to be reported by areas of a building to readily identify the location of the alarm-initiating device. Zoned fire alarm systems are often used in small facilities where a few zones can provide sufficient alarm annunciation.

Addressable Systems

With the advent of microprocessors and digital electronics, addressable FACPs and devices have become more common than zoned systems for medium and large facilities.

Addressable fire alarm systems use digital encoding and multiplex technology to more accurately identify alarm locations and device conditions. Each fire alarm device in a system is programmed with a unique address.

The FACP is capable of communicating with a single address or a group of addresses, depending on the functions required. The communication is often multiplexed over a common cable, which is sometimes referred to as a data bus. This arrangement significantly reduces the amount of cabling necessary to install the system. The communication channel allows two-way communication, thus enabling the FACP to control as well as monitor fire alarm devices.

A significant component of addressable fire alarm systems is the software programming necessary to make a system function correctly. System manufacturers include basic functional programming in all central control panels. Additional field programming usually is required to tailor a system's operation to a specific facility. Fire alarm system programming can represent a substantial portion of the installation effort, especially in facilities that require numerous interfaces with auxiliary building elements. Some operations of the central control panel are not field programmable because their responses are dictated by life safety codes. Therefore, manufacturers do not allow users to modify these essential functions.

The communication technologies employed in addressable systems allow for advanced features (e.g., self-adjusting smoke detectors) to accommodate sensitivity changes because of age and accumulation of dust prior to maintenance. These features are not available with zoned systems.

 © 2012 BICSI®

Supervision

Fire alarm system circuits are required to be continuously monitored (supervised) to ensure a system's integrity. This requirement 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. This trouble report is indicated at the central control panel, remote annunciation panels, and remote monitoring equipment.

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 alarm systems are often required to monitor or control auxiliary building components that are not part of the fire alarm 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.

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 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 not supervised.

These unsupervised circuits have the potential to be a weak link in the overall system of supervision. For this reason, fire alarm codes often dictate the physical length of the unsupervised circuit between a monitoring and control module and the equipment with which it interfaces. This distance limitation ensures that monitoring and control devices are located close to the associated building equipment.

Trouble Conditions

Overview

With addressable systems, the entire fire alarm system's individual components can be monitored for their state of readiness. The computer in the fire alarm system's control panel evaluates the information. If a problem is detected, a trouble signal is sent to the annunciation component of the system.

Trouble signals do not always merit the same response from personnel monitoring the system for a fire indication. For example, some signals may indicate a component's required maintenance and others its failure to continue to perform its function. In this case, personnel will acknowledge these trouble signals and direct technical response to check the component and make corrections or adjustments as necessary.

Supervisory Trouble Signal

The trouble alarm signal is distinctive in sound from the fire alarm signals and may be common to all supervised trouble circuits in a single system.

A trouble signal silence switch is permitted, providing its operation transfers the trouble indication to a visual indication (e.g., lamp or LED that remains lit until the trouble condition of the device is corrected). To avoid an inadvertent silence condition of all the fire alarm system's components' future trouble, the trouble signal silence switch is programmed so that the trouble signal will sound if the silence switch is in the silence position and no trouble is detected in the system.

Trouble signal indicators are found in each FACP or mounted adjacent to the panel. If the control panel is located in an area not regularly frequented by building personnel, additional trouble signals are installed in areas where they will be readily attended by personnel monitoring the building for a problem.

A single failure (break) in the wiring or an electrical ground fault (another type of electrical failure) in any of the supervised initiating (detecting) circuits will not cause the notification appliances to operate. Interruption or restoration of the main or secondary source of power to the FACP will not activate signals. Trouble signals will operate only on any standard alarm conditions identified within the system.

With intelligent systems, the fire alarm system can be monitored for inconsistencies in device status and unresponsive devices. The information is evaluated by the system, and a trouble signal is sent to the annunciation component of the system. Trouble signals do not always merit the same response from personnel monitoring the system. Personnel will acknowledge the system trouble and direct technical response to check the component and make corrections or adjustments as necessary.

 © 2012 BICSI®

Power Supplies

Two independent reliable sources of power are required for each central control panel. Each power supply must be capable of:

- Supplying the full load current required by the control panel.
- Monitoring initiation devices and associated signaling devices (notification appliances).

The condition of each power supply also is monitored by the central control panel.

The normal power supply is generally supplied by dedicated 120 V alternating current (ac) circuits. The circuit breaker serving the control panels should be clearly labeled. It is recommended that this circuit breaker be provided with a "lockable on" feature to prevent inadvertent switching.

A standby power supply is required in the event the normal power supply is interrupted. The standby power supply can be either of the following:

- Dedicated storage battery, which is usually a built-in component of the central control panel
- Dedicated circuit served by an engine generator and automatic transfer switch that transfers control to the emergency source upon sensing loss of power within a certain short time period

It is common practice to utilize both an emergency generator circuit and built-in batteries when emergency generator power is available. The standby power supply, if batteries alone, must be capable of powering the control unit for 24 hours in a normal state followed by a 15-minute period at full load with the unit in an alarm condition.

If an emergency engine generator circuit is utilized as the standby power supply, the dedicated storage batteries must be sized for 4 hours of normal operation in case the generator fails to start. Battery sizing calculations are done by the engineer designing the fire alarm system to verify that the system components total electrical load will operate reliably using the batteries for the predetermined period of time.

Booster power supplies are often required in cases where the main system power supply is not sufficient to power all devices, particularly for systems with large quantities of NAC circuits and devices and/or because of circuit lengths. Booster power supplies can be located at the main control panel or remotely within the building and are subject to the same requirements as the main power supply.

System Inputs and Outputs

When the fire alarm system is required to provide control functions, system modules with the appropriate outputs are provided. Fire alarm control modules usually do not supply (source) the control voltage; therefore, equipment being controlled must provide a control circuit voltage.

Control modules typically provide "dry" contact outputs that can be interconnected with equipment control circuits to provide start/stop, open/close, and similar control functions. Outputs, such as pager notification, also can be initiated to alert maintenance personnel to an alarm or trouble condition.

System Inputs and Outputs, continued

When monitoring functions are required, modules with terminals to receive the appropriate normally open or normally closed dry contact inputs are provided. Fire alarm monitoring modules usually source the control voltage; therefore, the devices being monitored must provide dry contacts.

Fire alarm monitoring and control modules are permitted or required to interface with other building systems to provide auxiliary functions. The nonfire alarm equipment or devices should not interfere with the operation of the fire alarm system.

Some examples of the fire alarm system interfaces are:

- Security and door access control systems.
- Fire sprinkling systems.
- Building automation systems.
- Heating and ventilating systems.
- Elevator systems.
- Fire-rated doors.

Auxiliary fire detection and alarm functions are discussed further in the following section on remote monitoring and control modules.

Remote Monitoring and Control Modules

A building's fire alarm system is required to interface with many systems and devices external to the fire alarm system. This is necessary to provide a unified life safety system. Monitoring and control modules provide this interface.

Fire alarm system control modules are used to interface with fire suppression systems, elevators, HVAC systems, and security systems. When modules are required to provide a monitoring function, they usually interface with the building system device they are monitoring through a digital (on/off) output from the building system device. This output is often a dry contact that opens or closes as an indication of some abnormal event.

The control module converts this output from the building's device into a fire alarm system input. An example of a common monitoring function is the interface between a building's fire alarm system and the readiness of its fire sprinkler system.

As discussed in the previous section, tamper switches are installed on shutoff valves in sprinkler piping at the location in which the piping enters the building. If a valve is operated, a contact in the tamper switch closes and provides a digital input to the fire alarm system control module associated with the tamper switch. The fire alarm system is programmed to indicate this condition at the control panel and its related annunciators, if installed. In this way, the control module monitors the position of the fire sprinkler valves and alerts the appropriate personnel if the valves are not in the fully open position.

In a similar fashion, control modules can control other building components. An example of a common control function is the closing of doors in fire-rated walls and the recalling of elevators to a designated level of the building upon the initiation of a fire event.

 © 2012 BICSI®

Remote Monitoring and Control Modules, continued

Smoke detectors in specific locations initiate a signal to the central control panel. The central control panel then signals the control modules that interface with the components' control circuit (door closers' control unit or elevator control panel). These control units are external to the fire alarm system and actuate to close doors and return elevators to a designated floor.

Modern fire alarm system control and monitoring modules are available as addressable devices for use in addressable systems. This feature provides each module with a unique system address and allows central control panel programming to include specific instructions for each module.

In a zoned system, fire alarm monitoring and control functions are provided by dedicated relays located in the central control panel or in remote control panels. Operational logic is hardwired into the system rather than programmed through software. While manufacturers still provide hardwired monitoring and control devices, addressable devices are becoming more common because of the flexibility provided through software programming and lower prices of components as more market penetration is being realized.

Remote Control (Annunciator) Panels

When large fire alarm control systems are installed, it often becomes necessary to install remote control panels. These panels are connected to the central control panel and can include some or all of the features contained in the central control panel.

Remote control panels can include functional logic as does the central control panel, or they can simply be slave units to the central panel.

Remote panels also can be installed to provide alarm, supervisory, and trouble indications at locations within the facility to alert personnel responsible for the system operation and maintenance such as facility personnel. Remote panels containing only these features are often referred to as remote annunciators.

Fire department personnel responding to alarm conditions can use remote annunciators to quickly identify the alarm location within the facility. Remote annunciators are usually required to be installed at locations where emergency personnel enter when responding to a fire alarm if the central control panel is not installed at this location.

The annunciator panel is connected to the main FACP and performs several functions. The annunciator panel:

- Announces (through visual and audible indications) that the alarm condition has been activated.
- Enables responding personnel to identify the location of an activated alarm quickly and accurately.
- Indicates the status of emergency equipment or fire safety functions that might affect the safety of building occupants in a fire event.

Remote Monitoring and Control Modules, continued

These systems are required to mirror several functions of the main FACP, including both audible and visual notification.

Graphical Displays

Graphical displays are a little more sophisticated. These displays are placed on either a silk-screened plan of the building or a computer type of monitor. This aids in determining the exact location of trouble or alarm conditions within the building.

The silk-screened plan is generally an architecturally scaled version of the protected areas or zones with indicators showing the location of the various sensors. When an alarm activates, the operator can quickly determine the area affected by the alarm.

A monitor type of display is used to visually enhance the display of the alarm. This usually shows a graphic of the building plan and can display text messages as to the location and type of alarm. Enhanced versions are usually a touch screen type where the operator monitoring the building can simply touch the screen to acknowledge the alarm call or expand the view of the troubled area.

Signaling

Annunciators receive their signals from either the main control panel/console or a remote panel. These signals are transmitted via:

- Hardwired copper conductors, using the fire alarm protocol, usually proprietary in nature.
- The system network connection.
- Wireless connections.
- A combination of the above.

Zones

Zones of origin of the alarm condition initiation can be shown on either the standard display or the graphical display. Zones are typically set up in floor levels or specific areas. The display is arranged to indicate which floors or areas of a particular floor (zone) have the alarm or trouble condition.

An example of a supervisory condition would be when a valve tamper switch has been activated. An example of an alarm condition is when a water flow switch in the fire sprinkler system or in-duct smoke detector has been activated.

 © 2012 BICSI®

Digital Alarm Communicator System (DACS)

Overview

Digital alarm communicator system (DACS) units are used in:

- Central station service systems.
- Proprietary supervising station systems.
- Public emergency alarm reporting systems.

A DACS is required to connect protected premises with one or more of these supervised systems to a continuously attended supervising or monitoring station. This reports a message, identifying the change in condition at the protected premises.

Transmitters

Digital Alarm Communicator Transmitter (DACT) Dialers

A DACT has the ability to attain a telephone line dial tone, dial a preassigned number for the DACR, receive confirmation from the DACR that it can receive a signal, and transmit the signal to the DACR. The DACT also receives verification once the DACR has accepted the signal. The time required to obtain a dial tone and perform these operations may not exceed 90 seconds per attempt.

A DACT is programmed so that when a signal is transmitted to the DACR, it seizes the telephone line at the protected premises. It disconnects any outgoing or incoming telephone calls and prevents the use of the telephone line for any new outgoing telephone calls until signal transmission has been completed.

A DACT has the ability to reset and retry if the first attempt to complete a call to the DACR is unsuccessful. Failure to make connection with a DACR will not prevent subsequent attempts to transmit an alarm condition where the alarm is generated by any of the other initiating or signaling circuits.

A minimum of five and a maximum of 10 additional attempts should be made until the connection is made and the signal has been transmitted. If the maximum number of attempts to complete the transmission is reached, a failure notification is made at the FACP.

Transmission Means

The following requirements apply to all DACTs:

- A DACT is connected to two separate channels of transmission at the protected premises.
- A DACT is capable of selecting the means of transmission in the event of failure of the other means.
- The primary means of transmission is a telephone line connected to the public switched network and is the first transmission attempt utilized.
- Each DACT is programmed to call a second DACR line when the signal transmission sequence to the first called line is unsuccessful.

 © 2012 BICSI®

Digital Alarm Communicator Transmitter (DACT) Dialers, continued

Transmission Channels

A DACT employs one of the following combinations of transmission channels:

- Two telephone lines.
- One telephone line and one cellular telephone connection.
- One telephone line and one one-way radio system.
- One telephone line equipped with a derived local channel.
- One telephone line and a one-way private radio alarm system.
- One telephone line and a private microwave radio system.
- One telephone line and a two-way radio frequency multiplex system.
- A single integrated services digital network telephone line using a NRTL-listed terminal adapter specifically listed for supervising station fire alarm service. In this case, the path between the transmitter and the telephone network is monitored for integrity so that a failure in the path is annunciated at the supervising central station within 200 seconds.

The following requirements apply to all combinations of transmission channels listed above:

- Both channels are supervised.
- Both channels are tested at regular intervals not exceeding 24 hours.
  - For public cellular telephone service, a test signal is transmitted at least monthly.
  - If two telephone lines are used, it is permitted to test each telephone line at alternating 24-hour intervals.
- The failure of either transmission channel sends a trouble signal on the other channel within 4 minutes.
- When one transmission channel fails, all status change signals are sent over the other channel except when used in combination with a DACT. In this case, a derived local channel is not required to send status change signals other than those indicating that a failure exists on the telephone line.
- The primary channel is capable of delivering an indication to the DACT that the supervising station has received the message.
- The first attempt to send a status change signal uses the primary channel unless the primary channel is known to have failed.
- Simultaneous transmission over both channels is permitted.
- Failure of telephone lines or cellular service is annunciated locally.

Digital Alarm Communicator Transmitter (DACT) Dialers, continued

Long Distance

If long-distance telephone service is used, the second number must be through a different long-distance service provider if multiple providers are available.

This requirement for use of two different long-distance providers prevents a lost signal because of a fault in one long-distance provider's network. This requirement is not meant to apply in local situations where signal traffic is strictly within the area covered by one local telephone company.

Because it is never known if a subscriber has changed long-distance providers, it is recommended that, if direct dialer service is used, a telephone call is forced onto a specific long-distance provider's network using the dialing prefix carrier identification code (CIC) specific to each long-distance provider.

Call Forwarding

If a DACT is programmed to call a telephone line that is call forwarded to the line of the DACR, a means to verify the integrity of the call-forwarding feature every 4 hours must be provided.

Call forwarding should not be confused with wide area telephone service (WATS) or toll-free service. WATS or toll-free service is achieved by dialing a specific prefix and is a dedicated service used mainly for its toll-free feature. In call forwarding, all calls are preprogrammed to terminate at a fixed telephone line or to a dedicated line.

Protocol

The Ademco Group's contact identification protocol has become a prevalent and respected format for digital communications between alarm systems and central monitoring stations. Many manufacturers have adopted it, and it is seeking industry-wide compatibility.

The Security Industry Association (SIA) also acknowledges Ademco's contribution to communications in this area of the security industry. SIA publishes this protocol as a de facto security industry standard and accepts the industry's request for modifications to this protocol. The document title is SIA DC-05-1999.09, *Digital Communication Standard—Ademco® Contact ID Protocol—for Alarm System Communications*.

 © 2012 BICSI®

Digital Alarm Radio Transmitter (DART)

If any DACT signal transmission is unsuccessful, the information is transmitted by means of the digital alarm radio transmitter (DART).

The DART is capable of demonstrating a minimum 90-percent probability of successfully completing each transmission sequence. Transmission sequences are repeated a minimum of five times. The DART transmission can be terminated in less than five sequences if the DACT successfully communicates to the DACR.

Transmission Means

The following requirements apply to all DARTs:

- A DART transmits a digital code or another approved signal by use of radio transmission to its associated digital alarm radio receiver (DARR).
- Signal repetition, digital parity check, or another approved means of signal verification is used.
- The DART complies with applicable Federal Communications Commission (FCC) rules consistent with its operating frequency.

Testing

Each DART automatically initiates and completes a test signal transmission sequence to its associated DARR at least once every 24 hours.

Receivers

Digital Alarm Communicator Receiver (DACR)

Spare DACRs are available in the supervising station. The spare DACRs can be switched into the place of a failed DACR within 30 seconds after detection of failure. One spare DACR can serve as a backup for up to five DACRs in use.

The number of incoming telephone lines to a DACR is limited to eight lines. If the signal receiving, processing, display, and recording equipment at the supervising station is duplicated and a switchover can be accomplished in less than 30 seconds with no loss of signal during this period, the number of incoming lines to the unit is permitted to be unlimited.

Reception Requirements

The DACR at the supervising station is connected to a minimum of two separate incoming telephone lines. The lines have the following characteristics:

- The lines are used for no other purpose than receiving signals from a DACT.
- The lines are unlisted.
- The failure of any telephone line connected to a DACR because of loss of line voltage is annunciated visually and audibly in the supervising station.

Testing

A signal must be received on each individual incoming DACR line at least once every 24 hours. The failure to receive a test signal from the protected premises is treated as a trouble signal.

Digital Alarm Radio Receiver (DARR)

A spare DARR is available in the supervising station and can be switched into the place of a failed unit within 30 seconds after detection of failure.

Facilities are available at the supervising station for supervisory and control functions of subsidiary and repeater station radio receiving equipment. This is accomplished via a supervised circuit where the radio equipment is remotely located from the supervising station.

The following conditions are supervised:

- Failure of ac power supplying the radio equipment
- Malfunction of receiver
- Malfunction of antenna and interconnecting cable
- Indication of automatic switchover of the DARR
- Malfunction of data transmission line between the DARR and the supervising station

 © 2012 BICSI®

Internet Protocol (IP) Alarm Communicator System

Overview

IP alarm communicator system devices can be used in central station fire alarm systems.

An IP alarm communicator system is a two-way, always-on IP communication system, consisting of a transmitter (IP alarm communicator transmitter) and receiver (IP alarm communicator receiver). These devices are connected to an existing LAN or wide area network (WAN). As new technologies emerge that provide communications devices and methods to connect to supervising station fire alarm systems, governing bodies are setting criteria for these technologies.

Internet Protocol (IP) Alarm Communicator System Transmitter

An IP alarm communicator system transmitter uses a network connection as a means of high-speed, supervised communication to the central station. The IP alarm communicator transmitter is programmed to report to two different IP addresses. The IP addresses are programmed such that if one of the IP addresses fails, the other address is a backup. These IP addresses are static or always on. These devices typically support dynamic host configuration protocol (DHCP [dynamic IP addresses]). IP alarm communicators also support data encryption to safeguard against unauthorized interception (e.g., hacking).

An IP alarm communicator transmitter uses minimum bandwidth on a network, allowing data transfer to be fast and accurate. IP alarm communicator transmitters can be installed adjacent to existing fire alarm panels and configured to monitor the existing alarm and trouble contacts, typically monitored by a digital dialer. IP alarm communicator transmitters also can monitor Ademco's contact identification.

An IP alarm communicator transmitter:

- Typically contains four on board zones (inputs) and can be expanded to as many as 12 zones.
- Has software that can be locally or remotely uploaded and downloaded.
- Typically contains two outputs.
- Is listed for commercial applications.

The main difference between a DACT and an IP alarm communicator transmitter is that a DACT requires a secondary means of communication, usually in the form of a telephone line.

With the implementation on voice over Internet protocol (VoIP) telephone systems in an environment where the existing communication method was a local dialer, the basis of the VoIP does not allow the dialer to "seize" the telephone line as needed to dial the central station on a consistent basis. This makes the existing dialer noncompliant with the codes that require the ability to consistently seize the telephone line.

Internet Protocol (IP) Alarm Communicator System Receiver

An IP alarm communicator system receiver uses a network connection as a means of high-speed, supervised communication to the central station. The IP alarm communicator receiver is programmed to receive information from two different IP addresses of the IP alarm communicator transmitter. The IP alarm communicator transmitter allows for time stamps to all data received prior to transmitting the data via transmission control protocol/Internet protocol (TCP/IP), universal serial bus (USB), or via a serial port. The IP alarm communicator receiver can provide data to an existing alarm monitoring software; however, compatibility needs to be determined by the system manufacturers.

The IP alarm communicator receiver is often located in the central station of a campus. Applicable codes require a secondary or back-up receiving device. These devices can be rack mounted in the central station along with other fire alarm monitoring equipment.

The IP addresses are programmed such that if one of the IP addresses fails, the other address is a backup. These IP addresses are static or always on. These devices typically support DHCP (dynamic IP addresses) and support data encryption to safeguard against unauthorized interception (e.g., hacking).

Internet Protocol (IP)-Based Solution

The IP alarm communicator system networked alarm signals can be transmitted over an existing network relatively inexpensively by adding a data drop adjacent to or into an existing fire alarm panel and installing an IP alarm communicator transmitter. Configuration of these systems requires the assignment of IP addresses and configuration of the central station receiver and monitoring software.

IP alarm communicator system signals can be received and processed at remote locations via the Internet. Signals can also be monitored at remote locations if the primary central station becomes disabled.

IP alarm communicator system devices offer a higher level of security. Their devices can be polled more often than the applicable codes require, thus providing a more timely response to alarm or trouble signals.

Some of the disadvantages are that the IP communicators need to be manufactured by the same vendor to form a properly matched pair, and the IP alarm communicator system needs to be approved by the local AHJ.

Even though the IP alarm communicator system meets the appropriate and applicable codes, the local AHJ does not always agree. Care must be used in the selection and application of these systems. It is the integrator's responsibility for the system design as well as coordination and education of these emerging technologies with the end user and the AHJ.

 © 2012 BICSI®



Chapter 8
Notification, Communication, and Display Devices

Notification and display devices provide a means of communicating through the use of audio or display devices or a combination of both. Chapter 8 discusses audio communication, emergency telephones, public address (PA) systems, and display devices.

Table of Contents

Notification, Communication, and Display Devices 8-1
Introduction 8-1
Audio Communication Systems 8-1
Voice Communication Systems 8-3
Intercom 8-3
Principles of Operation 8-4
Hardwired Systems 8-4
Wireless Systems 8-4
Internet Protocol (IP)-Based Systems 8-4
Emergency Telephones 8-5
Emergency Communication Telephones 8-5
Public Address (PA) Systems 8-6
Overview 8-6
Types of Paging Systems 8-7
Internet Protocol (IP) Addressable Speakers 8-7
Centrally Amplified Systems 8-7
Distributed Amplified Systems 8-8
Components 8-8
Audio Input Circuits 8-9
Audio Output Circuits 8-9
Audibility 8-9
Intelligibility 8-10
Voice Telephone Systems for Notification 8-10
Centralized Calling 8-10
Noise Masking 8-10
Sound Reinforcement 8-10
Video Display Devices 8-11
Analog versus Digital Inputs for Display Devices 8-11

Tables

Table 8.1 Audio signal distance limitations 8-8

 © 2012 BICSI®

Notification, Communication, and Display Devices

Introduction

Notification and display devices provide a means of communicating messages through the use of audio or display devices or a combination of both. Notification devices provide audio communication in one or both directions, whereas display devices communicate messages by displaying them on a video screen or other visual devices, such as lights, strobes, and visual display boards. Regulatory requirements, such as those in the Americans with Disabilities Act (ADA), must be taken into consideration when designing notification systems.

Audio Communication Systems

Two primary functions for audio communication systems as they relate to electronic safety and security (ESS) are:

- Life safety.
- Public address (PA).

NOTE: PA announcement systems do not have as high a degree of reliability as life safety announcement systems. PA systems generally are not supervised and therefore should not be relied upon as the primary life safety announcement system.

The purpose of life safety systems is to provide supervised notification of a potential life safety concern. In many systems, loudspeakers or horns may be addressed individually, in logical groups (e.g., zones), or all at once. A life safety system may be accessed through:

- A telephone system via an interactive voice response or a live operator.
- The Internet.
- A dedicated console or microphone.

Life safety systems may also include prerecorded messages.

The system may be used to provide instruction to building occupants on where to seek places of safety and shelter in the event of an emergency (e.g., tornado, chemical spill). The design and installation of a life safety system must conform to the local authority having jurisdiction (AHJ), including compliance with standards (e.g., UL 2572).

A PA system allows the ability to broadcast voice messages or audio programming across a network of loudspeakers. This type of system may have the capability to provide background music, time tones, night ringing, alerting tones, and one-way and talk-back paging to any zone in the system. In addition to notifying authorities of an incident, the ESS designer can use an audio communication system to provide a means of delivering time-sensitive instructions or messages during an emergency situation.

Audio Communication Systems, continued

The audio communication system must be carefully integrated with other systems (e.g., fire alarm) to not deliver mixed or conflicting messages.

Adding audio communication to an ESS system can improve safety for those at risk by reducing that risk and liability and shortening recovery time. In addition, emergency responders can make better decisions by using lists of who has been contacted and having a means of providing additional information.

The following systems can be integrated with other communication systems to deliver a consistent message:

- PA systems
- Sound reinforcement
- Cellular telephones
- Text messaging
- Pagers
- Personal digital assistant
- E-mail
- Instant messaging
- Digital signage
- Notification and visual display devices
- Telephone systems
- Video projectors
- Community antenna TV messages
- Radio systems
- Speaker strobes
- Radio and TV broadcasts
- Website

 © 2012 BICSI®

Voice Communication Systems

Intercom

An intercom is an electronic communication system intended for limited or private dialogue. Intercoms can incorporate connections to landlines, cellular telephones, and other intercom systems over telephone or data lines or door release devices. Permanent intercoms installed in buildings generally are composed of fixed microphone and speaker units that connect to a central control panel. An intercom can connect a few rooms or many rooms (e.g., schools, hospitals) and may even be connected to a central office (CO) service.

Many facilities now use audio and video intercoms to identify visitors who seek access at locked building entrances. Intercom systems may be integrated with the building's access control system.

The primary components of an intercom system are the:

- Master station.
- Remote station.

The master station receives calls from the remote stations. The master station is typically staffed with an operator.

Remote station configurations may include the following:

- Substation—Unit that is capable of only initiating a call to a master station but is not capable of initiating a call to other stations (sometimes called slave units).
- Door station—Unit that is capable of only initiating a call to a master station. It is typically weatherproof.
- Intercom station—Full-featured remote unit that is capable of initiating and receiving party line conversation, individual conversation, and signaling.
- Wall mount station—Fixed-position intercom station with a built-in loudspeaker. May have a flush-mounted microphone, handheld push-to-talk microphone, or telephone-style handset.
- Portable—Mobile intercom, sometimes called a belt pack.
- Handset—Permanent or portable telephone-style connection to an intercom station. Holds both an earpiece and a push-to-talk microphone.
- Headset—Portable intercom connections from a belt pack to one or both ears via headphones with an integrated microphone on a boom arm.

Principles of Operation

Hardwired Systems

The components in most intercom systems are not interchangeable or compatible with each other across different manufacturers' systems. Analog intercom systems have several common system components. Voice signals are carried embedded in a direct current (dc) power bus of 12 to 48 volts dc (Vdc).

Signaling between stations can be through the use of separate conductors or carried in the main voice pair via tone frequencies. Multiple channels of simultaneous conversations can be carried in a cable by frequency division multiplexing (FDM) or time division multiplexing (TDM) or through additional pairs in the same cable. Hardwired systems can include packetized network transmission solutions.

Wireless Systems

The choice of product and system design will bear heavily on the performance and security of a wireless system. Additionally, conflicting carrier frequencies and signal power from other wireless devices (e.g., digital enhanced cordless telecommunications [DECT] cordless telephones, wireless data networks, remote audio speakers) can cause interference and signal loss.

To mitigate concerns over privacy, the use of encrypted wireless intercoms can reduce this risk. Placement, installation, construction, grounding (earthing), and shielding methods can reduce some of the effects of external interference.

The ESS designer should review frequencies utilized by wireless devices, the existing radio frequencies being utilized at the location, and frequency assignments to the system operator (licensee) to avoid system interference. The system operator's (licensee) frequency coordinator shall be consulted during the design phase to assist in determining proper frequency assignments.

Systems that utilize the building power wiring system with power-line carrier (PLC) as their wiring are sometimes referred to as wireless intercoms.

Internet Protocol (IP)-Based Systems

Unlike an analog intercom system, an Internet protocol (IP) intercom system employs packet audio technology that is transmitted over an IP network. An IP intercom system typically consists of audio exchanges, IP network audio adapters, IP amplifiers, IP active loudspeakers, IP paging stations, and various interfacing units that allow integration with LANs, wide area networks, or optical fiber networks. The system can be designed to allow duplex conversation between stations, paging broadcasts, timely broadcasts, background music broadcasts, and video transmission between stations.

Unlike a traditional analog intercom system that is typically point-to-point in its design and functions, an IP intercom system can be used to transmit audio and video signals over a wide geographical area. An IP intercom system can be more flexible in both deployment and operation as its means of distribution is via the network and requires far less infrastructure than a similar analog system.

 © 2012 BICSI®

Emergency Telephones

Emergency Communication Telephones

Emergency communication telephones provide a quick and dedicated way to notify authorities of an emergency. Emergency telephones are often purpose-built devices dedicated to that single function.

Emergency communication telephones can be located on the interior or exterior of a building. They also can be mounted on freestanding towers.

Optional components include:

- A strobe light at the telephone to identify the location of the call.
- Surveillance cameras to remotely observe the caller.
- External speakers to communicate with the caller.

Emergency communication telephones may be integrated into the telecommunications network using the following:

- Analog telephone
- Wireless telephone
- IP

Public Address (PA) Systems

Overview

PA systems may be accessed from standard telephones, either with or without being connected to a telephone system, or equipped for access from CO lines. Some systems use dedicated (e.g., push-to-talk) microphones or a dedicated console; however, using telephone access is more common in modern systems.

When integrated to the telephone system, the voice page is made from any telephone by dialing a code or pressing a button and then making an announcement. Many facilities are now required by governmental AHJ to have systems in place specifically for emergency and safety announcements.

In addition to an emergency life safety system, the building paging system is often used for emergency and routine announcements. Stop and start work tones, background music, and personnel tracking are all considered common uses of a building PA system.

The paging equipment is connected to the loudspeaker distribution system in the building. Loudspeakers may be flush mounted in the ceiling, suspended from the ceiling, or wall mounted. Horns are often mounted on walls, racks, poles, or I-beams or suspended from ceilings.

In larger buildings or multibuilding campus applications, there may be multiple zones for the paging system. The audio paging cable runs typically return to the nearest telecommunications room (TR) or equipment room (ER), which allows for easier maintenance, troubleshooting, and system changes.

In addition to one-way paging, overhead paging systems can include the following options:

- Two-way talk-back paging (talk and then listen for a response from the speaker)
- Multiple zones (areas to be paged separately [e.g., office, factory])
- Group call (page multiple areas or zones at once)
- All call (page all areas or zones at once)
- Background music
- Night ringing
- Time clock or class change tones
- Alert or alarm tones
- Battery backup
- Override input
- Line supervision
- Noise masking/speech privacy

 © 2012 BICSI®

Types of Paging Systems

Three main technologies are employed in paging systems:

- IP addressable speakers
- Centrally amplified systems
- Distributed amplified systems

With both centrally amplified systems and distributed amplified systems, the voice page may be accessed by a microphone or telephone. The voice signal is amplified and broadcast over the speakers or horns.

Internet Protocol (IP) Addressable Speakers

IP addressable speakers can be used for zoned systems, multiple buildings, or remote locations.

Each loudspeaker or group of loudspeakers must have its own IP address. The digital signal is sent to distributed amplifiers or amplified loudspeakers with the selected IP address. The IP signal alone will not power the loudspeakers. There must be some type of powered amplifier at the loudspeaker location. IP addressable speakers can be powered utilizing power over Ethernet (PoE). The software (or a hardware matrix switch) allows the user to select which loudspeakers receive the audio signal. Several signals can be sent simultaneously to different locations.

Variable delays between input and delivery can cause audio quality problems and need to be considered in the network design.

Cabling for IP addressable speakers is categorized balanced twisted-pair or optical fiber cable, with local media conversion to return the media to balanced twisted-pair.

Centrally Amplified Systems

A centrally amplified system places the amplifier at the central distribution point for the system. Cabling is extended from this amplifier to the loudspeakers.

Two types of amplifiers and loudspeakers can be used in a centrally amplified system:

- Constant voltage
- Constant current

The constant voltage system is more common in distributed paging systems. Constant voltage, typically 25, 70, or 100 volts (V), is tapped in the field to adjust the loudspeaker volume and load.

The constant current systems are more common in smaller installations and require more consideration in design because the loudspeakers need to be balanced, based on load rating. Constant current is typically driven into a 4 or 8 ohm loudspeaker system.

In both constant current and constant voltage systems, the cable is usually 18 American wire gauge (AWG [1.0 millimeter (mm [0.039 inches (in)])]) or larger and is often shielded. In some localities, conduit may be required due to the voltages (70 or 100 V). Verify this requirement with the local AHJ.

Types of Paging Systems, continued

Distributed Amplified Systems

A distributed amplified system places amplifiers away from the central distribution point. Small amplifiers are placed directly on the loudspeaker mounting frame (e.g., ceiling loudspeakers) or inside the housing (e.g., horn-type loudspeakers).

The ESS designer should be familiar with the following items when designing a PA system:

- Sound pressure level (SPL)
- Loudspeaker selection and placement
- Loudspeaker distribution patterns
- Loudspeaker polarity
- Signal feedback

Components

The basic components in the PA system are the:

- Loudspeaker.
- Power supply.
- Control unit.
- Amplifier or audio mixer.

The control unit performs several functions. It interfaces with the telephone system. All of the access methods listed above are accommodated in the control unit. Zone paging—the ability to send an audio signal to a specific group of loudspeakers—also may be a function of the control unit.

Distributed amplified systems are designed to utilize balanced twisted-pair cable. Category- rated cabling is not necessary but may be used. Table 8.1 details how far the audio signal can be distributed using a 24 AWG [0.51 mm (0.020 in)] or 22 AWG [0.64 mm (0.025 in)] conductor cable.

Table 8.1
Audio signal distance limitations

	Number of Speakers	
Cable Length	**22 AWG [0.64 mm (0.025 in)]**	**24 AWG [0.51 mm (0.020 in)]**
30.5 m (100 ft)	150	150
61 m (200 ft)	150	120
122 m (400 ft)	100	60
244 m (801 ft)	50	30
488 m (1601 ft)	25	15

AWG = American wire gauge
ft = Foot
in = Inch
m = Meter
mm = Millimeter

 © 2012 BICSI®

Components, continued

In general, when the distance limitations are exceeded for either dc power or audio, a dc power supply or extender audio amplifier is added to continue the entire distance of the speaker run. Both of these devices require external power. The ESS designer shall review existing codes and standards in collaboration with the AHJ to determine whether power supplies or amplifiers may be located in the space above a ceiling within an approved enclosure.

Audio Input Circuits

Two types of inputs are commonly used in PA systems:

- Microphone—This circuit conducts the signal from a microphone to a preamplifier or audio mixer. The cable should have two conductors with a shield. The typical connector on this cable is called an X series (X latching resilient rubber compound [XLR]), although conductors may be directly terminated on other types of terminating devices. The typical signal levels for this circuit are -80 decibel milliwatt (dBm) to -20 dBm.
- Line-level—This circuit connects the output of a microphone preamplifier, tape player, compact disc (CD) player, or telephone common equipment to an audio mixer or amplifier. The cable may have one or two conductors with an overall shield. The typical signal levels are -20 dBm to 0 dBm.

Audio Output Circuits

Audio output cabling connects the output of a 25, 70, or 100 V amplifier to the loudspeaker impedance matching transformers. It is usually an 18 AWG [1.0 mm (0.039 in)] or larger, two-conductor stranded cable. Shielded cable is necessary when running higher voltage level speaker lines in close proximity to voice or data cabling. Typical connectors for this cable are spade lugs.

Microphone and line-level cables should not be run in close proximity to audio output cables because crosstalk may occur. In many jurisdictions, audio output circuits cannot share pathways with other power-limited or communication circuits, and must be installed in dedicated pathways.

Audibility

Since hearing is the most common mode of alarm perception, audibility is perhaps the single most important aspect of alarm signaling.

Effective audibility can be compromised in many ways, including:

- Alarm level—If output levels are not sufficient, occupants will be unaware of alarm events.
- Alarm clarity—If alarm tones and patterns are not clearly recognizable, occupants may misinterpret the nature of the alarm.
- Alarm reliability—Excessive false alarms can create mistrust and doubt, which can lead to ignoring alarm events.

Codes and standards contain extensive rules and guidelines to address these issues.

Intelligibility

It is common for voice messages to be audible but not intelligible. Crowded subway stations, large auditoriums, and houses of worship are examples of areas that may have sufficient audible output but poor intelligibility. Codes and standards require that audible messages be intelligible but may not expressly define required levels of intelligibility.

Voice Telephone Systems for Notification

One of the advantages of using telephone for audio communication is that because it allows two-way communication, there is feedback that the message has been delivered to the correct individual.

A disadvantage is that people have to sign up so you can call their current telephone number. Visitors will not be notified, and telephone calls can be missed.

Centralized Calling

Some organizations set up telephone banks. They have rooms with large numbers of telephones and give each person a list of numbers to call and a script to read. Emergency notification requires a large number of telephone lines to be available.

Noise Masking

A noise masking system is often used in financial and medical office applications and uses pink noise to create an artificial sound barrier in open office environments to provide increased privacy by masking conversations. Noise masking systems can be stand-alone systems or may simply be an additional audio input into an overhead paging system.

Sound Reinforcement

A sound reinforcement system typically is used in auditoriums and theaters to amplify the voices of people speaking, live entertainment, prerecorded music, or other audio sources.

NOTE: For more information on sound reinforcement systems, refer to the current edition of the BICSI®/InfoComm International® *AV Design Reference Manual*.

 © 2012 BICSI®

Video Display Devices

Information can be provided to an audience through the use of video display devices. This method may be used to provide emergency instructions or general information.

When selecting a display device, the ESS designer must consider the viewing angle, screen size, and viewing distance to determine the required display resolution.

Common types of display devices include:

- Cathode ray tube displays (legacy).
- Liquid crystal displays.
- Plasma displays.
- Video walls.
- Projection devices.
- Light-emitting diode (LED).
- Organic LED.

Analog versus Digital Inputs for Display Devices

For security applications, the previously described display devices will support either analog or digital sources at a variety of resolutions. These displays may have interlaced or progressive scan technology.

Display devices using an analog video source may use red, green, blue, horizontal sync, vertical sync (RGBHV); component video red, green, blue (RGB) or white, blue, red (Y, Pb, Pr); separated video (S-video [Y/C]); or composite analog video connectivity.

Display devices with digital sources may use display port, digital visual interface–digital (DVI-D), serial digital interface (SDI), high-definition serial digital interface (HDSDI), digital visual interface–integrated (DVI-I), or high-definition multimedia interface (HDMI) connectivity.

Extended display identification data (EDID) is a handshaking method that these digital displays use to exchange display capabilities, such as native resolution, with sources to match audio and video output format to the display input. EDID can provide the best possible image. In some circumstances, the data may not be exchanged successfully and can cause resolution problems or no image display. Hardware may need to be added to the video switching path to properly pass the EDID to the display.

To prevent illegal copying and multiple displays of content, “analog sunset” was included in the Advanced Access Content System (AACS) license agreement. AACS restricts analog output when playing an encrypted Blu-ray Disc™ or new content from video sources such as cable TV receivers and digital video recorders. Analog sunset shall not apply to computers when not playing Blu-ray Discs.

After 2010, Blu-ray Disc players limited analog video output of protected content to standard definition. After 2013, Blu-ray Disc players shall not produce analog signals for protected content.



Chapter 9
Special Systems

Chapter 9 explains the design and application of various specialty systems. It provides an electronic safety and security (ESS) designer with the fundamental tools necessary to properly design basic systems as well as a level of knowledge to work with specific system providers. Some of the systems discussed include nurse call, radio frequency identification (RFID), at-risk human perimeter systems, and asset management systems.

Table of Contents

Special Systems 9-1
Introduction 9-1
Nurse Call 9-1
Overview 9-1
System Types 9-1
Tone/Visual Nurse Call System 9-1
Audiovisual (AV) Nurse Call System 9-2
Nurse Call System Components 9-3
Initiation Devices 9-3
Central Equipment 9-7
Notification Devices 9-7
Wireless Nurse Call Systems 9-8
Nurse Call System Wiring 9-9
Radio Frequency Identification (RFID)-Based Systems 9-10
Overview 9-10
At-Risk Human Perimeter Systems 9-11
Supervised Care Elopement Prevention/Patient Wandering 9-11
Infant Abduction Prevention 9-11
System Options 9-12
Asset Management Systems 9-12
Retail Tagging Technology 9-12

Figures

Figure 9.1 Typical nurse call staff emergency station 9-3
Figure 9.2 Typical nurse call bedside station 9-4
Figure 9.3 Typical nurse call code call station 9-5
Figure 9.4 Typical nurse call staff station 9-6
Figure 9.5 Nurse call system traditional one-line diagram 9-9
Figure 9.6 Typical radio frequency identification tag 9-10

 © 2012 BICSI®

Special Systems

Introduction

This chapter is an overview of the design and application of various specialty systems. The intent is to provide an electronic safety and security (ESS) designer with the fundamental tools to properly design some of the more basic systems as well as a level of knowledge necessary to work in cooperation with the specific system providers.

Nurse Call

Overview

The primary purpose of a nurse call system usually is calling nurses, as the name implies. The term "nurse call" can be misleading because most systems are not limited to this function. Depending on the occupants in the space, the nurse call system may be used to notify doctors, nurses, orderlies, wait staff, or any other staff. In addition, a system may notify staff using designated tones, lights, voice communication, text messaging, or other communication. Typically, a nurse call system can be supplemented by or interfaced with a paging system to annunciate code calls or to page specific staff.

The design and installation of nurse call systems must comply with all governing regulations.

System Types

Nurse call systems can be categorized by the type of communication used. The sophistication of the communication is determined by the type of facility and staff of the health care institution.

Tone / Visual Nurse Call System

A tone/visual nurse call system typically is used in locations where supervision is required without the threat of emergency medical attention. Examples of when to use this system are as follows:

- Patients need only supervision—Supervised care facility
- Patients are under constant supervision—Intensive care unit (ICU), preoperative area (preop), operation recovery area, and emergency department
- Sophisticated voice communications are not necessary—Clinical area

At the basic level of nurse call design, tone/visual nurse call systems provide an opportunity for medical staff or patients to notify the supervising staff if there is a problem. Notification is provided using a special tone (or pattern of tones) and a flashing light at the supervising station and the entrance or door of the room or area where the incident occurred. This directs staff to the area where supervision is necessary.

System Types, continued

Audiovisual (AV) Nurse Call System

Voice communication allows health care practitioners to perform their duties in a more efficient and personal manner. Voice communication enables staff to supervise patients remotely. Newer technologies (e.g., remote patient monitoring, telemetry, camera supervision) are being used to offset the growing shortage of qualified staff.

An audiovisual (AV) nurse call system typically is used in locations where supervision is required along with the threat of emergency medical attention. Virtually all areas of a hospital would fall under this description unless it is permitted to use a tone/visual nurse call system as described above.

AV nurse call systems at the very rudimentary level provide an opportunity for medical staff or the patients to notify the supervising staff if there is a problem. Notification is provided using a special tone (or pattern of tones) or flashing light similar to the tone/visual system. AV systems also provide the additional option of a prerecorded or live voice message. Notification typically is present at the supervising station and the entrance of the room or area where the incident occurred.

 © 2012 BICSI®

Nurse Call System Components

Tone/visual and AV nurse call systems share many of the same standard components or options within the same common device categories.

Nurse call system devices can be separated into three categories—initiation devices, central equipment, and notification devices:

- Initiation devices primarily are used to create an electronic signal that is sent to the central equipment or notification devices or to initiate an alarm/event.
- The central equipment primarily is used for electrical or electronic processing and routing of the alarm and signal between initiation devices and notification devices.
- Notification devices primarily function to convert the electronic signal into a recognizable alarm to notify the appropriate supervising staff of an alarm/event.

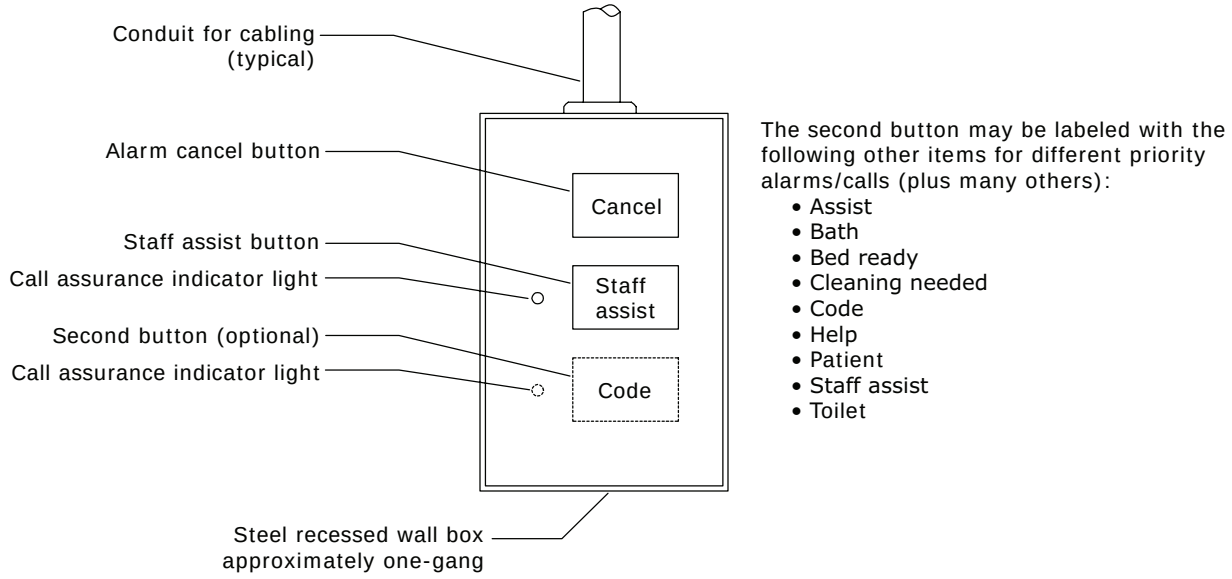
Devices are described below in this order to demonstrate the signal flow from initiation to signal processing and then notification.

Initiation Devices

Staff Emergency Station

A staff emergency station is a device that is initiated by a staff member to request additional help (see Figure 9.1).

Figure 9.1
Typical nurse call staff emergency station



Nurse Call System Components, continued

Bathroom Station

A bathroom station is a wall- or ceiling-mounted device that is used if a patient needs to alert the supervising staff while using the bathroom. Occasionally, these devices have a pull cord instead of a push button.

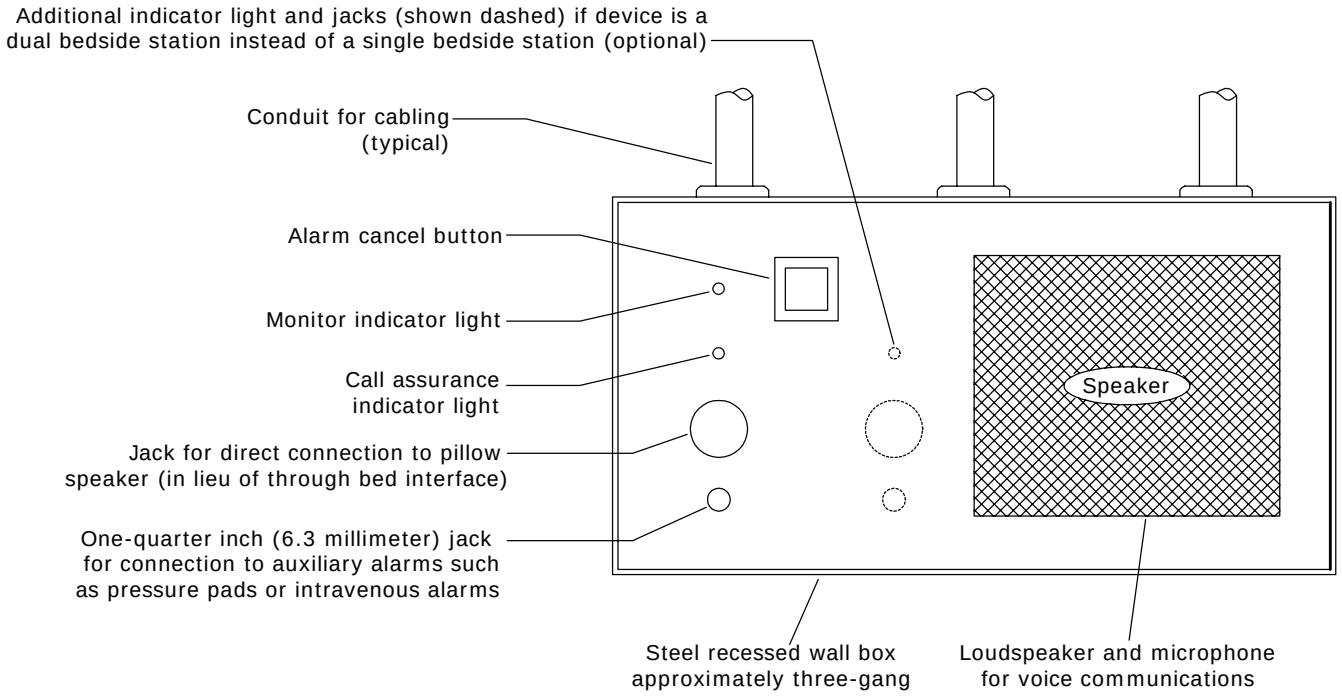
Pillow Speaker

A pillow speaker is a device that connects to the bedside station or bed to provide controls for a patient to contact the nurse call system. Many pillow speakers have switches and space for the control of additional devices (e.g., TV, window shade, radio, lighting).

Bedside Station

A bedside station is a wall- or table-mounted device at the head of a patient's bed and provides connections for one or two pillow speakers (see Figure 9.2). These connections also may be used to connect patient monitors or additional auxiliary devices (e.g., intravenous [IV] pump alarms) to the nurse call system. Call buttons and tone speakers are integrated with the bedside station for the patient to request help and receive acknowledgment.

Figure 9.2
Typical nurse call bedside station



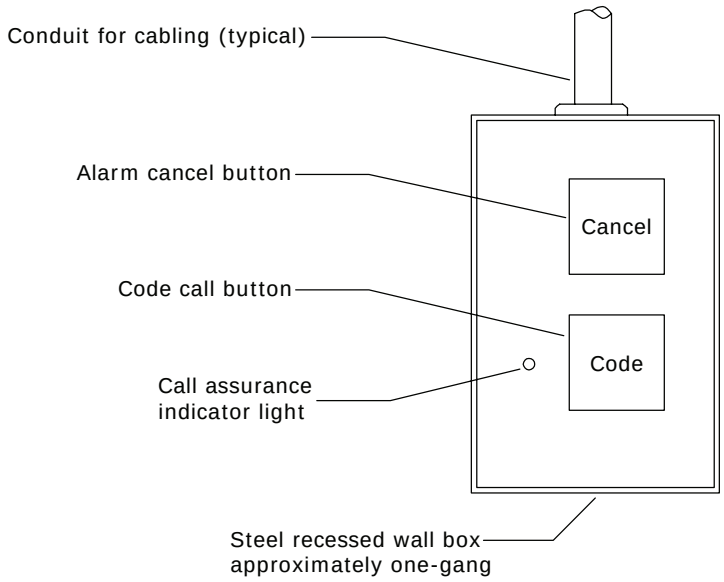
 © 2012 BICSI®

Nurse Call System Components, continued

Code Call Station

A code call station is a device that has one or more buttons that initiate different code calls to the staff (see Figure 9.3). The alarm signal can be silenced only from the actual code call station to ensure proper supervision and inspection. The typical application is a device that alerts the staff to a high-priority incident.

Figure 9.3
Typical nurse call code call station



Nurse Call System Components, continued

Geriatric Push Plate Code Call Station

A geriatric code call station has a large push plate or pull cord that is easier for limited dexterity individuals to use to signal a code call.

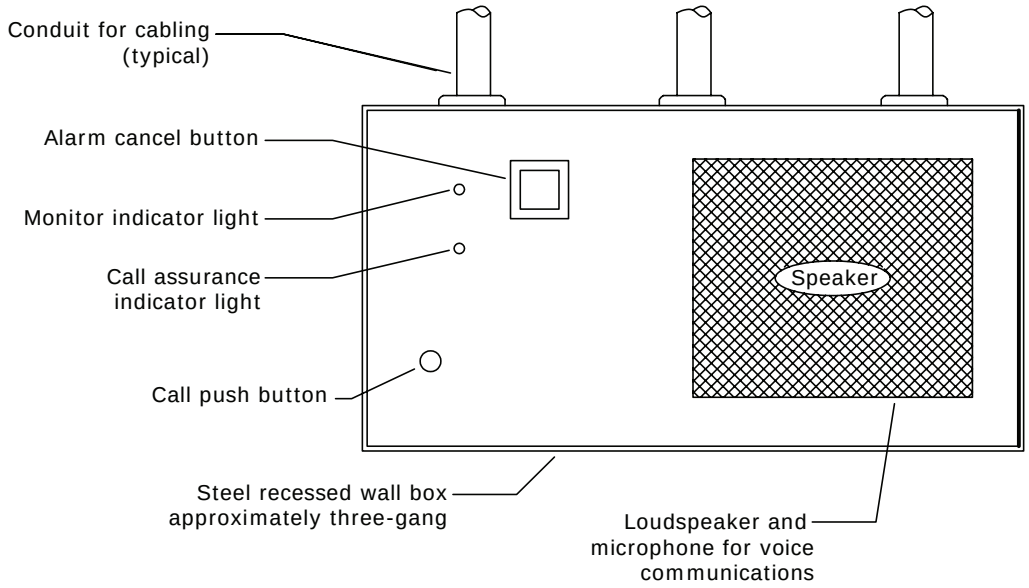
Tamper Resistant Code Call Station

A tamper resistant code call station is used in psychiatric wards or detention center areas. Specialty hardware is required to remove the fasteners, which renders the device tamper resistant. Tamper resistant devices typically are constructed of all metal parts for durability.

Staff Station

A staff station is a wall-mounted device that is used by the staff to make an intercom call to additional staff located at a main nurse station (see Figure 9.4). This type of station can be used only on AV nurse call systems.

Figure 9.4
Typical nurse call staff station



Staff Register Station

A staff register station is a wall-mounted device that alerts the nurse call system that a staff member is present in the room. These may operate using infrared (IR), radio frequency (RF), radio frequency identification (RFID), special buttons, or keyed switches. This type of station can be used only on AV nurse call systems.

Bed Interface

A bed interface is a device that provides additional bed control and functionality for patient room controls from the bed. With some manufacturers, the device can permit a pillow speaker to connect directly to the bed instead of the bedside station as well. This connection can be wireless or hardwired. This option can eliminate damaged connectors and cordage due to accidental movement of the patient bed. This type of station can be used only on AV nurse call systems.

 © 2012 BICSI®

Nurse Call System Components, continued

Tamper Resistant Ceiling Microphone

A tamper resistant ceiling microphone commonly is used in psychiatric wards or detention center patient rooms. An important use for this device is to monitor the room when staff is present to protect against patient violence. This type of station can be used only on AV nurse call systems.

Tamper Resistant Hall Station

A tamper resistant hall station commonly is used in psychiatric wards or detention center corridors. This device is designed to alert staff of an alarm condition associated with a tamper resistant ceiling microphone. This device is essential for staff safety because it can alert staff of a problem before entering a high-security patient room. This type of station can be used only on AV nurse call systems.

Central Equipment

Intermediate Cross-Connect (IC [Building Distributor (BD)])

A traditional nurse call system typically has a group of termination blocks on the wall or in a cabinet. This consists of various types of balanced twisted-pair cabling. An end-to-end Internet protocol (IP)-based system would use all of the same type of equipment as a typical data network (on a dedicated network), with horizontal cabling, patch panels, and patch cords.

System Interfaces

Nurse call systems typically are required to be electrically isolated from all other systems. Nurse call systems have interfaces that allow the system both to remain electrically isolated and communicate with other systems.

Central Equipment Location

Active control hardware for a nurse call system typically is housed in a centrally located room.

Notification Devices

Master Station

A master station functions as the main interface between the nurse call system and the supervising staff. These stations can be touch screen, push button, or computer based.

Minimaster Station

A minimaster station shares the same role as a master station. A minimaster station commonly has less functionality or less priority or control than a master station. Minimaster stations typically are located in smaller, secondary nurse stations or alcoves.

Nurse Call System Components, continued

Annunciator Panel

An annunciator panel is similar to a minimaster station but typically is wall mounted with little control over the system. Annunciator panels are used when the only requirement is notification of the alert location.

Paging Systems

Paging systems may be used as part of the nurse call system. Refer to Chapter 8: Notification, Communication, and Display Devices for more information.

Corridor Light

A corridor or zone light is a notification light that can be wall or ceiling mounted. Additionally, a corridor light can emit a tone associated with the light.

Zone Light

A zone light is a device that shares the overall functionality and design of a corridor light. The function of a zone light is to provide staff with a summary of multiple corridor light rooms or areas. Zone lights display and sound an alarm if any one or multiple of the combined rooms have an alarm condition. In multiple corridor nursing units, zone lights shall be installed at the intersections of corridors.

Wireless Nurse Call Systems

Wireless technologies that have proven useful are:

- Wireless hands-free voice recognition communication.
- Wireless telephone technology.
- Wireless asset tracking, patient monitoring, and staff locating.

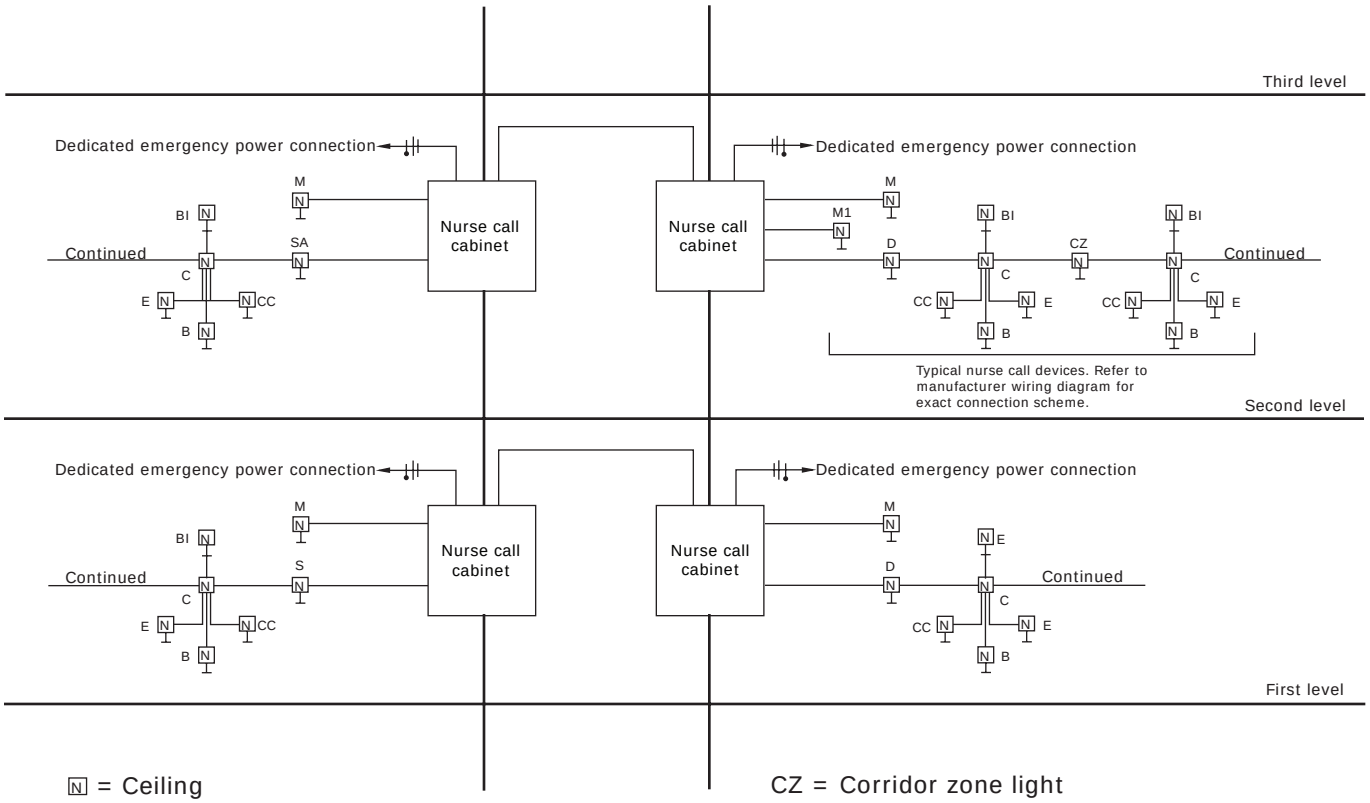
NOTE: Care should be used to select frequencies that will not interfere with other hospital systems. If the ESS designer believes that the use of wireless systems would be of value in a project but is not well acquainted with wireless transmission systems and issues, the ESS designer should seek the counsel of qualified personnel, such as a BICSI-certified wireless designer.

 © 2012 BICSI®

Nurse Call System Wiring

Nurse call systems may use balanced twisted-pair, shielded twisted-pair, or multiconductor cable or a combination of these. The wiring requirements for a nurse call system are governed by the manufacturer of the system. Installation documentation should be referenced for the correct wiring requirements (see Figure 9.5).

Figure 9.5
Nurse call system traditional one-line diagram



N = Ceiling
N = Wall
B = Single bedside station
BI = Bed interface unit for pillow speaker
C = Corridor dome light
CC = Code call station
CZ = Corridor zone light
D = Duty station
E = Bathroom/toilet/shower emergency station
M = Master station
M1 = Minimaster station
S = Staff station
SA = Staff assist emergency call station

Radio Frequency Identification (RFID)-Based Systems

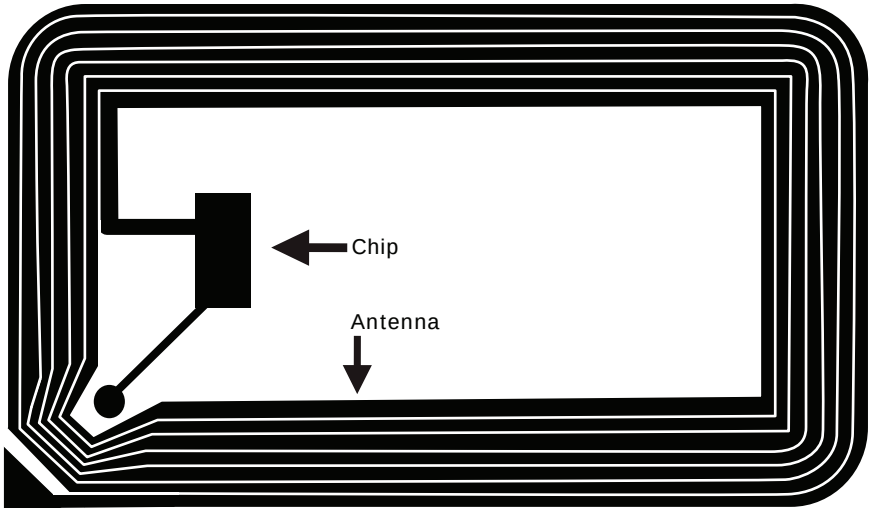
Overview

RFID denotes technologies that use radio waves for automatic identification and data collection. Among the various methods of RFID object identification, the most common is storing the serial number that identifies the object and other information on a microchip that is attached to an antenna.

The chip and the antenna together are called an RFID transponder or an RFID tag (see Figure 9.6). The antenna enables the chip to transmit the identification information to a reader. The reader converts the radio waves returned from the RFID tag into a form that can be transmitted to and interpreted by a computer processor.

NOTE: See Chapter 4: Access Control Systems for more information.

Figure 9.6
Typical radio frequency identification tag



The intent of this section is to discuss RFID and its uses for ESS. Although many applications use this technology, the following applications have been identified as common uses for ESS:

- At-risk human perimeter systems (e.g., supervised care, hospitals)
- Asset management systems
- Retail loss prevention

 © 2012 BICSI®

At-Risk Human Perimeter Systems

At-risk human perimeter systems are designed to alert medical staff when a sensor attached to a patient passes outside the allowed area. The system design and advancement closely mimic those of loss prevention systems because of the similarity in technical and functional design.

These systems can be categorized into two major groups with completely different risks:

- Supervised care facilities utilize systems designed to protect patients from wandering or delopement.
- Baby alert systems are designed for use in nursery and birthing medical units to protect patients from abduction.

Supervised Care Elopement Prevention / Patient Wandering

Supervised care facilities are dedicated to patients who cannot care for themselves. The nature of the illness and disabilities of patients of this type make it necessary to protect them from elopement.

ESS systems have been designed to alert staff when a patient attempts to cross a predetermined boundary. The sophistication of these systems and the options available can vary, but the main function is to provide perimeter security for at-risk patients while allowing free access and egress for select populations, visitors, and staff. These systems also can help a facility present a more open and inviting environment by decreasing the requirement for locked doors and other types of architectural security.

The functionality of these systems often involves the following:

- Wireless door sensors are located at perimeter or secure area doors.
- When a patient wearing a wireless transmitter (pendant or anklet) approaches the door, the sensor locks the door and can trigger an alarm after a predetermined time or if the door is breached while the transmitter is in range of the sensor.
- A keypad or access control card reader is often installed at the door to allow authorized personnel to override the door alarm when an at-risk patient needs to be escorted through the door.
- Doors often are put on a time schedule; for example, doors are unlocked during the day or locked in the evening based upon the operational requirements of the facility.
- Alarm functions from these doors can be integrated to a facility's access control or emergency notification system to alert staff when a remote door has been breached.

Infant Abduction Prevention

Infant abduction systems are similar to the supervised care elopement systems. Both systems use similar products and principles of design. Unlike the elopement system, these systems are intended to deter persons with malicious intentions.

Infant abduction systems include additional options specifically driven by its purpose. The software used can include mother and infant matching options; this is convenient during the patients stay and vital at checkout. Elevators, doors, staff only areas, and all points of egress are designed to automatically lock and prevent access when the transmitter device enters a predetermined area.

At-Risk Human Perimeter Systems, continued

System Options

At-risk human perimeter systems include options such as:

- Real-time tracking and locating of assets, patients, and staff.
- Intelligent software capable of recognizing trends.
- Loitering recognition.
- Multiple programmable security levels.
- Ability to lock doors when a risk is present.
- Logging.
- Network and computer integration.
- Fall detection.
- Paging.
- Elevator deactivation.
- Multiple display and annunciator.
- Voice, tone, or visual alarms.

Asset Management Systems

The technology used for asset management systems can vary depending on the asset to be tracked. All technologies include a database to store permanent information on the asset and update the location of the asset when new information is received. Asset management systems commonly use RFID for electronic identification.

Retail Tagging Technology

Tracking, identifying, and counting merchandise can offer efficiency to retail establishments. The use of electronic tagging in the retail environment has grown as the cost and advantages have become more appealing.

Uses of RFID in retail applications may include:

- Inventory management.
- Shoplifting deterrence.
- Employee theft deterrence.
- Returns and warranty.
- Operational efficiency.

 © 2012 BICSI®



Chapter 10
Network Concepts

Section 1 of Chapter 10 focuses on design considerations for networks utilized in electronic safety and security (ESS) applications. Section 2 provides an overview of threats, countermeasures, and implementation guidelines for security as they relate to network-based ESS system design. Risks and control measures are explained and discussed.

Table of Contents

SECTION 1: NETWORK DESIGN PRINCIPLES

Network Design Principles 10-1
Overview 10-1
Information Technology (IT) and Electronic Safety and Security (ESS) 10-2
Internet Protocol (IP)-Based Electronic Safety and Security (ESS) Systems 10-2
Electronic Safety and Security (ESS) Supporting Networks 10-2
Intelligence to the Edge Devices 10-2
Internet Protocol (IP)-Based Electronic Safety and Security (ESS) System Planning, Design, and Implementation Considerations 10-3
Systems Integration and Interfacing 10-3
Scalability 10-3
Resource Sharing 10-3
Reliability 10-5
Resiliency 10-5
Standardization 10-6
Network Management and Administration 10-7
Bandwidth and Quality of Service (QoS) 10-8
Network Infrastructure 10-9
Internet Protocol (IP) Network Architecture 10-10
Overview 10-10
Types of Networks 10-10
Open Systems Interconnection (OSI) Reference Model 10-11
Layer 7 (Application) Services 10-14
Layer 6 (Presentation) Services 10-14
Layer 5 (Session) Services 10-14
Layer 4 (Transport) Services 10-14
Layer 3 (Network) Services 10-14
Layer 2 (Data Link) Services 10-14
Layer 1 (Physical) Services 10-14
Internet Protocol (IP)-Based Access Control Systems (ACS) 10-15
Cabling Infrastructure 10-15
Communications 10-15
Expandability 10-16
Reliability 10-16
Management 10-16

Internet Protocol (IP)-Based Video Surveillance Systems (VSS) . . . 10-17
Characteristics . . . 10-17
Internet Protocol (IP)-Based Voice Communication Systems . . . 10-19
Overview . . . 10-19
System Architecture . . . 10-20
End-to-End Internet Protocol (IP) Paging Systems . . . 10-20
Hybrid Internet Protocol (IP)/Traditional Paging Systems . . . 10-22
Determining System Capacity . . . 10-23
Miscellaneous Systems Utilizing Internet Protocol (IP) . . . 10-24
Overview . . . 10-24
Characteristics . . . 10-24
System Architecture . . . 10-25
Fire Alarm (FA) Hybrid/Internet Protocol (IP) System . . . 10-25
Intrusion Detection (Burglar Alarm) Hybrid/Internet Protocol (IP) System . . . 10-27
Nurse Call Hybrid/Internet Protocol (IP) System . . . 10-29
Determining Internet Protocol (IP) System Capacity . . . 10-29
SECTION 2: NETWORK SECURITY
Network Security . . . 10-31
Overview . . . 10-31
Risks . . . 10-33
Denial of Service . . . 10-33
Replay Attacks . . . 10-33
Spoofing . . . 10-33
Backdoors . . . 10-33
Malicious Codes . . . 10-34
System Control . . . 10-34
Social Engineering . . . 10-34
Phishing and Spear Phishing . . . 10-35
Mobile Devices . . . 10-35
Insider Threats . . . 10-35
Control Measures . . . 10-36
Overview . . . 10-36
Firewalls . . . 10-36
Intrusion Detection and Prevention Systems . . . 10-41
Network Segregation with Virtual LANs (VLANs) . . . 10-41
Virtual Private Networks (VPNs) . . . 10-41

 © 2012 BICSI®

Access Control Lists (ACLs) 10-41
Network Admission Control (NAC)
Network Access Protection (NAP) Systems 10-42
Dial-Back Modems 10-42
Network Behavior Analysis 10-42
Vulnerability Scanners 10-42
Server Hardening 10-42
Authentication Methods 10-43
Software Patching 10-43
Antivirus 10-43
Encryption 10-43
Security Information and Event Management (SIEM) 10-44
Awareness Training 10-44
Background Checks 10-44
Segregation of Duties 10-44
Audits 10-44
General Security Recommendations 10-45
Develop a Security Policy 10-45
Establish Physical Security 10-45
Lockdown Perimeter Security 10-45
Enable Existing Security Features 10-46
Secure Operational Traffic 10-46
Secure Management Traffic 10-46
Manage Configuration 10-47
Eliminate Security Deficiencies 10-47
Continuous Security Training 10-47
Perform Security Audits 10-47
Trends 10-47

Figures

Figure 10.1 Open Systems Interconnection Reference Model 10-11
Figure 10.2 Message transfer described using the Open Systems Interconnection Reference Model 10-13
Figure 10.3 End-to-end Internet protocol paging system diagram 10-21
Figure 10.4 Hybrid Internet protocol/traditional paging system diagram using an Internet protocol backbone 10-22
Figure 10.5 Hybrid Internet protocol/traditional fire alarm system diagram 10-26
Figure 10.6 Hybrid Internet protocol/traditional intrusion detection systems diagram 10-28
Figure 10.7 Hybrid Internet protocol/traditional nurse call system diagram 10-30
Figure 10.8 Stand-alone network 10-37
Figure 10.9 Enterprise network 10-38
Figure 10.10 Example of security zones 10-40

Tables

Table 10.1 Challenges to Internet protocol migration 10-24

 © 2012 BICSI®

Network Design Principles

Overview

This section provides an introduction to the design principles for Internet protocol (IP)-based electronic safety and security (ESS) systems. It includes a brief overview of the IP network-based security world, followed by a general introduction to network architecture and the considerations necessary for planning, designing, and implementing state-of-the-art systems.

The material has been written to reflect the contents of the current editions of the BICSI® *Network Design Reference Manual* (*NDRM*) and *Telecommunications Distribution Methods Manual*, both of which provide extensive coverage of network technologies and design principles.

Information presented in this section includes the:

- Historical development of security systems architecture and application.
- Basic IP networking fundamentals as applied to ESS systems.
- Planning and design of the IP architecture for ESS applications to meet performance requirements.
- Advantages and challenges of each type of ESS system, comprising:
  - Access control.
  - Video surveillance.
  - Voice communication.
  - Intrusion detection.
  - Fire alarm.
  - Nurse call.
  - Specialty systems.

Security systems rely on the transmission of mission-critical life safety information in real time with the ability to review that information later for the preparation of incident reports or as evidence in court. The role of information technology (IT) is to transport, process, store, and present information for review and disposition.

With current technologies, detailed information can be collected, distributed, and stored for review in ways that were unavailable with traditional, non-IP, security systems. With these technological advances and the movement toward IP networks, an increasing number of detection technologies have been introduced. When utilized properly, these devices provide the ability to detect and respond to a greater number of stimuli than ever before, improving the overall level of safety and security.

Information Technology (IT) and Electronic Safety and Security (ESS)

Internet Protocol (IP)-Based Electronic Safety and Security (ESS) Systems

IP-based ESS systems typically consist of monitors, countermeasures, controls, and sensors placed at strategic locations throughout a facility or a geographic zone. These devices utilize existing standards-based network architecture to interconnect through electrical conductors or wireless devices to a control panel. This panel sends information to other devices on the system that interpret this information and invoke predetermined responses.

Generally, networks are implemented to enable the sharing of resources and the exchange of information between users. As the number of resources, users, and connections increases, networks must be routinely modified to accommodate the growth, making network design a dynamic and continual process.

For example, the addition of a secured door could necessitate a card reader and keypad or biometric reader, request to exit (REX) device, intercom for two-way voice communication, and possibly a video camera for visual identification. Each of these devices requires special consideration and coordination to establish network connectivity as well as to determine the impact these additional devices will place on the supporting network. These issues, topics, and concerns are addressed throughout this section.

Electronic Safety and Security (ESS) Supporting Networks

Physically, a network can be as small as two connected computers and the media used to enable the connections, which can be physical or wireless.

A network cabling infrastructure is a combination of products, design principles, physical configuration, functional organization, operational procedures, and data formats used as the basis for the design, construction, modification, and operation of an information technology systems (ITS) network.

The structured grouping of hardware (e.g., network cabling equipment), software, and applications creates the network architecture that allows for the transport of voice, data, and video signals between network devices in a building or campus or across a geographic area. The successful integration of these three elements allows the exchange of information and data and the sharing of resources among users, administrators, and devices.

Intelligence to the Edge Devices

As intelligence and functionality migrate to edge devices, such as cameras and card readers, the ESS designer will be able to integrate and control most aspects of a business, including ITS; network and Internet access; heating, ventilating, and air conditioning (HVAC) control; elevator control; physical access; and video surveillance.

 © 2012 BICSI®

Intelligence to the Edge Devices, continued

The applications will be determined by the end user's needs and the ESS designer's or integrator's knowledge and abilities. Pushing intelligence to the edge devices will be the future of convergence in the security sector.

By embedding analytics technology in devices, the ESS designer can create "smart" devices, which are capable of reducing bandwidth and storage requirements. These intelligent devices provide two-way communication, are interactive, and can act independently as decision makers, thereby increasing the accuracy of alarms, preventing false positives, and increasing the effectiveness of security resources.

Additionally, because intelligent edge devices analyze captured data in real time as events are detected, an alert can be sent immediately to the appropriate parties, thereby dramatically reducing response time.

Internet Protocol (IP)-Based Electronic Safety and Security (ESS) System Planning, Design, and Implementation Considerations

The following topics are discussed in detail for each of the ESS systems covered in this section.

Systems Integration and Interfacing

Systems integration is a major advantage of network-based systems that integrate disparate systems together and provide interfaces designed to achieve interoperability, seamless communication, and operational efficiency. The integration of data systems allows diverse systems to share or access information across functional or system boundaries.

NOTE: See Chapter 11: Systems Integration for more detailed information.

Scalability

IP-network technology makes it possible for an organizational network to easily and economically scale beyond the physical boundaries of a building or campus to suit any size installation and support growth after the initial deployment. For example, access control systems (ACS) could be expanded across multiple facilities by adding new devices to the existing network infrastructure.

ESS networks that are intended to scale over time must be designed with quality of service (QoS) in mind.

Resource Sharing

In many instances, it is difficult to justify the purchase of costly devices, services, or software if only one computer can access them at a time. IP networks allow for the sharing of these resources.

Internet Protocol (IP)-Based Electronic Safety and Security (ESS) System Planning, Design, and Implementation Considerations, continued

Based on control measures established by the network administrator, users may access various types of resources connected to the network through the server. The types of resources include:

- Software applications.
- Peripheral devices.
- User-created files.
- Internet access.
- Management tools.

A peripheral device is any piece of equipment that can be connected to and controlled by a computer via the network. Examples of peripherals include printers, scanners, modems, and removable storage devices.

Multiple network users can access a peripheral if the device is connected to the network either directly or indirectly:

- Direct connection—The peripheral device can be equipped with a network interface card (NIC) and software compatible with the type of network in use.
- Indirect connection—The peripheral device is connected to a station or a server on the network, and its resources are made available through the network operating system (NOS) software.

Without networks, each computer stores data locally, unlike mainframes or minicomputers, both of which use centralized storage. As a result, faulty reporting and decision making can occur if the same data is updated on some computers but not on others. Information sharing and data exchange are also problematic in this area. A network makes it possible to centralize data. All files shared by users are stored in a central location, which guarantees consistency and simplifies the update process.

In addition to user-created files, software applications can be installed on a centralized storage device accessible from any computer connected to the network locally or remotely. This accelerates the deployment process since any application or update only needs to be installed once on the network.

Examples of ESS applications that make use of the resource sharing capabilities include:

- Access control databases and activity reports.
- Video streaming and data collection.
- Video analytics.
- Alarm reporting.
- Access control and time and attendance integration.

 © 2012 BICSI®

Internet Protocol (IP)-Based Electronic Safety and Security (ESS) System Planning, Design, and Implementation Considerations, continued

Examples of network resources that can be utilized by ESS devices include:

- Printers.
- Storage and archiving equipment.
- Compact disc/digital versatile disc (CD/DVD) writers.
- Servers.

A network must be equipped with services designed for resource sharing, including:

- Access control—Necessary in cases where two or more devices attempt to use a shared resource at the same time (e.g., telecommunications circuit between two sites, a printer).
- Synchronization—Ensure that a receiving device is listening when a sending device is transmitting to that device.
- Flow control—Monitor and adjust the rate at which data is transferred from a sender to a receiver in order to minimize transfer time and data loss. For example, if a receiving device is occupied with other tasks, it will use flow control to ask the sending device to pause transmission.
- Error control—Necessary to verify that a message was transferred successfully between a sender and a receiver or to request a retransmission if the transfer was not successful as determined by error checking.

Reliability

Reliability is the predictable behavior of a system or a group of integrated systems during operation.

As building systems become more integrated and complex, they become less reliable. Reliability is cumulative in a system and decreases as significant or critical components are added.

Reliability is an important attribute in distinguishing one IP security solution from another. For example, choosing cameras with a built-in memory buffer captures video in the event of a loss of connectivity. When the network becomes available again, the data can be recaptured as if the network was never down. The size of the buffer determines how long the camera can reliably capture data without the supporting network.

Resiliency

The primary reason for designing resilience into a network is to avoid single points of failure that can have a devastating impact on mission-critical business functions. Today's networks allow for layers of resilience, so even if a network component fails, backup telecommunications paths can reroute the event transmissions around the problem component.

Internet Protocol (IP)-Based Electronic Safety and Security (ESS) System Planning, Design, and Implementation Considerations, continued

To adequately protect the exchange, transfer, and storage of data across a network, both network resilience and service resilience must be incorporated into the design:

- Network resilience is accomplished through the design of alternate data paths between two IP network switches. This allows the network to maintain operation in the event of a cable fault.
- Server resilience is accomplished by locating a duplicate server in a remote location to achieve a "hot" resilience. Service resilience protects a network against significant disruption and costs in terms of time, resources, and money in the event of a single storage device failure.

Backups may not exist for critical data if users do not duplicate their files on a regular basis. A network can be equipped with a backup system that runs at specific intervals, ensuring that critical data is mirrored and stored, making it available from a secondary source if needed.

Power supply resilience allows for uninterrupted service in the event of a loss of primary power. This important component of the system resilience plan makes use of power loss detection, power distribution, power quality monitoring, and battery backup to ensure reliable and continuous line voltage power to equipment.

Standardization

The standardization of technologies, processes, architectures, infrastructure, installation practices, and other related network hardware results in a high level of interoperability. The flexibility of standardized network hardware used in IP-based security systems gives users more options for equipment integration, acquisition, maintenance, upgrade, and replacement.

IP system design, installation, and testing methods are well defined because of generally accepted standards and practices for the data networking industry. Additionally, standardized network hardware is widely available and cost-effective.

Telecommunications cabling standards are developed to provide compatibility with existing and future network technologies. These standards make it possible to implement a cabling infrastructure using a structured approach where a common set of design and performance guidelines ensures compatibility between cabling systems and network technologies. The term structured cabling system (SCS) is often used to describe a standards-based cabling infrastructure.

 © 2012 BICSI®

Internet Protocol (IP)-Based Electronic Safety and Security (ESS) System Planning, Design, and Implementation Considerations, continued

Network Management and Administration

Network management is the combination of planning, procedures, hardware, software, and personnel needed to maintain network operations at maximum efficiency at all times.

Because changes in hardware and software are routine on most networks, network administrators must be able to perform multiple network-related tasks.

Networked devices make it easier for a network administrator to monitor, control, and change the configuration of any station from a centralized location using management software.

The network replaces the need for physical access to a station for management tasks such as:

- Taking inventory of the hardware and software components in specific stations across the network.
- Installing or updating station software, including the station's operating system (OS). Update configurations may be in response to vendor initiatives (e.g., installing patches or upgrades).
- Identifying and tracking new network components and their relationships to existing components. Maintain or change the configurations of network components as needed (e.g., when a device needs to be relocated).
- Scanning for viruses and other undesirable software.
- Copying all new or modified files from the station to a network backup device.
- Powering on or powering off the station. For instance, after configuration changes, the shutdown and restart of the device is required.
- Updating the basic input output system (BIOS).

Management software also can be used to notify network administrators of component failure in a station. In some cases, the software can detect and report any attempt to remove components, reducing the possibility of theft or unauthorized modifications. This can be of significant importance when applied to ESS devices as they are frequently the target of vandalism.

Network management software plays an additional role in monitoring the network to ensure its desired operation. For example, a managed hub can be monitored and controlled using network management software. A network administrator can observe traffic conditions and collect operational status information on the hub as well as on all devices connected to the hub.

If needed, diagnostic routines can be initiated to discover the cause of a fault condition. All of these actions can be performed remotely through a centralized management console, which saves time by eliminating the need to physically inspect the units. This is most applicable if ESS systems are spread over larger geographic areas, making on-site repairs difficult, if not impossible (e.g., remote mounted cameras, motion detectors, other access control and monitoring devices installed in remote or hazardous locations).

Internet Protocol (IP)-Based Electronic Safety and Security (ESS) System Planning, Design, and Implementation Considerations, continued

Bandwidth and Quality of Service (QoS)

Bandwidth, commonly referred to as the transmission capacity of a network, is the amount of data that can be passed along a communication channel in a given period of time. Inadequate bandwidth can cause bottlenecks, retransmissions, failed transmissions, and inadequate system performance.

When a message to be transported over a network consists of digitized fragments of continuous speech, it is critical for the network to deliver all fragments in order and with minimum loss, error, or delay. Failure to do so subjects the receiver to a noticeable degradation in the quality of speech.

This type of traffic is characterized as both:

- Loss sensitive.
- Delay sensitive.

Because of these factors, digital transmission is not always compatible with networks originally designed for traditional data traffic between devices. To provide an acceptable level of service, an organizational network must be able to identify, prioritize, and dedicate resources to the traffic generated by voice and other network intense, mission-critical applications. Networks designed to support these applications can be described as IP QoS capable.

The term QoS describes any technology developed to manage network traffic. In all cases, the role of QoS is to provide a guaranteed minimum data transfer rate, latency level, or both to any network application for specified users. QoS is a set of resource reservation control mechanisms that are put in place to ensure that a transmission channel has a minimum amount of bandwidth dedicated to a device or application along with a maximum delay in transmission that can be tolerated. This is important, for example, in IP voice traffic or when streaming real-time multimedia applications (e.g., video surveillance), which require fixed bit rates and are delay sensitive.

When data packets are transmitted over a network, QoS mechanisms give higher priority to real-time data than non-real-time data (e.g., file downloads).

The ESS planner must consider the integration and implementation of the following three QoS tools throughout the network:

- Classification—Identification of the application and marking its precedence.
- Prioritization—Giving priority to the voice application over any other. To improve performance, a technique known as traffic prioritization can be used. Prioritization makes it possible to assign different levels of priority to the applications running simultaneously on a station. For example, an NIC can be configured to transfer data to and from an IP camera before processing messages from any other application.
- Policing or shaping—Dropping or decreasing the priority of high volumes of traffic.

 © 2012 BICSI®

Internet Protocol (IP)-Based Electronic Safety and Security (ESS) System Planning, Design, and Implementation Considerations, continued

Network Infrastructure

The network in the building should be installed in accordance with BICSI best practices. The IP network infrastructure allows devices to utilize power over Ethernet (PoE):

- Data and power are provided over one cable. Networked devices can receive power from a PoE-enabled switch or midspan through the same standard cable that transmits data and video.
- A midspan unit may be used to "inject" power onto the cable; installing a separate power line is no longer needed.
- The complexity and duration of installation are reduced by removing the separate power component.
- An uninterruptible power supply (UPS) allows the devices to function in case of power failure.

Internet Protocol (IP) Network Architecture

Overview

The intent of this section is to provide a basic overview of IP networks with descriptions of the types, components, and communication methods commonly used by ESS systems. The following topics are covered in this section:

- Types of networks (LAN, campus area network [CAN], metropolitan area network [MAN], wide area network [WAN])
- Open Systems Interconnection (OSI) Reference Model

NOTE: Refer to BICSI's *NDRM* for further details on the material covered in this section.

Types of Networks

Networks can be characterized using one or more technical or operational attributes (e.g., type of technology, number of connected users and devices). One common attribute used to categorize networks is geographic area or span where a network is labeled on the basis of the physical area it covers.

The most common types of networks in terms of geographic area from the smallest to the largest are:

- Local.
- Campus.
- Metropolitan (or metro).
- Extended (or wide area).

A LAN covers an area generally associated with some or all of the space within a building. In most cases, multiple work space devices are connected to centralized devices (e.g., switches, servers) to form a LAN. One LAN can serve a single department, multiple groups, or all users within a building. Cabling, wireless, or a combination of both can be used to link LAN devices.

A CAN is created by linking the LANs located in two or more buildings that are in close proximity to each other. Connections between the buildings can be made using cabling or wireless technologies.

NOTE: The term campus LAN is also used to describe a CAN.

A MAN is created by linking the networks located at two or more sites within a city. Connections can be made using cabling or wireless technologies with optical fiber cabling often used to link a customer's buildings to a facility operated by an ITS service provider.

A WAN is created by linking the networks located at two or more sites distributed over geographic distances that extend beyond the span of a single metropolitan area. These include links between cities, countries, and in the case of global WANs, continents.

 © 2012 BICSI®

Open Systems Interconnection (OSI) Reference Model

Communication on a network occurs at many levels (e.g., applications, diagnostics, device control). In 1978, the International Organization for Standardization (ISO) introduced a framework for classifying all of the processes associated with message exchange on a network. This framework is formally called the OSI Reference Model, but it is commonly referred to as the OSI model.

The objective of the OSI model is to provide a structured approach for the development of all types of networks. The model specifies the sequence of processes required for network message transfer between applications running on different systems.

NOTE: In this context, a system can be defined as two or more computers and the associated software, peripherals, operators, physical processes, and media that form an autonomous unit capable of processing and transferring data.

This broad definition of a system makes it possible to use the OSI model to describe any type of network, from a residential LAN to the Internet.

The OSI model uses an approach called layering to illustrate and explain the message exchange process. This approach divides the various functions and services provided by a network into discrete groupings called layers. In the OSI model, seven layers are used (see Figure 10.1).

Figure 10.1
Open Systems Interconnection Reference Model

Layer 7	Application layer
Layer 6	Presentation layer
Layer 5	Session layer
Layer 4	Transport layer
Layer 3	Network layer
Layer 2	Data Link layer
Layer 1	Physical layer

NOTE: A layer function can be described by number or by name. For example, the terms Layer 3 switching and Network layer switching refer to the same process.

Open Systems Interconnection (OSI) Reference Model, continued

In the OSI model, each layer provides services to the layer above while hiding from that layer the processes used to implement the services. Ideally, changes can be made to any layer without requiring changes to any of the other layers as long as the inputs and outputs of the changed layer remain the same. For example, specifications for transmission over optical fiber cabling can be incorporated into Layer 1 of an existing LAN technology without modifying operations in Layer 2. This makes it possible to take advantage of new technologies within a given layer without sacrificing compatibility with existing networks.

The layers in the OSI model are commonly described as being connected to each other in vertical form, also called a stack or protocol stack. The stack defines how network hardware and software interact at various levels to transfer messages between devices on a LAN and between LANs on an internetwork.

Protocol stacks have the following characteristics:

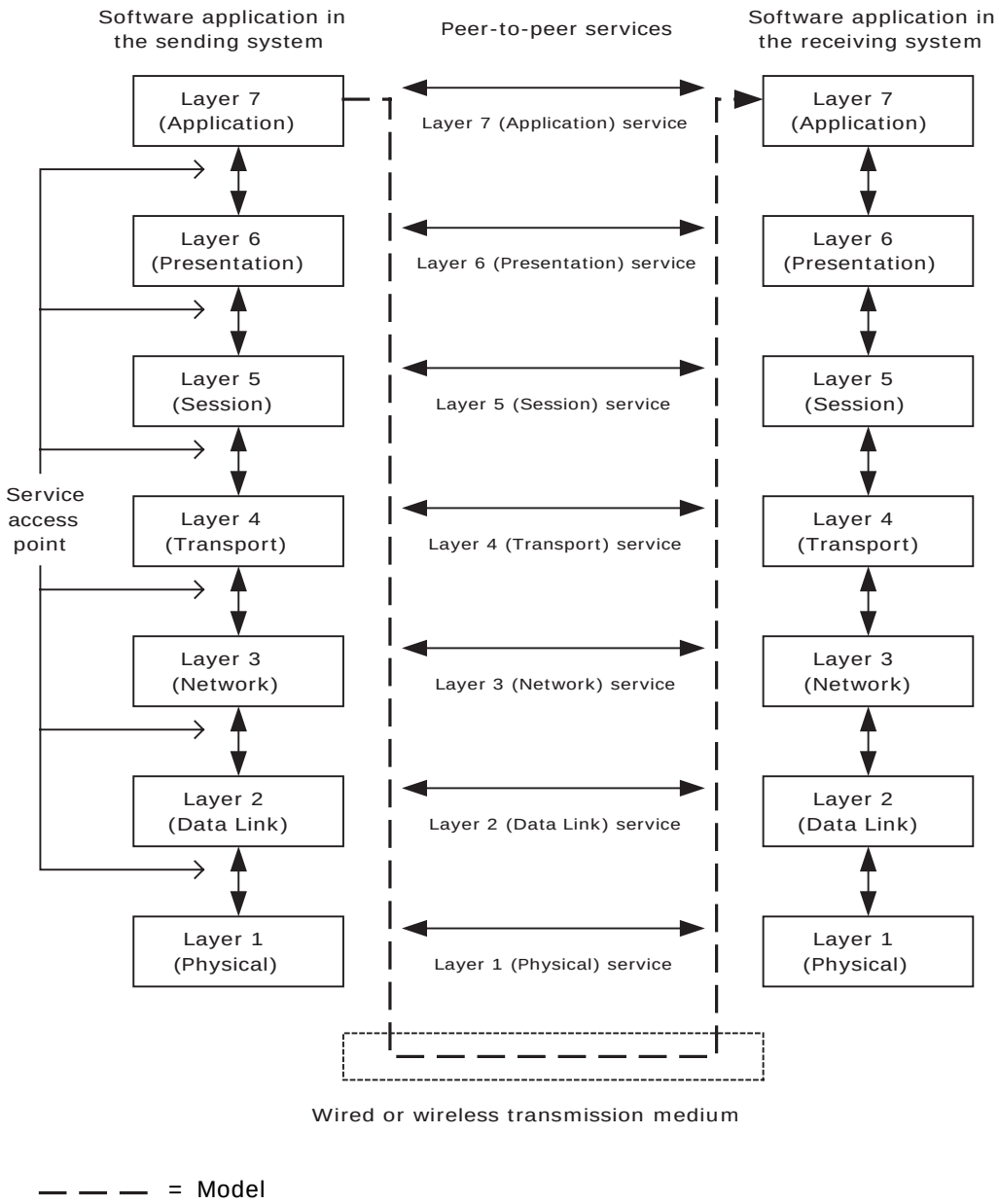
- Each layer provides a set of services.
- Services of each layer and the stack are defined by protocols.
- Lower layers provide services to upper layers.
- Service access points (SAP) are the connection points between layers.

When a message needs to be transferred between two systems, a peer-to-peer relationship is established between the corresponding layers in the protocol stack of each system—a given layer at one end communicates with its counterpart at the other end over the network. The message, along with any control information, is passed down from the sending layer to the layer below. This process continues until the lowest layer in the stack is reached. The data is then transmitted from the lowest layer of the sending system to the lowest layer in the receiving system where it is passed up through the layers until it reaches the counterpart, or peer, of the sending layer (see Figure 10.2).

 © 2012 BICSI®

Open Systems Interconnection (OSI) Reference Model, continued

Figure 10.2
Message transfer described using the Open Systems Interconnection Reference Model



Open Systems Interconnection (OSI) Reference Model, continued

Layer 7 (Application) Services

Layer 7 services make it possible for identical or nonidentical applications running on different systems to use a network to exchange information. Services defined by this layer include file transfer, message handling, and remote management. For example, various types and versions of e-mail software can use the same Layer 7 protocols to exchange messages over the Internet.

Layer 6 (Presentation) Services

Layer 6 services are responsible for various forms of data conversion. This layer negotiates and establishes a common form for data representation, which includes character code translations, data compression, and message encryption.

Layer 5 (Session) Services

Layer 5 services are responsible for synchronizing and managing data transfer between network devices. For example, a Layer 5 protocol can direct a device to start, stop, restart, or abandon data transfer activity.

Layer 4 (Transport) Services

Layer 4 services make it possible to assign various levels of quality to the data transfer process. When a connection is being established between network devices, the Layer 4 protocol can be used to select a particular class of service. This layer also can monitor the transfer for billing purposes, ensure that the appropriate service quality is maintained, and generate an alert if this quality has been compromised.

Layer 3 (Network) Services

Layer 3 services are responsible for internetwork data transfer (e.g., between LANs connected to the Internet). If multiple routes exist between the networks, a Layer 3 protocol can choose the most appropriate one based on such criteria as message priority, route congestion, or route cost.

Layer 2 (Data Link) Services

Layer 2 services are responsible for intranetwork data transfer (e.g., between devices connected to a LAN). Some of the functions of a Layer 2 protocol include device identification and managed access to a shared transmission channel.

Layer 1 (Physical) Services

Layer 1 services are responsible for the transfer of bits over various media.

NOTE: The OSI model does not explicitly define cabling or wireless transmission media.

 © 2012 BICSI®

Internet Protocol (IP)-Based Access Control Systems (ACS)

With the advent of access control over Ethernet, manual programming at each door controller is unnecessary. By using the power and ubiquity of the Transmission Control Protocol/Internet protocol (TCP/IP) network combined with systems that have the intelligence embedded at the door itself, hundreds or even thousands of access points can be programmed in minutes with new employee statistics and card key codes.

By streamlining this process, companies can systematically add employees or, at a moment's notice, keep a recently terminated employee from accessing secure areas of an operation. These capabilities in access control mark the next wave of a technical evolution in the security industry.

With the prevalence and ease of installation of IP networks, any technology that historically used a proprietary cabled communication protocol is subject to being migrated to an open standard Ethernet solution.

Cabling Infrastructure

The cabling infrastructure utilized for the IP-based ACS is the same as that for the data network. The common cabling system allows for significant savings in an IP-based ACS compared with a traditional system in the access control world. Emerging technologies are pushing traditional cabling out to the edge device. Some systems still maintain the multiconductor/multipair cabling approach.

Communications

Edge IP summarily compliments access control much like IP cameras enhanced the surveillance world.

With the use of edge devices, the software can now talk directly to the edge device through the network. The use of a master control panel with multiple subpanels is slowly being phased out. This concept is similarly used in IP video where the digital video recorder (DVR) is in a common location. As a result, both video and access control can now be truly scalable in increments of one access point with a relatively consistent installation cost.

An IP-based system utilizes a common user interface. A common user interface allows for an easier installation and provides for operator ease use. A common interface does not require multiple system administration functions or other management tasks. A single user login provides simple and secure access to all security functions. IP-based ACS network devices can all be managed by a corporate network management tool.

In most cases, IP access control costs less than traditional access control topologies. Cost savings occur not only in the cost of the devices themselves but also in the cost to run and maintain the associated wiring. With traditional topologies, a bundle of cables is run from a telecommunications room (TR) or an equipment room (ER) to the door. This wiring is run separately from the other communication wiring in a building and is singular in purpose. With IP access control, the wiring to the door is the same wiring used for the computers, telephones, and IP cameras. Combining the access control communication cable installation into a larger wiring contract leads to a lower cost per door.

Expandability

IP-based distributed processing allows for modular and economical system expansion. An IP-based ACS supports integration as a means of migration from legacy systems and provides a cost-effective solution with a clear path to future upgrades. IP-based ACS door system manufacturers ensure a consistent product version and consistent upgrade path.

Training and product support also take on a more focused approach without requiring the end user to act as a navigator and mediator between various manufacturers. An IP-based system also ensures the latest standards-based software, networking, and hardware technology.

Another difference between IP-based ACS control and traditional access control is the issue of PoE. On the positive side, most network rooms already have emergency power to the network devices that will continue to operate even when power to the building is lost while traditional power requires battery backup. PoE provides the same advantage to the IP access approach. One issue faced by the IP-based ACS designer is power to the locking device that may be required to unlock at loss of power to the building in order to meet applicable codes. It is more likely that installers will use PoE for the reader and REX device, but power to the locks will be provided from a separate power source.

Reliability

Depending on the configuration of the hardware, IP-based ACS control is as reliable as, or even more reliable than, the traditional topology of multireader controllers. With multidoor controllers, a single point of failure could cause multiple doors to become inoperable. With IP-based ACS control, each door is independent of other doors, so a single point of failure will only cause one door to be inoperable. Today's networks can be designed to allow for layers of resilience, so even if a network component fails, backup communication paths can reroute the event transmissions around the problem component.

In today's corporate environment, the network gets monitored and enhanced more frequently than it used to simply because of the critical nature of the information and system support the network is providing to the business. The network is typically carrying the information that keeps the company functioning.

As long as IP access still has power, the only impact of network communication failure is that the events will not be transmitted to the host application when the events occur. The IP-based ACS device still functions and employees can still enter while all the events continue without consequence. Once the network communication path is reestablished, all events that took place during a power or system lapse will be transmitted to the host. The loss of communication is a universal problem that affects both Ethernet and serially connected devices uniformly.

Management

With the evolution of IP-based ACS, management has become easier. The IT department can establish a virtual LAN (VLAN) to isolate the access control traffic as well as client accessibility. By allowing the IT department to manage and maintain the ACS, software upgrades are easier and more consistent as the IT department regularly performs scheduled software and hardware upgrades.

 © 2012 BICSI®

Internet Protocol (IP)-Based Video Surveillance Systems (VSS)

Characteristics

Devices that stream video over IP networks transmit frames and packets of video data to a single location or multiple locations for different purposes. A network video camera or multichannel video encoder can send a video stream to a single network video recorder, video decoder location, or multiple locations of the same type of equipment.

Even though the transport is standardized with IP video, each manufacturer uses a special version of a video compression engine in the video source that must be decoded by the recording and control system. In order to transmit and store video images practically and efficiently, it requires compression before it can be transmitted or recorded. The more the images are compressed (more information has been discarded), the lesser the quality.

Motion-Joint Photographic Experts Group (M-JPEG) video compression is commonly used in IP video cameras. The camera captures still images and compresses them into Joint Photographic Experts Group (JPEG) format. A camera can capture many images in one second (e.g., 30 frames per second [f/s]). These images can then be transmitted over the network and viewed in sequence so they appear similar to a movie. However, each frame is a fully detailed still image that may be relevant for admissibility in court. Moving Picture Experts Group (MPEG)-4 compares two compressed images, the first being used as a reference. It then transmits only the parts of the second image that have changed compared with the reference.

The latest iteration of MPEG-4 is MPEG-4 Part 10, H.264, which is the most efficient compression technology to date and the most resource intensive to decode and display. However, the efficiency of H.264 compression makes this technology suitable where content from real-time video streams needs to be stored and retained for long periods of time.

With a network infrastructure in place, there are lower installation costs when PoE (IEEE 802.3at) devices are used, eliminating the need for and vulnerability of localized power supplies.

The ESS designer is encouraged to use professional imaging over networks using the most qualified and professional product possible. Making the video available to as many users as possible who have permission to view and control the video streams is a goal of the IP-based video system.

Characteristics, continued

Prior to the IP video system deployment, the ESS designer should consider:

- Developing a comprehensive performance specification for a video-based surveillance system.
- Publishing a network video commissioning statement to specify the system deployment that includes:
  - Step-by-step staging, programming, installation, and commissioning tasks.
  - Division of responsibilities.
  - Acceptance test criteria.

The security contractor or whoever is commissioning the IP video system should consider the following tasks:

- Make resolution adjustments, as required, to meet end user requirements and revise IP video camera bandwidth maps.
- Verify recording, control, and management system design.
- Verify recording system performance and utilization with a full set of users and IP video streams.
- Ensure that users have the live and recorded image quality they need.
- Check common network usage scenarios with the IP video system:
  - Record system utilization with recording streams and monitor users.
  - Network switch functions to support bandwidth load and failure scenarios.
  - Provide recovery from the most common and reasonable infrastructure failures.
  - Simulate as many network conditions and loads as possible for components, edge devices, and infrastructure.

 © 2012 BICSI®

Internet Protocol (IP)-Based Voice Communication Systems

Overview

With the continued convergence of traditional voice communication with IP-based data networks (voice over Internet protocol [VoIP]) comes emerging technologies to converge other voice communication systems onto the IP network.

The following are some examples of voice communication systems that have begun to utilize the IP network in varying degrees:

- Telephone systems
- Mass notification systems (emergency voice/alarm communication)
- Wireless telephone communication systems
- Public address systems

Of these systems, the only voice communication systems that will be used primarily for the safety and security of the occupants are mass notification and public address systems.

Mass notification systems and overhead paging systems are virtually identical in function, but they often use different technologies and are regulated differently.

Characteristic IP speakers may have volume output levels changed over the IP network if sound levels require or if there are moves, adds, or changes (MAC) to the utilization of the space. This is easier than changing the taps on a transformer or changing wiring after installation.

Using PoE, only one cable would need to be run to the device (with both power and signal wiring run on one network cable). This is in contrast to the daisy-chained signal cabling requiring separate power cabling.

Traditional constant-voltage systems are often required to be installed in conduit because of electrical codes. IP-based cabling may almost always be installed without conduit by using J-hooks and cable trays.

Some local and national codes require a mass notification system for high-rise buildings. That system must be approved by a nationally recognized testing laboratory (NRTL). This means that the entire IP network using switches and routers (if needed) would be required to be listed. It is difficult for mass notification systems to use IP networking, often making these systems have their own isolated network.

Overview, continued

Cabling for traditional constant-voltage systems often is done with all cabling for one zone connected on one line from the amplifier (daisy-chained together). Cabling for IP systems requires that each device be connected directly to the data network in a star topology (homerun to the TR) and requires more cabling.

Cabling for traditional constant-voltage systems often is done using one amplified signal (no need for separate local power supply wiring and signal cabling, but only one twisted-pair cable).

Using IP systems, there must be both data cabling and power supply wiring to the speaker/device in the following situations:

- If PoE is not utilized
- If using optical fiber cabling
- If the power required for the speaker exceeds the PoE limit

System Architecture

There are multiple ways to utilize the data IP network for paging. Two distinct scenarios are the end-to-end IP system and many hybrid IP systems.

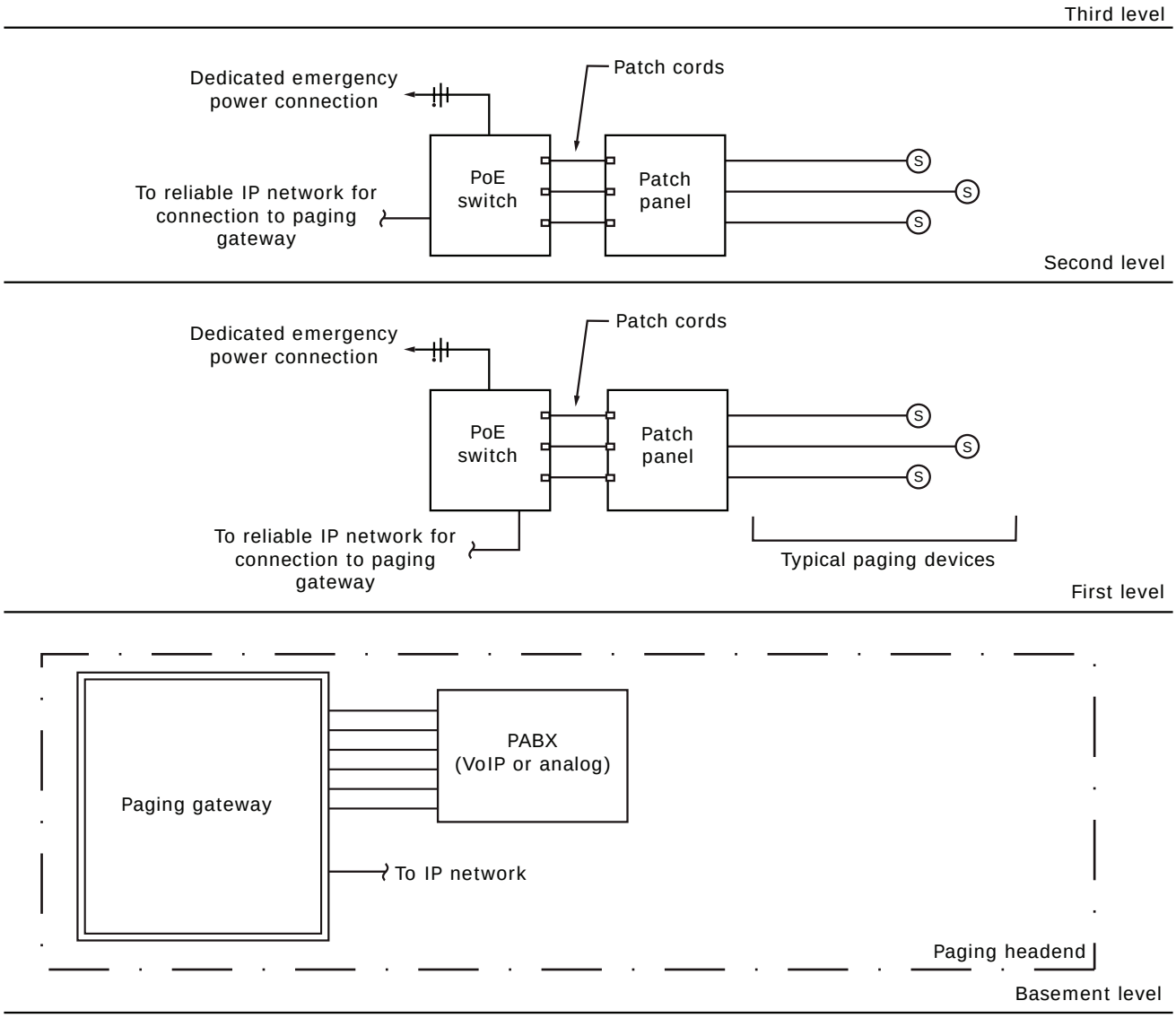
End-to-End Internet Protocol (IP) Paging Systems

End-to-end IP paging systems have all devices connected directly to the data IP network (see Figure 10.3). This provides ultimate flexibility in volume levels, zone reorganization in the event of MAC, and reused cabling.

 © 2012 BICSI®

System Architecture, continued

Figure 10.3
End-to-end Internet protocol paging system diagram



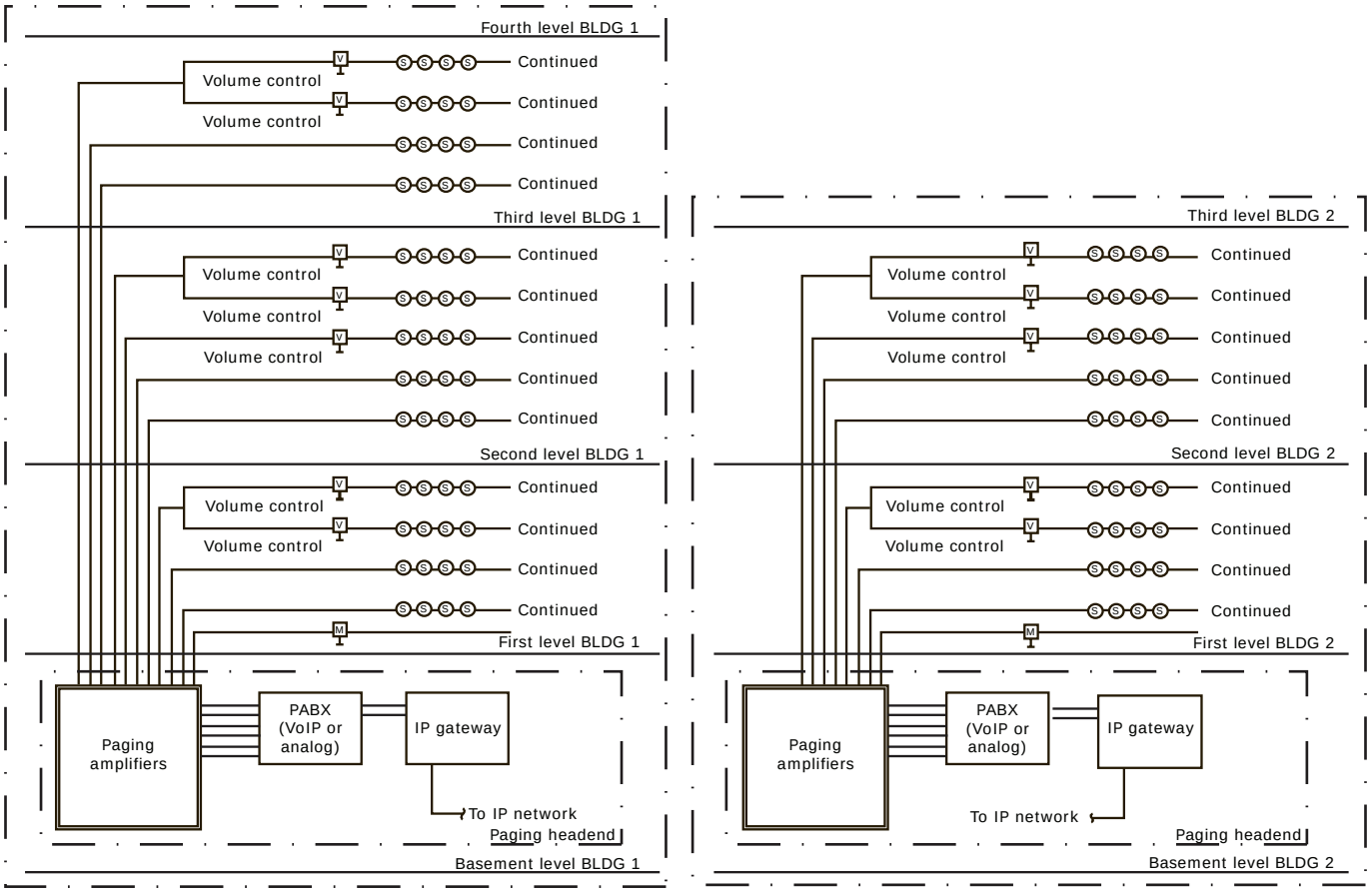
Ⓢ = Ceiling-mounted speaker
IP = Internet protocol
PABX = Private automatic branch exchange
PoE = Power over Ethernet
VoIP = Voice over Internet protocol

System Architecture, continued

Hybrid Internet Protocol (IP)/Traditional Paging Systems

There are many ways to provide an IP-based connection between components in a paging system (see Figure 10.4).

Figure 10.4
Hybrid Internet protocol/traditional paging system diagram using an Internet protocol backbone



Ⓢ = Ceiling mounted speaker
HM = Microphone outlet
HV = Volume control unit
BLDG = Building
IP = Internet protocol
PABX = Private automatic branch exchange
VoIP = Voice over Internet Protocol

 © 2012 BICSI®

Determining System Capacity

In traditional paging calculations, the maximum number of simultaneous pages (as required by utilization of the facility) is determined. In IP-based systems, the same number of simultaneous pages may be used for bandwidth calculations.

Each simultaneous page would typically require about 140 kilobits per second (kb/s) per channel. There is a large amount of diversity in this paging requirement, so this requirement is conservative.

The following formula may be used:

(# of simultaneous pages) × (140 kb/s) = Total bandwidth required at the IP gateway

The required bandwidth within the IP network may decrease proportionally the farther the device is from the paging gateway because of the zones. Farther zones from the paging gateway will not be competing for bandwidth from zones that are closer to the paging gateway. Closer paging zones will transmit to the farther zones only by way of the gateway. This is similar to a water pipe from the city. The closest main pipes to the water tower are the largest, and the main pipes farthest away are the smallest.

Always verify the bandwidth requirements with the manufacturer to obtain the most accurate results.

Miscellaneous Systems Utilizing Internet Protocol (IP)

Overview

Some ESS systems are not conducive to utilizing IP exclusively.

For some systems, the obstacles have been overcome by the benefits of common cabling, common devices, available installers, increased system management, open and accepted protocol, and increased flexibility. Some ESS systems that have begun to converge include access control, video surveillance, and voice communication systems.

The following systems will be discussed to determine if there is any IP utilization and whether they are impeded from IP convergence:

- Fire alarm (FA) systems
- Intrusion detection (burglar alarm) systems (IDS)
- Nurse call systems

Characteristics

IDS, FA systems, and nurse call systems are often challenged with hurdles to a converged IP solution (see Table 10.1).

Table 10.1
Challenges to Internet protocol migration

IP-Based Systems	Traditional Systems
Larger cabling quantities	Smaller cabling quantities
Newer technology not readily used	Incumbent technology already used
NRTL-listed system difficult to define	NRTL-listed system is easily defined
Power transport limited by PoE	Power transport of virtually any size
Shorter cabling distances	Longer cabling distances
Star cabling topology	Daisy-chain/ring cabling topology
VPN perceived as insecure	Separate network perceived as secure

IP = Internet protocol
NRTL = Nationally recognized testing laboratory
PoE = Power over Ethernet
VPN = Virtual private network

An obstacle for these systems is the requirement that the system be an NRTL-listed system for installation in a commercial building. The NRTL requirements typically require the system to operate as a separate system entirely from all other systems. Refer to applicable codes, standards, and regulations for each project.

 © 2012 BICSI®

System Architecture

Fire Alarm (FA) Hybrid / Internet Protocol (IP) System

NOTE: For FA systems, always refer to applicable codes, standards, and regulations for each project. Requirements vary largely from city to city and will determine the feasibility of utilizing IP for any parts of the system.

FA systems are typically the most protected communication systems in any particular building. The requirements are typically heavily regulated because of the life safety nature of the system. An FA system must function in an emergency because it protects the safety of human life.

The use of any IP for any communication was previously discouraged or not allowed. With the advancement of TCP/IP technology and increasing reliability of this IP network, IP use has been allowed in some jurisdictions.

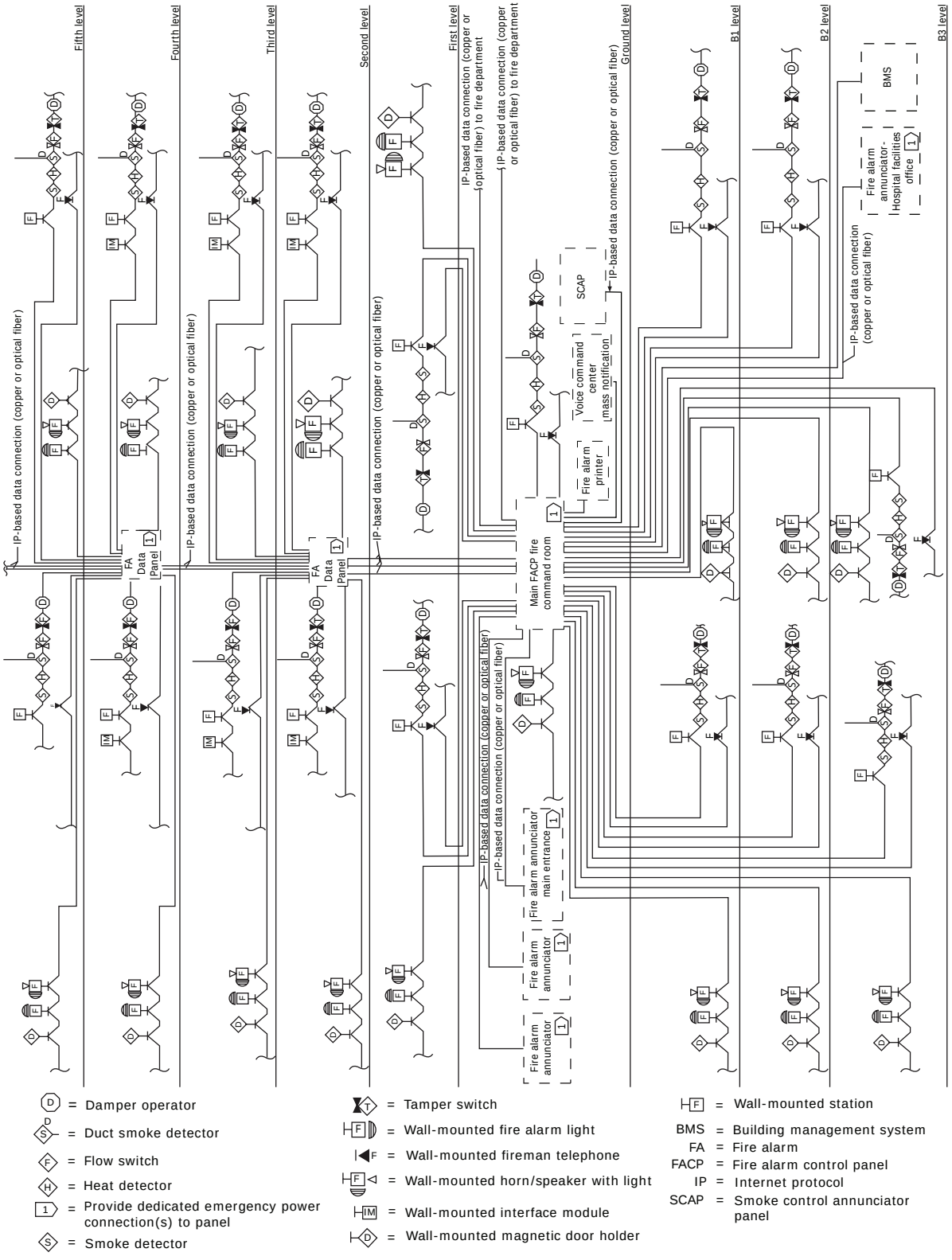
Some examples of how a system could be organized that utilizes IP communication include the following (see Figure 10.5):

- IP backbone between panels—Typically requires a separate dedicated FA network of switches and backbone cabling. This is isolated from the data IP network.
- IP connection for monitoring between buildings—Uses data IP network.
- IP connection to the fire department for alarm notification—Uses data IP network (typically with many requirements on the network).

NOTE: Figure 10.5 is simplified and does not show the switches and network topology of the IP connections, but it illustrates that a connection occurs.

System Architecture, continued

Figure 10.5
Hybrid Internet protocol/traditional fire alarm system diagram



 © 2012 BICSI®

System Architecture, continued

Intrusion Detection (Burglar Alarm) Hybrid / Internet Protocol (IP) System

An IDS typically is used to protect the assets of a building when no occupants are present (see Figure 10.6). An IDS sometimes is called a burglar alarm system because the notification of a possible burglary is the most prominent use of these systems.

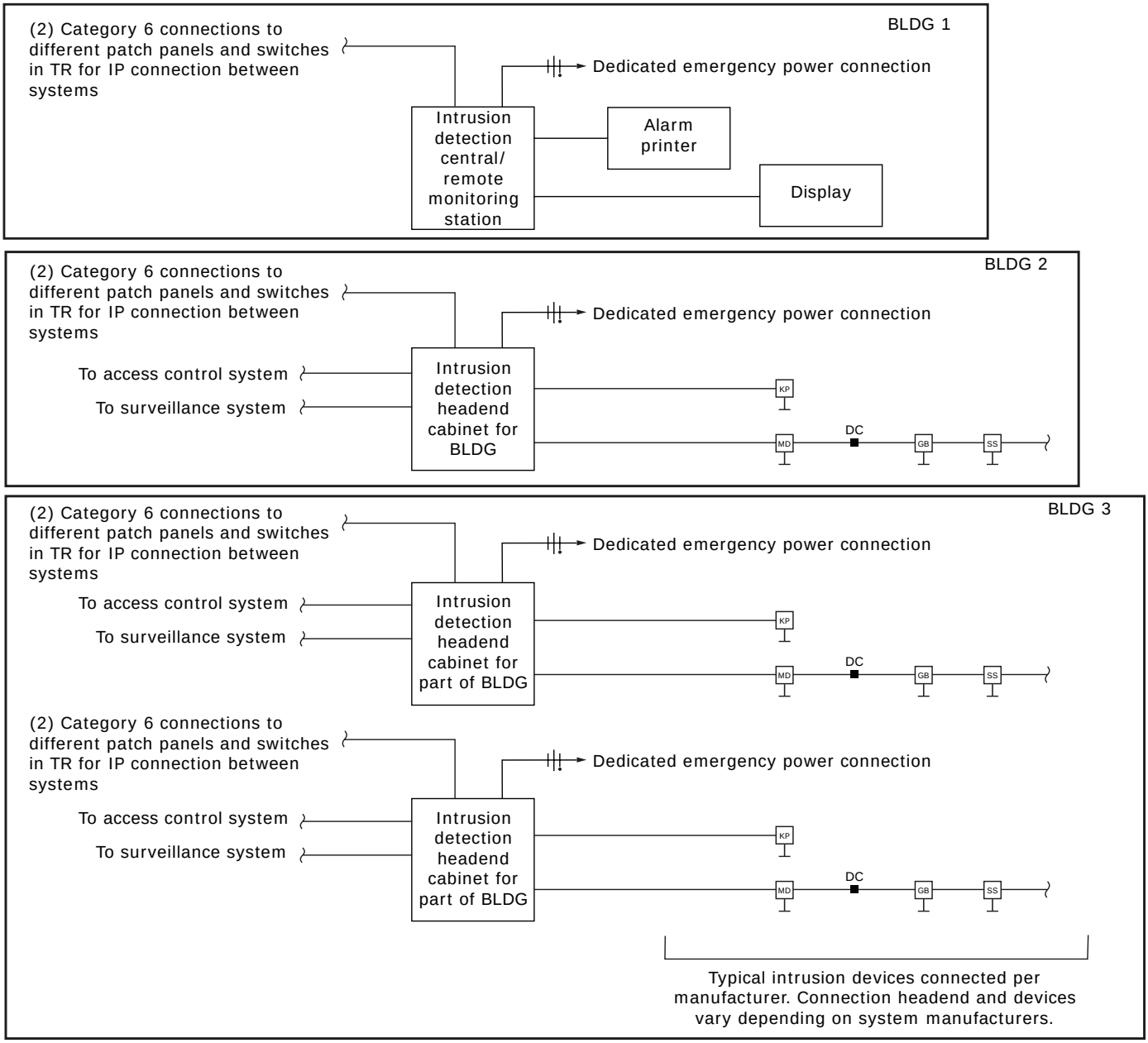
The device is not typically IP based, but there are applications of systems to have an IP-based connection between multiple headends of systems.

The following are ways that a system could utilize IP communication:

- Campus—Between headends in each building and as a connection to the central/remote monitoring.
- Single owner of multiple buildings—Between headends in each building and as a connection to the central/remote monitoring.
- Single building with a single owner—As a connection to a remote monitoring service.

System Architecture, continued

Figure 10.6
Hybrid Internet protocol/traditional intrusion detection systems diagram



■ DC = Ceiling-mounted speaker
⊢KP = Microphone outlet
⊢MD = Volume control unit
⊢GB = Glass break sensor
⊢SS = Shock/pressure sensor

BLDG = Building
IP = Internet protocol
TR = Telecommunications room

 © 2012 BICSI®

System Architecture, continued

Nurse Call Hybrid / Internet Protocol (IP) System

There are two major utilization methods for IP-based communication for a nurse call system (see Figure 10.7):

- One method of communication between nurse call systems (the headend in each area) connects the large-scale code calls between the systems.
- The second method is to have all nurse call devices be IP based on a separate stand-alone nurse call network with backbone cabling, switches, and a connection to the data IP network only where an IP gateway is allowed.

Determining Internet Protocol (IP) System Capacity

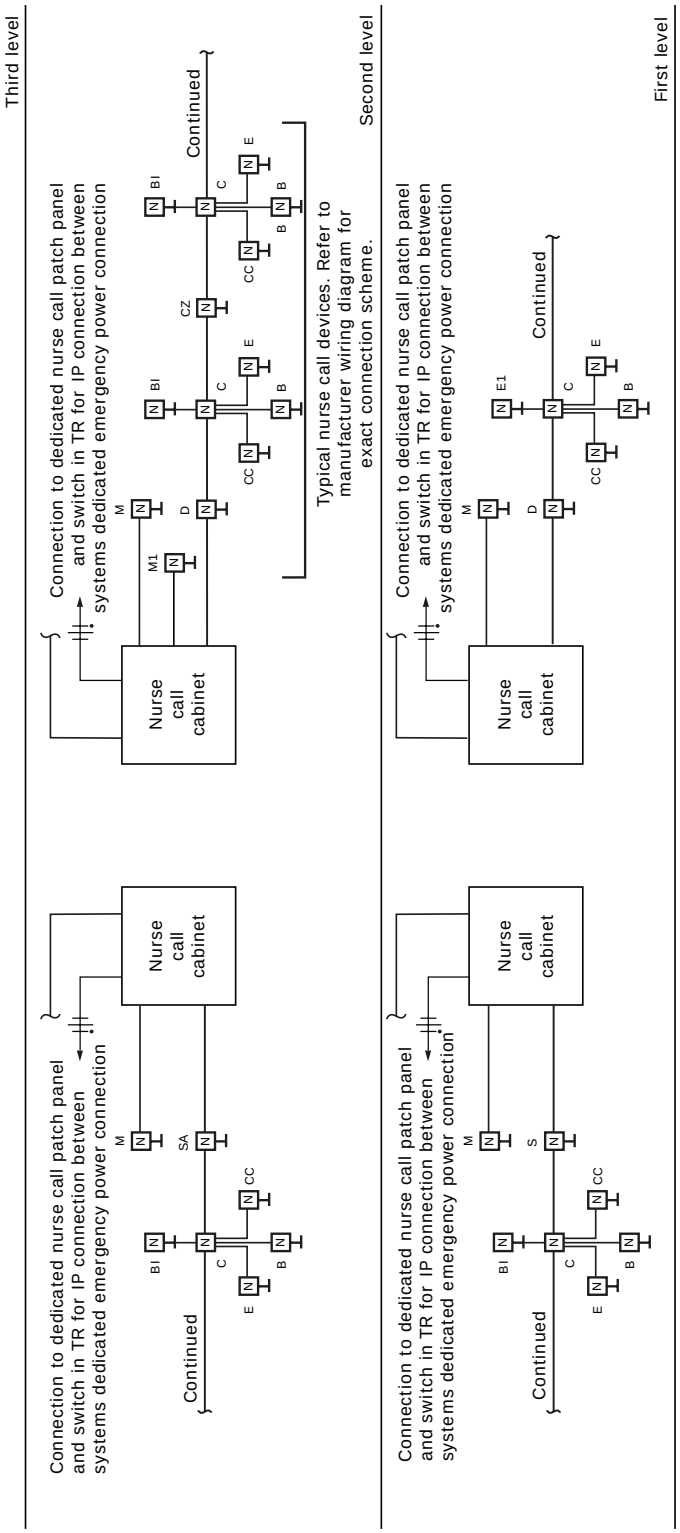
Most IP-based communication devices for these safety and security systems should have a dedicated IP address. A dedicated address allows for supervision of each device with ease and security.

Most devices and communications of this type (text communication) do not have significant bandwidth requirements. Any voice communication requires verification of existing bandwidth capabilities of the data IP network. If used, the voice that is run over an IP network for a nurse call system is through a dedicated nurse call IP network or through dedicated voice communication cabling.

A dedicated network with text and voice for a nurse call system would not typically exceed the available bandwidth on most 100+ megabits per second (Mb/s) networks. Verify all requirements for systems with the system manufacturers to obtain the most accurate requirements for the network.

Determining Internet Protocol (IP) System Capacity, continued

Figure 10.7
Hybrid Internet protocol/traditional nurse call system diagram



 © 2012 BICSI®

Network Security

Overview

This section provides a broad overview of threats and countermeasures for network security as it relates to IP-based ESS system design. It is not intended to be a comprehensive or detailed source on the subject of information security (InfoSec), which is a rapidly evolving discipline. After reading this section, the reader should be familiar with the terminology necessary to intelligently discuss the specific requirements for network security with competent professionals.

Historically, ESS systems were physically isolated and relied upon point-to-point (PTP) communications. To gain improvements in efficiency, ESS systems began to migrate to network-based communications and grow external connections. Many were designed prior to the wide-scale adoption of network security products and practices, and unfortunately, most lacked adequate consideration of and protection from network attack. This trend has evolved for myriad reasons, and now ESS systems are often connected to the Internet.

Connecting an ESS system to any external network, either a corporate network or the Internet, whether directly or indirectly through a corporate LAN and its firewalls, makes it vulnerable to network attack. Security measures are necessary to mitigate and manage these vulnerabilities but often cannot totally eliminate them. Along with this connectivity, some level of risk must be accepted. Total isolation from non-ESS networks is the only means of making an ESS system impervious to network attack. Admittedly, such isolation comes with a high price and may be unworkable. Therefore, it is necessary for the ESS designer to understand the risks in interconnecting the ESS network and to discuss those risks and potential countermeasures with competent professionals before finalizing a design.

The primary objectives of network security are the confidentiality, integrity, and availability (CIA) of the protected assets. Threats against CIA can create risk. Risks are determined by factoring the threats and vulnerabilities along with impact:

$$\text{Risk} = \frac{\text{Threat} \times \text{Vulnerability} \times \text{Impact}}{\text{Control measures}}$$

Control measures are applied to mitigate risks. The perception of risk varies based on the importance of the data or function of the network. The acceptable level of risk that can be tolerated is explicitly determined by the organization. The definition of acceptable risk levels and appropriate controls is typically outlined in a security policy.

Overview, continued

A security policy should normally address the following issues:

- Privacy—Guidance to users on the importance of limiting information to individuals who need to know.
- Acceptable use—Network activities that are considered acceptable within the organization at a user, department, office, or organizational level.
- User and network node authentication—Definition of systems responsible for identifying validation credentials. This typically is part of the operating system supporting the network and can be augmented by additional security measures as required.
- Data protection—Virus, spyware controls, encryption, and portable storage device management (e.g., universal serial bus [USB] thumb drives, portable drives, tablets, smartphones, laptops).
- Internet usage—Definition of what constitutes proper business use of Internet resources.
- Data access—Assignment of appropriate access to data based upon function within the organization.
- Policy compliance—Consequences of the failure to comply with all network policies and definition of steps taken to ensure compliance.

Each of these policies is intended to address a specific set of risks. These policies also incur a cost to the organization that must be recognized and balanced against the potential impact of a realized risk. Additional hardware and software required to implement the policies, associated labor to maintain systems, and operational constraints impacting potential customer interaction must be considered when designing network security policies.

 © 2012 BICSI®

Risks

The purpose of ESS systems is to reduce risk in the physical and logical environments. If the underlying components are compromised, the overall system does not fulfill its purpose. Several scenarios could undermine ESS systems as illustrated by the following threats and associated organizational impacts.

Denial of Service

As a function of resiliency, some IP-based ACS operate under cached information in the event of a network outage. If a network outage is forced by a denial of service (DoS) attack, this could allow an individual with revoked access to enter the facility.

In an effort to reduce costs, some facilities have reduced the number of security personnel in favor of IP-based cameras, centralized monitoring, and digital video recordings. If IP-based video cameras cannot be reached, activity in those areas is not monitored, and the data could be lost, making physical breaches virtually invisible.

Such risks are not limited to IP-based camera networks. Nearly all modern security DVRs (including ones that do not support IP cameras) offer remote monitoring from a user's handheld or desktop device over the Internet. Some of these systems can be compromised by a relatively modest DoS attack, allowing hackers time to gain physical access to a location while the camera images are not being recorded.

DoS attacks are often distributed across hundreds or thousands of computers, often part of a botnet, in a distributed denial of service (DDoS) attack. Such attacks are more difficult to defend against because they can originate from so many sources.

Replay Attacks

If logical access to the network is available, transmitted data can be captured, manipulated, and replayed. The data could be a system authentication, the addition of an access card, approval for access into a restricted area, or pausing of a surveillance recording. Any of these events could provide access to an unauthorized entity.

Spoofing

Closely related to replay attacks are spoof exploits, where a hacker impersonates a device or user who has authorized access. Such attacks are easier on systems with weak or nonexistent authentication or ones relying on security through obscurity—the hope that attackers will overlook or not be aware of a particular vulnerability because a system is not widely used.

Backdoors

Systems often are shipped with service or administrator accounts with easily guessed (or nonexistent) passwords. Such easy backdoor access is often overlooked, particularly in physical security systems that are assumed to be inaccessible from the outside world.

Malicious Codes

Malicious codes, including viruses, worms, or Trojans, can disrupt services and undermine CIA. The result is an ESS system that does not meet its design intent. In the context of the ESS system, the devices are typically application specific and on an isolated network. This significantly limits the exposure to malicious codes, but the risk still exists.

System Control

If physical access to equipment or network connections (including wireless) is available, new hardware could be introduced or the system compromised. This includes remote access to maintenance modems discovered by war dialers. War dialers allow an attacker to discover open modems by entering a telephone number range and allowing the tool to systematically call each number.

With physical access, keystroke loggers can be installed to capture passwords and transmit them wirelessly or over the Internet. Several websites are dedicated to listing default passwords for any device imaginable, including security systems. With the correct password, an attacker can redirect video cameras, delete data or security log files, add new access cards, and perform other functions normally protected by security control processes.

Even changing the default password of a device is no guarantee. Brute-force attacks or dictionary attacks guess thousands of passwords a second until the correct one is found. On devices that do not limit password retries (e.g., three attempts before lockout), there may be few or no indications that an attack is in progress.

Spoofing or impersonation of legitimate devices (e.g., wireless access points) also can be used to compromise a security system. Such man-in-the-middle attacks might occur at a shared resource, such as a fake coffeehouse wireless fidelity (Wi-Fi) connection, where user credentials might be scanned as they are entered by an unsuspecting user.

Logs can be interrupted when another device claims the IP address of the log server.

Social Engineering

Humans have a built-in mechanism to be friendly and trusting. Social engineering is the use of pretext to exploit this cooperative nature and obtain information or influence action. Social engineers also may employ intimidation and impersonation as well as snooping and eavesdropping.

An example of social engineering is a telephone call to a user from a person falsely identifying himself or herself as a network support person needing the user's user identification and password to troubleshoot a network issue. In many cases, the user will provide the data without a second thought.

 © 2012 BICSI®

Phishing and Spear Phishing

Another type of social engineering is phishing, where unsuspecting users might receive apparently legitimate requests to validate their login credentials and that offer a convenient button to do so. Phishing attacks are often seen as fraudulent e-mails or entire websites, which often appear legitimate to the victim. Phishing attacks tend to be fairly widely targeted (e.g., customers of a particular bank, government agency, private company). As security systems become more commoditized, it is not unreasonable to expect such attacks to target them as well.

Spear phishing refers to specifically targeted attacks against a small group or a single individual, often with detailed information to make the message or website look even more trustworthy. Such attacks are usually one in a series of measures to gain access to high-value targets, such as company websites, which are then ransacked.

Mobile Devices

Increasingly, users are requesting access to security networks from their handheld and portable devices. Inexpensive security camera systems advertise that they can be monitored from handheld devices. Such distributed access also represents a distributed threat, introducing the potential for many more attack risks, particularly if clients store their access credentials on the device.

Insider Threats

The most damaging impact often comes from authorized users that abuse their access. The system administrator can start maintenance and shut down important systems at an opportune time to allow accomplices to breach the perimeter unseen. Either scenario can negate the expensive ESS infrastructure and bypass the expected controls.

Control Measures

Overview

The practice of securing information has many parallels to the primary domain of this manual, physical security. In physical security, the countermeasures serve to deter, delay, or detect attacks on assets. Physical security designers may deploy various countermeasures intended to discourage potential attackers, slow them down, or detect the attacks in real time before the assets have been compromised.

The equivalent of physical security's countermeasures in the InfoSec world is security controls or control measures. As discussed in this section, control measures are put in place to provide layers of protection for the information assets they are intended to shield from vulnerability and compromise of CIA from cyber attacks.

It is important to understand that just like a physical structure (e.g., home, business), the architecture of the network, computing, or storage device will invariably affect its vulnerability. As terminal server and mainframe systems have been shifted to client/server architecture, data has been exposed to risk in increasing levels. Client/server environments create more data in motion that can be stolen, delayed, or damaged. Cloud computing, software-as-a-service (SaaS), and service-oriented architecture (SOA) systems provide even more potential for risk since the computing assets may not be under the control of the purchaser.

Data being stored or processed on systems outside of the security of the computer room or data center is subject to hacking or unauthorized access. Because sensitive files are stored on workstations and laptops, the physical theft of a central processing unit (CPU) or laptop often can allow an attacker to browse and decrypt files containing business or personal information without much risk of discovery.

The protection of information assets is not simple. Even more than physical security countermeasures, InfoSec is the interaction between people, processes, and technology. In contrast to physical countermeasures, InfoSec is the adaptability of the attack on data assets. Control measures are required to be pervasive and must involve an ongoing process of evaluation and revision.

The following sections provide an overview of technical control measures that are meant to protect information assets.

Firewalls

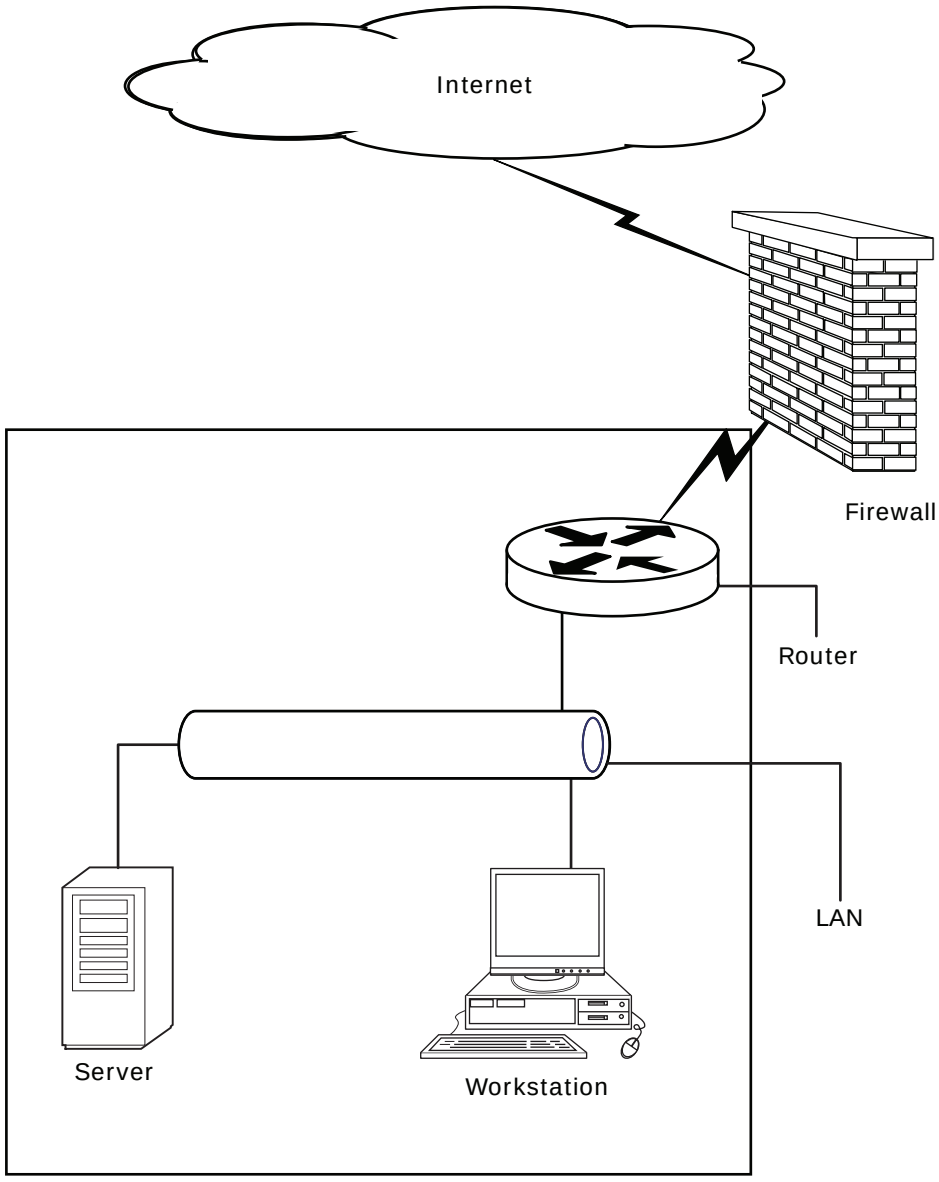
A firewall is hardware or software designed to keep unwanted and unauthorized traffic from entering a network or any computer attached to a network from an unauthorized device or network. A firewall's decision on what traffic to permit to enter a network or computer system is based upon the IP address of the device or network sending the traffic. Firewalls can protect stand-alone networks (see Figure 10.8) or enterprise networks (see Figure 10.9).

 © 2012 BICSI®

Firewalls, continued

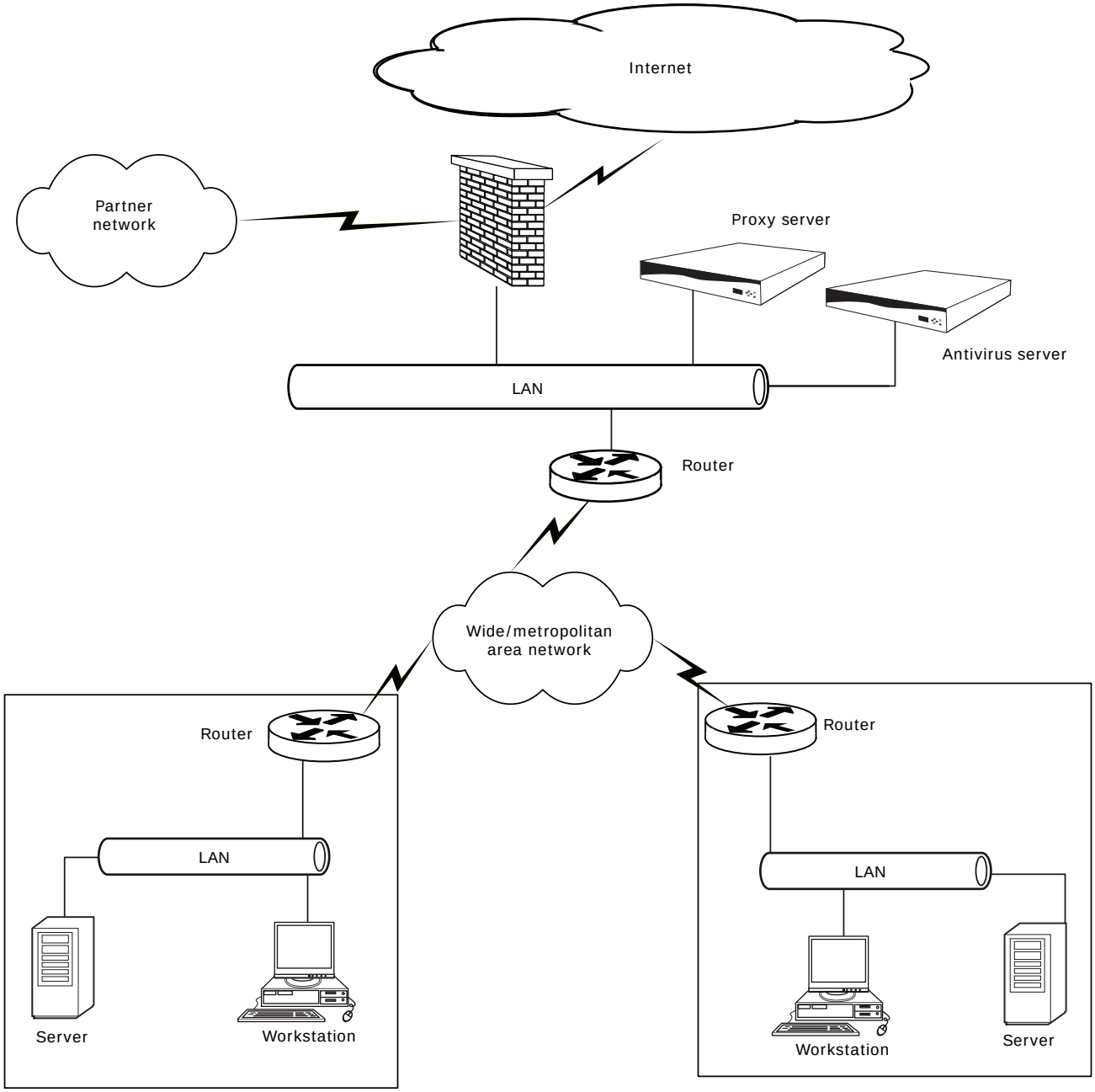
In an enterprise network, these decisions typically are based on policies implemented by the firewall administrator. The security policies implemented within a firewall can restrict what services are allowed to be accessed, specific IP addresses and ranges of IP addresses, and even what logical ports the firewall will permit network packets to access. Firewalls also can offer extensive reporting and tracing functionality.

Figure 10.8
Stand-alone network



Firewalls, continued

Figure 10.9
Enterprise network



 © 2012 BICSI®

Firewalls, continued

Firewalls are types of gateways that can be housed in servers, routers, specialized hardware devices, or software loaded on a computer. They work by examining network packets as they enter and exit the network. Those packets that do not pass the requirements configured in the firewall are filtered out and are not permitted to pass.

Modern firewalls filter traffic based on several network packet attributes, including:

- Source IP address.
- Source port.
- Destination IP address or port.
- Applications.
- Protocols (e.g., file transfer protocol [FTP], hypertext transfer protocol [HTTP]).
- Domain name of the source.

In general, firewalls can be grouped into the following three categories:

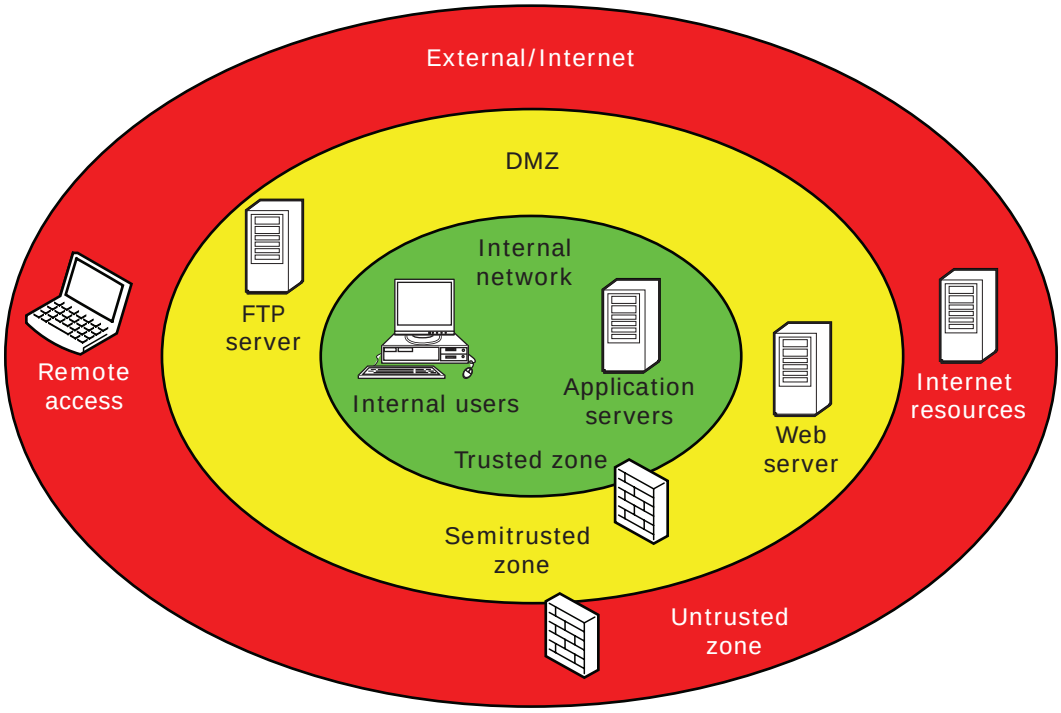
- A packet filter firewall examines each network datagram and uses an access control list (ACL) to determine if an inbound or outbound datagram should be discarded (filtered) or allowed to pass through the firewall. This type of firewall inspects addresses to determine what to filter.
- A circuit gateway firewall permits an inbound or outbound connection to take place on the basis of authentication and authorization criteria. This type of firewall does not inspect each datagram—once the user or device is granted access to the communications channel, it can send and receive any type of data.
- A proxy server firewall takes the place of another network device and initiates all communications on its behalf. The proxy server inspects all incoming and outgoing messages before they are forwarded to the destination. The devices at both ends of the connection never communicate directly—each communicates with the proxy server, which represents itself as one of the devices when communicating with the other.

Firewalls can be used to create security zones (see Figure 10.10). Each zone is associated with a level of trust such as:

- Untrusted—May include the Internet or other hostile networks.
- Semitrusted—May include a demilitarized zone (DMZ) or partner networks.
- Trusted—May include the corporate or enterprise network.

Firewalls, continued

Figure 10.10
Example of security zones



DMZ = Demilitarized zone
FTP = File transfer protocol

A DMZ is a network segment that operates as a neutral zone between a company's private network and the outside public network. It is intended to avoid direct communication between devices in untrusted zones with devices in a trusted zone. ESS devices (e.g., credential databases) should normally be in a trusted zone.

Users of the public network can only access devices in the DMZ. If an outside user compromised a device in the DMZ, only that device might be compromised, but other assets would not be directly at risk.

There are many threats for which firewalls do not provide effective control measures. Malware, ransomware, viruses, Trojan horses, and insider attacks are typical weaknesses of this type of control.

 © 2012 BICSI®

Intrusion Detection and Prevention Systems

While firewalls prevent potentially harmful traffic from entering the network, an IDS detects an unauthorized use or attack upon a network. Once an IDS detects a security breach, a number of actions are possible to mitigate the threat. Where the IDS can simply watch for attacks and report breaches, the intrusion prevention system (IPS) can protect system files. The IPS also is capable of working in concert with firewalls to reconfigure ACLs to actively block a subsequent attack (active IDS).

An IDS consists of three components:

- Sensors that collect traffic
- Analyzers that look for suspicious activity
- Administrator interface that collects output from the analyzer

There are two primary IDS types:

- A host-based IDS monitors activity within a specific computer.
- A network IDS monitors activity on the network where it is attached.

Network Segregation with Virtual LANs (VLANs)

To reduce the total cost of ownership, many facilities use the same network infrastructure for office automation purposes as well as security systems and industrial control. To follow the principle of isolation, it is important to provide some separation between these systems. One way to provide this separation without the need for additional LAN equipment is the use of VLAN.

Virtual Private Networks (VPNs)

Rather than purchasing PTP circuits for dedicated and protected bandwidth between locations, many organizations use virtual private networks (VPNs). Similarly, VPN point-to-multipoint arrangements allow one or many individuals to connect to an organization securely and privately, usually involving software on the client end and hardware on the enterprise end.

Access Control Lists (ACLs)

For facilities that do not have firewalls or the budget to add firewalls, it is possible to set up some restrictions using ACLs on routers and switches to limit traffic crossing these devices. The restrictions can be configured based on source and destination IP addresses as well as port numbers. The functionality is similar to firewalls, but without some of the deeper functionality or specific security design. Because these devices are not specifically designed for this feature, there may be an impact on throughput.

Network Admission Control (NAC) and Network Access Protection (NAP) Systems

Variously called network admission control (NAC) and network access protection (NAP), these technologies are intended to scan endpoint devices for vulnerabilities and patch levels before they are allowed to connect to a trusted network. Network admission systems or ACS typically address the ability of an unauthorized network device to attach to the LAN and obtain an IP address or communicate with other network devices. Many of these systems operate on the basis of IEEE 802.1X authentication with port access controls.

Dial-Back Modems

Dial-back modems mitigate the risk of unauthorized remote access by disconnecting from inbound calls and dialing back only numbers that have been preprogrammed. As modem use mostly has been replaced with Internet-based access, such devices tend to be rarer, although they act as a valuable control option during DoS attacks.

Network Behavior Analysis

Network behavior analysis systems capture information from traffic flowing over the network to determine the source and destination as well as the protocol and any anomalies in the traffic that might indicate malicious traffic. These systems can use direct packet capture or more often use NetFlow or sFlow data streams as input for the traffic information.

Vulnerability Scanners

Vulnerability scanners send specially crafted network traffic to devices on the network to determine the operating system, configuration, and patch status of each device. Sometimes, a login is used to determine additional information from the registry. These scanners identify vulnerabilities on the device (e.g., easily guessed passwords, missing security patches). Many systems include workflow software for follow-up of patching or configuration changes.

Server Hardening

Server hardening can be used to shut down any unused processes or irrelevant software modules on a device. The logic being that these processes may introduce vulnerabilities, and by removing the processes, the vulnerabilities are also eliminated. This precludes the application of some specific patches and can make applying the patches unnecessary.

 © 2012 BICSI®

Authentication Methods

Authentication uses one or more of the following three factors to validate identity:

- Something you know—Usually a user name and password
- Something you have—A security token, access card, or proximity detection device
- Something you are—Physical attributes (e.g., fingerprint, retinal scan)

Some methods are biometric based (something you are), including fingerprint readers, iris scanners, and voice recognition. These factors can be combined into a stronger authentication model (two factor authentication).

Software Patching

All software has flaws. Many of these flaws can be exploited to obtain access, elevate privileges, or leak information. When software developers become aware of these vulnerabilities, they typically create patches to the original software. These patches alter the original software in order to eliminate the vulnerability. Sometimes, these patches introduce additional flaws that may be more serious than the original flaw or may interrupt the normal function of the original software.

If the risk of poor quality patches is graphed over time in comparison to the risk of exploits against the vulnerability, there is an ideal point where the risk of applying new software intercepts the introduction of exploits targeting the originally flawed software. Because of the decreasing time to exploit releases, this time frame continually decreases.

For the reasons stated above, it is critical that all service packs, hotfixes, and other patches are tested on a nonproduction test network prior to implementation to ensure their predictable impact and adequate security.

Zero-day attacks (attacks that are exploited on or before the release of patches) are potentially the most serious as systems are effectively unprotected against them.

Antivirus

Antivirus software (and all anti-malware software) typically detects threats by comparison of files to signatures of known malicious code. As such, it is necessary not only to install the software but also to ensure continued updates to the virus signature database. This requires access to the Internet or to an internal system that maintains copies of all the updates.

Encryption

Encryption obfuscates the actual data to make it unreadable to anyone but the authorized users of the data. Data encryption is applied to data in transport through secure protocols (e.g., Internet protocol security [IPSec], applicability statement 2 [AS2], transport layer security [TLS], secure sockets layer [SSL]). Data encryption also can be applied to data at rest with specific software for whole disk encryption or encrypted folders. Access to the login credentials or an open system can undermine the use of encryption.

Security Information and Event Management (SIEM)

Security information and event management (SIEM) systems coordinate input from firewalls, network IDS, antivirus software, activity logs, and other security feeds to create a view of any security incident. This coordinated approach can provide better intelligence during an IDS alert. With improved information, it is possible to verify that the target system is patched and immune to the perceived threat.

Awareness Training

One valuable control tool against social engineering (e.g., phishing attacks) is awareness training. This training should target system users as well as administrators so that they know what data or processes are sensitive and could undermine the overall system security. This will assist in recognizing attempts to gather important information and detect pretexts.

Background Checks

People who operate and maintain networks should be scrutinized as carefully as the design of the ESS systems. As part of the employment process, it is important to include background checks to ensure that authorized access is appropriately given to employees who are expected to be trustworthy.

Segregation of Duties

The principle of least privilege should be assigned to the functions of individuals. By carefully designing processes, it is possible to ensure that no individual has the ability to bypass control measures. For example, one person could be responsible for monitoring video feeds while another person is responsible for archiving the video and changing tapes. This would require collusion or cooperation between the two individuals to bypass the capability of identifying activity covered by the video.

Audits

One of the most valuable tools in maintaining network security is performing frequent, irregularly scheduled security audits. This involves reviewing the log data that most ESS and network elements create in routine operation for signs of unusual, unexplained, or unauthorized activity. Since these system logs can be quite voluminous, a variety of automated tools often are used to assist in their review. Audits should not be performed by the same individuals who are responsible for the routine operation and administration of the system under review.

Audits are also useful in a multi-tenant or shared user physical environment. ACS provide rapid access when clients want to know what employee visited a site or utilized a shared resource during certain time frames.

 © 2012 BICSI®

General Security Recommendations

The following are general network security recommendations and practices for ESS systems:

- Develop a security policy.
- Establish physical security.
- Lockdown perimeter security.
- Enable existing security features.
- Secure operational traffic.
- Secure management traffic.
- Manage configuration.
- Eliminate security deficiencies.
- Provide continuous security training.
- Perform security audits.

Develop a Security Policy

A security policy defines the controls, behaviors, and expectations of users and processes and lays the groundwork for securing ESS assets. Since the acceptable range of use of ESS systems is narrower and they have more demanding operational requirements than ITS, they also demand their own security policy.

Establish Physical Security

Establish effective physical security to protect ESS equipment from physical damage and unauthorized access.

Lockdown Perimeter Security

Eliminate all external connections to the perimeter of the ESS network that are not necessary. For necessary connections, authenticate, authorize, and monitor any use over those connections, including:

- Understand, document, and periodically review the necessity for each external connection.
- Consider the use of security products for perimeter protection that meet published, well-known, and accepted security standards.
- Allow only authorized users of devices to reach authorized destinations during authorized time periods and log the details of the activity.

General Security Recommendations, continued

Enable Existing Security Features

Effectively utilize security features of current ESS and infrastructure devices, including:

- Configure all available user access controls.
- Change the defaults and use strong passwords that expire regularly.
- Eliminate or protect any paths over which plaintext access control cannot be avoided.
- Do not reuse or share user identifications or passwords among systems or personnel.
- Keep operational security in mind—do not reveal valuable information about the network through sign-on banners, device names, or other means.
- Configure router ACLs to restrict network protocols and connectivity.
- Use switch VLANs to isolate like traffic, making ACLs easier to apply and manage.
- Use MAC filtering to block out unauthorized devices.

Guides on the secure configuration of network devices are available from various sources, including manufacturers and user groups.

Secure Operational Traffic

Eliminate any unnecessary operational traffic by:

- Disabling nonessential features on ESS network devices.
- Putting like devices on the same VLAN and then using router and switch security features to allow only authorized devices, their required protocols, and their specific network connectivity on those VLANs.

Secure Management Traffic

Use dedicated hosts for device management. Use router and switch security features to allow only these hosts, using specific management protocols, to access infrastructure and ESS devices. Isolate and protect management traffic from operational traffic in any of the following ways:

- Manage devices through direct local connection.
- Manage devices using an out-of-band network or serial connection. This requires both dedicated communications bandwidth and a dedicated management interface on each device.
- Manage devices using a protected in-band remote connection. Use VLANs for in-band isolation, ACLs for traffic control, and VPNs, where available, for integrity.

 © 2012 BICSI®

General Security Recommendations, continued

Manage Configuration

Good configuration management starts with good documentation, which requires the following:

- Map out and document the entire ESS network, infrastructure, and device configurations.
- Prepare and configure new equipment off-line.
- Sanitize old equipment before disposal by clearing configuration information and user data from memory and disks, restoring factory defaults, and removing nonfactory labels.
- Keep infrastructure security features current with device moves, additions, and decommissions.
- Enable auditing features and periodically examine the resulting logs for signs of unusual activity.
- Synchronize to a common time reference so that audit logs become more useful during security incident response.

Develop a disaster recovery plan for the ESS system and test it periodically.

Eliminate Security Deficiencies

Identify security deficiencies (using established ESS security policy) and develop a plan to proactively eliminate them.

Continuous Security Training

Recommend that all security personnel receive comprehensive and relevant security training, with refreshers on a periodic basis.

Perform Security Audits

Verify the effectiveness of security measures by performing frequent, irregularly scheduled security audits.

Trends

A recent trend in network security is the concept of deperimeterization. The idea is that a perimeter is no longer sufficient to provide a trusted zone, and all devices and protocols used on the network should be robust enough to exist in a hostile environment. This concept makes use of inherently secure protocols that authenticate communications partners before allowing any transfer of data, secure operating systems and applications, and host-based intrusion prevention.

Chapter 11
Systems Integration

Chapter 11 discusses the concepts, systems, and processes related to the integration of electronic safety and security (ESS) systems, including command and control, data networks, building automation, fire-life-safety (FLS), and energy/lighting management.

Table of Contents

Systems Integration 11-1
Introduction 11-1
Electronic Safety and Security (ESS) Integration and Convergence 11-2
Features of Electronic Safety and Security (ESS) Integration 11-2
Standardized Components 11-2
Open Standards 11-2
User Training 11-3
Smart Environments and Privacy Issues 11-3
Role and Efficiency of Information Technology (IT) 11-3
Centralized Management/Control 11-4
Goals of Electronic Safety and Security (ESS) Integration 11-4
Convergence of Protocols/Standards 11-4
Modular Scalability 11-4
Convergence 11-4
Human Considerations 11-5
Need for Effective Response Planning 11-6
Improved Direct/Remote Access Control 11-6
Hosted Applications 11-6

Fundamentals of Integration 11-7
Multiple Systems within a Single Site 11-7
Single Systems across Multiple Sites 11-7
Multiple Systems across Multiple Sites 11-8
Remote Access 11-8

Electronic Safety and Security (ESS) Components 11-9
Sensor-Based System 11-9
Intrusion Detection Systems (IDS) 11-9
Access Control Systems (ACS) 11-10
Video Surveillance Systems (VSS) 11-11
Physical Security Information Management (PSIM) System 11-11
Building Automation Systems (BAS) 11-14
Examples 11-17

Software 11-17
Databases 11-18
Control and Monitoring 11-18
Scalability, Resilience, and Reliability 11-18
System Configuration and Expandability 11-19
Input/Output Matrix 11-19
Maps and Icons 11-20
System Response Times 11-20
System Expansion Capability 11-21
Electronic Safety and Security (ESS) Integration Process 11-21

Understanding the Risks Involved with Integration 11-24

Managing Risk 11-24
Risk Management Tools 11-24

Figures

Figure 11.1 Typical access control configuration 11-10
Figure 11.2 Sample physical security information management system 11-13
Figure 11.3 Typical network building automation system 11-16

Tables

Table 11.1 Multiple systems 11-12

 © 2012 BICSI®

Systems Integration

Introduction

This chapter covers concepts, systems, and processes related to the integration of electronic safety and security (ESS) systems. Through integration, ESS systems begin to share information, command, and control with a range of other systems, including data networks, building automation, fire-life-safety (FLS), and energy and lighting management.

Integrated ESS systems are deployed in many environments, including cities, facilities, campuses, and vehicles. These integrated systems can utilize common infrastructure, input, output, or data networks for information transport, including both wired and wireless information technology systems (ITS).

The integrated systems utilize various voice and data networks for their information transport, including:

- Public switched telephone network.
- Personal area network.
- LAN.
- Wide area network (WAN).
- Metropolitan area network.
- Cellular wireless (time division multiple access, code division multiple access, and Global System for Mobile Communications).
- Mesh wireless—licensed and unlicensed frequencies.
- Point-to-point wireless—licensed and unlicensed frequencies.

With the rapid changes in technology as well as the continued convergence to Internet protocol (IP), systems that operate independently and in isolation likely will not survive. Integrating systems is inevitable as companies strive to lower operational, maintenance, and personnel costs.

As system experts are forced to diversify, integrated hardware and software packages will become more prevalent. Systems that allow open architecture and more interconnection will replace proprietary systems.

ESS designers must know and understand the implications of:

- Integrating systems.
- Sharing information.
- Combining system vendors.
- IP convergence.

Electronic Safety and Security (ESS) Integration and Convergence

ESS integration involves convergence of ESS technologies into common ITS with other systems using common network protocols. As IP implementation continues to proliferate, ESS systems are converging from different applications with different infrastructures to a common platform. The control systems of an integrated solution can employ:

- Web servers.
- Graphical user interfaces (GUIs).
- Database technologies.
- Software components called intelligent agents.
- Decision support and active response systems.

An integrated ESS system also has a human component, including:

- ESS consultants.
- ESS designers.
- Technicians.
- Integrators.
- System end users.

Features of Electronic Safety and Security (ESS) Integration

Standardized Components

Adoption of industry standards may extend the installed life of products, encourage innovation, and open solutions to new markets. Standardization allows for enhanced integration of different physical security applications (e.g., intrusion detection systems [IDS], access control systems [ACS], video surveillance systems [VSS]).

In addition to fostering intercommunication between ESS components and systems, adoption of standards allows the integration of ESS components into other building systems, including:

- Building management systems (BMSs).
- FLS systems.
- Network monitoring and control systems.
- Support systems of other operations.

Standards produced by organizations, such as the Telecommunications Industry Association, Institute of Electrical and Electronics Engineers, Inc.® (IEEE®), International Organization for Standardization (ISO), and Internet Engineering Task Force, cross the boundaries of several industries by providing a common set of protocols.

Open Standards

The use of open standards, such as those produced by IEEE, ISO, and other international standards organizations, in component and system design allows compliant infrastructure to remain in place while other modules or components are added. Open standards tend to evolve, but they generally maintain backward compatibility for longer time spans than proprietary standards, mostly because of wide adoption in the installed base.

 © 2012 BICSI®

Features of Electronic Safety and Security (ESS) Integration, continued

Scalability through Open Standards

Scalability is the existing system's capability of growing to meet the customer's needs over time. Many legacy systems are not scalable, resulting in obsolescence of components or entire systems and requiring regular software and hardware replacements.

Open standards encourage a modular approach to systems design, whereby components from several manufacturers can be incorporated into an existing system to expand or scale its capabilities. Components that comply with open standards have a greater chance of staying in place while systems are scaled to meet the customer's needs.

The ability to use components from various manufacturers helps reduce costs when systems are past the design stage and are in the bidding processes for installation.

Improved Intelligence

Cross-industry open standards foster the interoperation between dissimilar systems, giving them the ability to coexist for new and wide-reaching purposes. The result of such standardization is the capability of sharing common logs and providing correlated statistics, visualization, and tracking among multiple systems.

User Training

The ESS designer must consider the cross-training aspect of a fully integrated ESS system. Although systems integration is the end goal, the ESS designer must be aware of the complications that may result from the cross-trained monitoring of building automation systems (BAS), BMSs, and ESS systems.

Smart Environments and Privacy Issues

Smart environments in commercial applications involve the use of sensor and control systems within human work environments (e.g., office spaces, factories). ESS systems are an important component of such applications.

ESS designers implementing fully integrated ESS systems must ensure that smart environments are sensitive to the client organization's culture as well as legislative issues concerning smart environments related to privacy issues and work safety requirements.

With the use of radio frequency identification (RFID) devices and other wireless security and access control technologies, a fully integrated system could track an employee's every movement. ESS designers should be aware that use of such transactional information for performance evaluation is possible and raises workplace monitoring concerns.

Role and Efficiency of Information Technology (IT)

Systems integration may generate unexpected labor savings. For example, if the heating, ventilating, and air conditioning (HVAC), security alarm, and fire alarm are integrated, monitoring of the three systems may be reduced to one department or central station monitoring firm.

Features of Electronic Safety and Security (ESS) Integration, continued

Centralized Management/Control

The need for a centralized point of control for a building or campus environment has grown. A single point of responsibility is a useful goal for ESS integration.

With the convergence of ESS systems, monitoring of these systems falls upon only a few individuals in a centralized command center. Often, these individuals are unfamiliar with the system's technical aspects.

Having easy-to-follow GUI linking and controlling these systems allow for more efficient training and productive time. Remote access allows for control and monitoring from a virtual command center. It also allows the management to view critical information in the time of emergency.

An advantage to this approach is that the integration of diverse systems simplifies the development of operational procedures that enhance the quality and speed of responses to unusual occurrences. Response assets can be quickly and effectively alerted with a top-down view of an incident.

Goals of Electronic Safety and Security (ESS) Integration

Several important goals pertaining to the use of ESS integration are discussed below.

Convergence of Protocols/Standards

As the number of ESS systems grows, the importance of standards and the convergence of protocols increase.

Modular Scalability

Through interoperability standards, adding new sensor systems into the existing integrated systems and using cameras as motion sensors, radiation detection, or wireless sensors can be accomplished seamlessly.

Convergence

With the advent of software control, existing sensors and systems can be employed in new ways to create previously unforeseen solutions. True integration of disparate systems can create entire new applications for ESS systems as integral components to building automation, automated safety systems, and entry into the world of smart environments.

Integration also may exist within as well as between systems as discussed in the following examples.

Access Control Systems (ACS) and Building Automation Systems (BAS)

An ACS may be integrated with the BAS to allow turning on the appropriate HVAC zones for the first person's arrival. Such a configuration allows the HVAC system to run only when needed.

 © 2012 BICSI®

Goals of Electronic Safety and Security (ESS) Integration, continued

Multiple Camera Tracking and Recognition Systems

Camera systems capable of applying video analytic technology to identify, target, count, and track the movement of individuals through a facility and coordinating them with ACS, network systems, and BMSs may yield security and system-to-system benefits.

Object-to-Human Association

The ability to associate luggage, a briefcase, a box, or another container with the person who initially held such an object is called object-to-human association. Airport applications may include software that alerts a monitoring center when a person leaves luggage unattended or picks up unattended luggage that person did not originally possess.

Human Considerations

The following sections discuss some human considerations of the ESS integration.

Simplified User Training

Operators are currently trained on individual control systems rather than several systems (perhaps with several operators). A security person may potentially monitor the system's ESS, BMS, and FLS system just as the engineering or maintenance personnel may monitor the security systems.

Although user training would be simplified, separate user training on application components relevant to job function should be given. The integrated systems' operation requires knowledge of both the individual systems and their interoperability.

Larger Pool of Technical Skills

ESS technologies are not exclusively tied to the vendor-trained security skill set. Skills transfer between installations, between vendor solutions, and across the ITS industry.

Simplified Serviceability

Technician training is also simplified. Although end components and hardware and software middleware (e.g., system control panels, application programming interfaces) may require specific vendor knowledge and training, an integrated system has more common components, including a common network and common computing systems for monitoring and control.

Once these common systems and infrastructure components are adopted, future expansion is likely to phase out the legacy systems, so the skills related to the integrated system components have an extended usefulness compared with those related to the legacy systems.

Troubleshooting and diagnosing from remote locations are facilitated through integrated systems. Such remote operations may save valuable travel and personnel time, particularly in widely distributed systems. Coordinating the data across the associated systems may improve diagnostics. Remote reconfiguration, restoration, and power-up provide new means of problem resolution.

Goals of Electronic Safety and Security (ESS) Integration, continued

Need for Effective Response Planning

Integrated systems require an integrated approach to response planning. Technology alone will not improve an organization's ability to respond effectively to an emergency. It is only through the development of thorough and effective procedures, the initial training of monitoring and response forces, and regular tests and reinforcement of training that the true value of integrated systems can be recognized by an organization.

Improved Direct/Remote Access Control

Through ITS pathways to remote systems, ESS components may be monitored and, in some cases, controlled from any location dictated by the user's needs.

The information about the system's states may now be controlled and distributed as needed. Through integration, Internet services allow controlled access to the system components. Notification via cellular telephone, tablet, text message, e-mail, pager, control interfaces, and even the activation of remote devices are accommodated through integration.

The nature of an integrated control system (ICS) allows new means for visualization and control, which may provide improved usability, productivity, and efficiency and generate labor savings. Operators are able to use the monitoring and control functions even though they may be unfamiliar with the technical aspects of the sensors and other parts of the system. Integrated help systems and process and procedure wizards allow access to technical help through online documentation.

Hosted Applications

As system manufacturers continue to develop and deploy software as a service (SaaS)-based products, integration and convergence become more relevant. This is due to central equipment being located in centralized data centers and services deployed to end users through the Internet. This trend may eliminate the need for premises central equipment. Only edge devices (e.g., card readers, video surveillance cameras, sensors) would be located at the premises.

 © 2012 BICSI®

Fundamentals of Integration

Integrated ESS systems may be classified by the number and locations of systems that communicate. The design, hardware, software, and monitoring vary greatly between multiple systems within a single site, single systems across multiple sites, multiple systems across multiple sites, and remote access.

Multiple Systems within a Single Site

The ability to interconnect multiple electronic systems within a single site provides enhanced levels of security and often results in savings through combined monitoring and insurance premium reduction.

The Ethernet/IP platform has facilitated the convergence of multiple systems through ease of:

- Use.
- Lower cost per port.
- Manageability.

Many software houses also have begun to produce umbrella integration software, which takes the dissimilar outputs of legacy security devices and allows converged command and control functions from a single workstation. In addition to reduced management and monitoring costs, these systems provide many opportunities for interoperability.

Businesses are increasingly combining the benefits of previously stand-alone systems like access control, RFID, and computer security to create location-sensitive adaptive user restrictions where users may only log on to a given system if they are physically present at the location. The ability to leverage data from multiple systems located in a single site provides many benefits.

Single Systems across Multiple Sites

Many of the same benefits of multiple converged systems in a single building or campus also extend to building or campus security systems connected between multiple sites. The benefits of systems' interconnections are often seen as part of a BAS effort.

Leading industry manufacturers and consultants are publishing evidence of the following benefits of convergence:

- Storage requirements lowered
- Number of servers reduced
- Improved video quality and the ability to recognize faces vastly improved over the previous system's capabilities

Single Systems across Multiple Sites, continued

- Reduction in false alarms in video surveillance areas
- Risk mitigated by expediting maintenance and repair
- Time required investigating security incidents reduced
- Reduction in maintenance costs
- Network protection and virus definitions implemented as soon as available, which increased security
- Surveillance system unified with other security systems (e.g., alarm detection system, ACS)

Multiple Systems across Multiple Sites

While a number of complexities and design issues surround the multisite convergence approach to electronic security, there are just as many benefits. Among them are substantial savings generated by using a single ITS and supporting infrastructure, contractor, and designer.

Multisite convergence also provides added opportunity to standardize hardware and practices between geographically diverse locations. In the multisystem, multisite environment, the ESS designer is faced with converging different security systems across diverse networks many times using dedicated leased lines or the Internet for command and control functionality. Combining these once unlinked systems will provide greatly enhanced asset protection and a more comprehensive safety and security design.

Remote Access

The growing need for access to information and the resulting availability of real-time information have led many security systems manufacturers to provide remote access. This access may take multiple forms.

Some of the more common forms are:

- Remote control and administration of systems.
- Remote access for monitoring or audit control of systems.

Remote access may use many different protocols to connect to individual systems. The ESS designer should be able to select systems that are compatible with the different protocols.

NOTE: Refer to Chapter 10: Network Concepts for security considerations that should be evaluated in the provision of remote access to ESS systems.

 © 2012 BICSI®

Electronic Safety and Security (ESS) Components

This section details the ESS components (e.g., sensors, cameras) and the networks, systems, and software involved in the integration of ESS systems. This section also looks at other non-ESS systems involved in the integration and presents several typical scenarios, including integrated building systems.

Sensor-Based System

ESS sensor-based systems incorporate the use of various analog and digital devices that measure and 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.

Intrusion Detection Systems (IDS)

An 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:
  - Passive infrared
  - Microwave
  - Photoelectric
  - Laser
  - Ultrasonic
  - Proximity
  - VSS cameras

The types of network IDS sensors include hardware and software devices connected to a LAN or WAN using, most often, transmission control protocol (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.

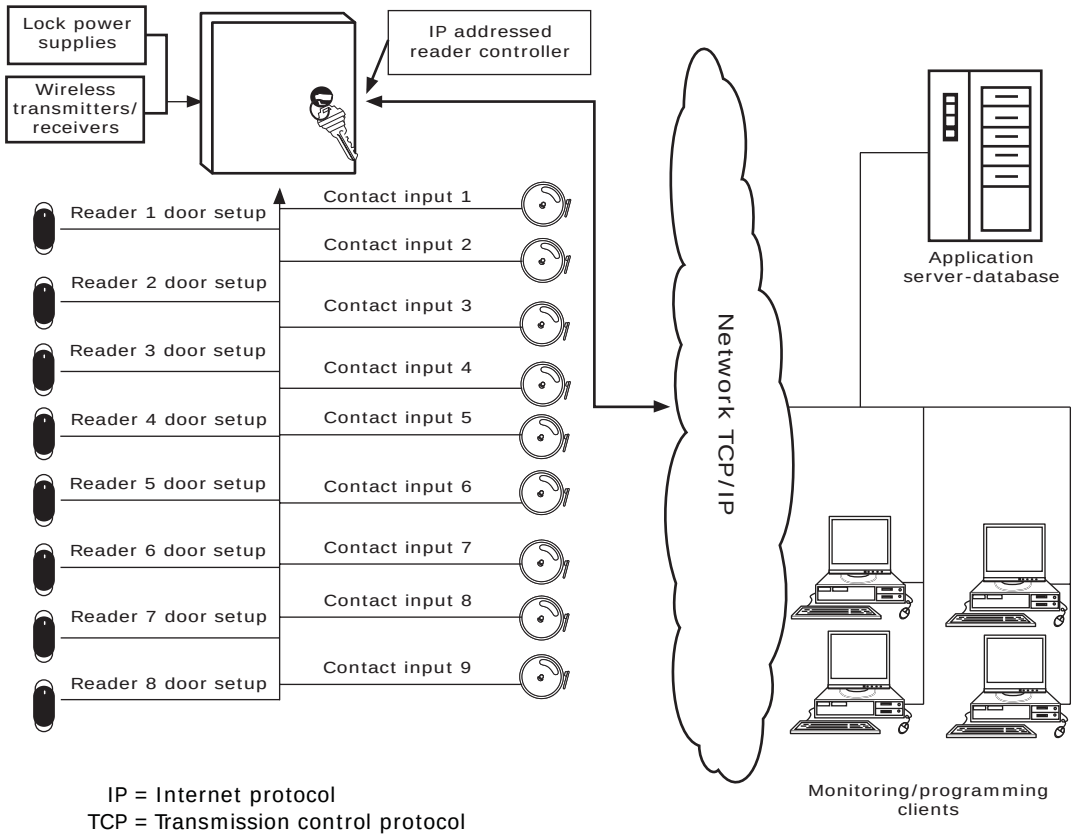
Access Control Systems (ACS)

In addition to the components and applications listed in Chapter 4: Access Control Systems, integrated ACS also may include:

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

Many ACS and IDS 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. Figure 11.1 demonstrates how the various inputs and outputs utilize integrated ACS hardware and software to communicate with dissimilar systems and networks.

Figure 11.1
Typical access control configuration



 © 2012 BICSI®

Video Surveillance Systems (VSS)

In addition to the components and applications listed in Chapter 5: Video Surveillance Systems, integrated systems also may include:

- Remote video.
- Advanced integrated surveillance systems:
  - Distributed integrated active remote multiple 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 SaaS. In addition, each of these subsystems may be controlled by other integrated systems (e.g., BAS, ACS) or just receive and manage information as with the physical security information management (PSIM) system.

Physical Security Information Management (PSIM) System

The digital video management system manages video content, whereas 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. Sample operations are shown in Table 11.1.

The ESS designer should consider the PSIM system as a user interface when multiple systems at a facility exist and require interoperability with a surveillance system. With a PSIM system, security personnel can manage situations or events without having to deal with the nuances of the underlying systems and technology.

The physical security industry has seen an introduction of new tools that are designed for establishing a performance baseline for a physical security program. Some of these tools provide dashboards that summarize alarm data by time and event correlation, and others enhance the security operator's response by programmable rule engines.

Physical Security Information Management (PSIM) System, continued

Table 11.1
Multiple systems

System Type

User Interface Type/Feature	Analog Video Surveillance	Network (IP) Video	Access Control	Identity Management	Intrusion Detection	Intercomm-unications	Fire and Life Safety
Hardware control	•	•	•		•	•	•
Digital video matrix system GUI, hardware	•	•					
Access control system GUI		•					
Identity management system GUI			•				
Physical security information management GUI	•	•	•	•	•	•	•
ASP or portal service provider		•	•	•			
Digital format display	•	•	•	•			
High-definition display		•	•				
Centralized or distributed server architecture	•	•	•	•			
Redundant or fault-tolerant server design	•	•	•	•			
Multiuser workstations	•	•	•	•			
Portable device		•	•	•			

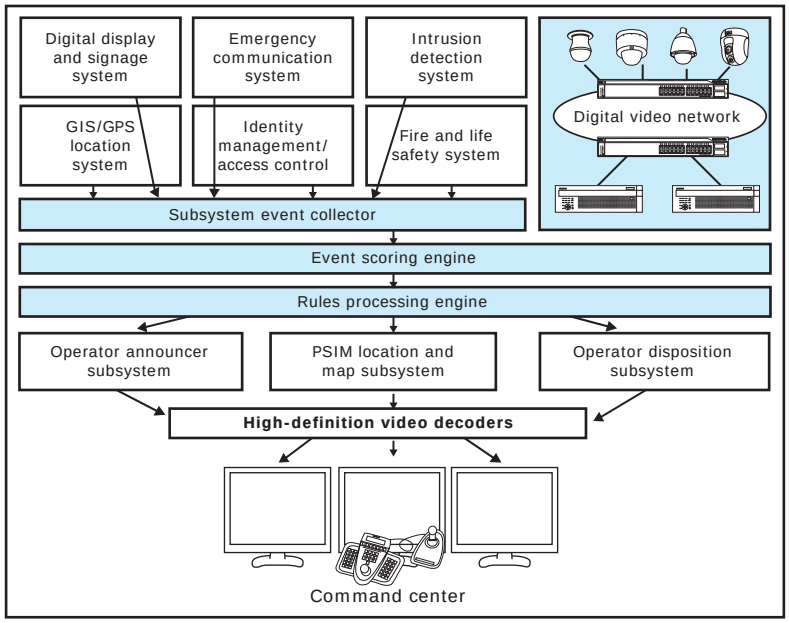
ASP = Application service provider
GUI = Graphical user interface
IP = Internet protocol

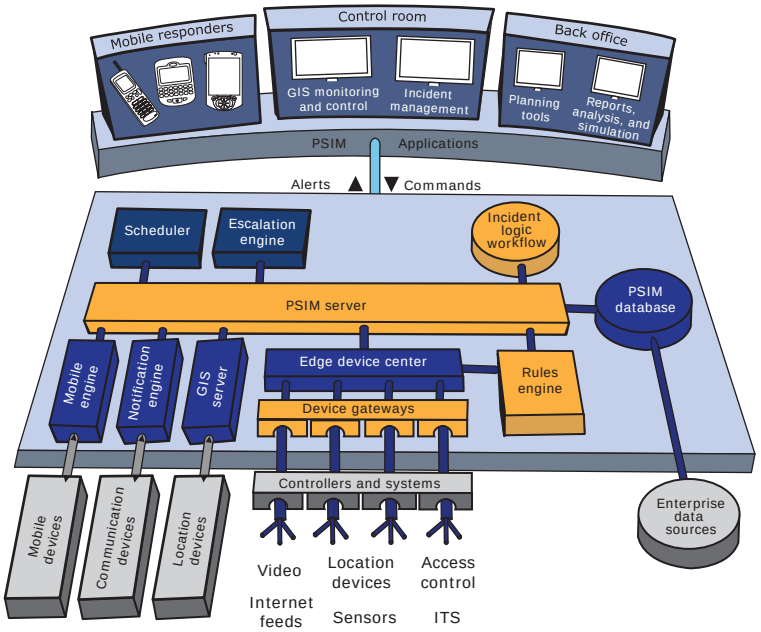
 © 2012 BICSI®

Physical Security Information Management (PSIM) System, continued

Physical security applications are best represented by user interface type and system class, forming the physical security application matrix in Figure 11.2.

Figure 11.2
Sample physical security information management system





GIS = Geographic information system
GPS = Global positioning satellite
ITS = Information technology systems
PSIM = Physical security information management

Building Automation Systems (BAS)

A BAS provides a vast opportunity for the integration of dissimilar systems on a common network using shared protocols and network transport. As BAS is the largest collective group of systems represented by HVAC, the potential financial and operational benefits of integrating these diverse systems are strong drivers for manufacturers to develop new hardware and software. They also are a strong motivation for the end user to request the integration of the low-voltage systems.

A BAS optimizes the administration, operations, and performance of HVAC equipment and associated alarm systems with defined networks and unique protocols. These functions are used for controlling the temperature and humidity levels in a facility. These systems also may provide for smoke control, maintaining pressure relationships between spaces, and fresh air for occupants. In most modern building systems, control systems of these functions are integrated into a single HVAC system.

By optimizing the performance and operations of the HVAC equipment, the goals are efficiency and ease of control. Generally, a BAS helps increase the interaction of mechanical systems within a building to improve occupant comfort and lower energy use. An integrated BAS uses computer-based monitoring to coordinate, organize, and optimize building control systems (e.g., security, FLS, elevators).

Over the years, several proprietary building automation network standards evolved in the marketplace. Proprietary solutions generally have controlled the commercial HVAC market, limiting the upgrade and expansion of the infrastructure to either vendor-compatible off-the-shelf products or costly custom solutions. Trying to get vendors to standardize or publish their proprietary protocols usually resulted in one-way open systems with the host system always playing the role of the master.

As systems age, parts for the proprietary systems become scarce and are often found only in secondary markets.

When selecting a BAS, the following are important:

- Flexibility
- Scalability
- Expandability

The ability to reconfigure and monitor changes made to an automation system in real time is important to building managers.

In recent years, open data protocols for building automation and control network (BACnet®), American Society of Heating, Refrigerating and Air-Conditioning Engineers Inc., and LonWorks® (Echelon®) have been promoted and implemented as primary protocols by numerous companies as an alternative to proprietary protocols.

 © 2012 BICSI®

Building Automation Systems (BAS), continued

Standardized BAS protocols (e.g., BACnet, LonWorks) and interfacing standards (e.g., object linking and embedding for process control) allow the exchange of information between different manufacturers' devices, systems, and programs in an agreed way.

Network standards are a prerequisite for the cost-effective integration of various manufacturers' subsystems. Because flexibility, scalability, and expandability are important when selecting a BAS, the ability to reconfigure and monitor changes using common protocols that easily allow changes, upgrades, and maintenance is essential to building managers.

Facilities must continuously meet business needs and reduce operating and maintenance costs. To effectively remove barriers to progress, a logic-based automation and control framework is needed that will allow many different systems to evolve.

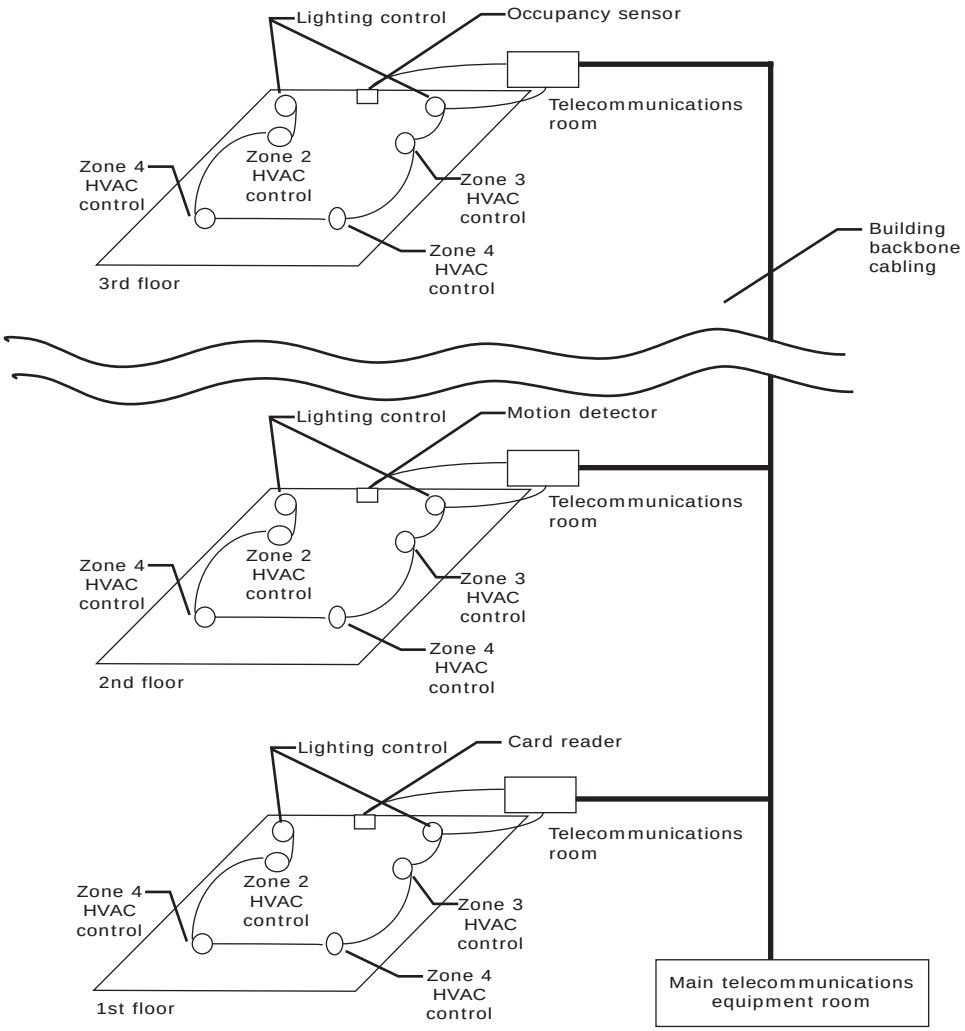
Typical customer requirements for building automation include:

- Affordable initial investment.
- Use of the existing ITS infrastructure.
- Unique user interface for all building domains (e.g., HVAC, lighting, fire, access, intrusion).
- Higher supplier independence for future system enhancements.
- Affordable operating, energy, and maintenance costs.
- Immediate building operability for mobile operators.
- Intuitive usability of operating controls for less experienced users.
- Technical competence center that serves many buildings in a defined geographic region.
- Comfort and service.
- Minimal energy consumption.

Building Automation Systems (BAS), continued

Standard features of a BMS are a common interface, open system standards, Internet technology, and advanced integration. Figure 11.3 shows a typical network BAS environment.

Figure 11.3
Typical network building automation system



HVAC = Heating, ventilating, and air conditioning
IP = Internet protocol

 © 2012 BICSI®

Building Automation Systems (BAS), continued

ITS technologies are being used by increasing numbers of BMSs. These features allow smooth data exchange with the customer's office automation system and business process. Existing ITS infrastructure (e.g., LAN/WAN) may be shared, which reduces cabling costs and allows flexible solutions.

ITS technologies generate additional benefits, including:

- Easier and centralized software updates.
- Reduced maintenance.
- Local operation using slim, low-cost clients that require only a browser.

Examples

An integration scenario would be the adaptation of a facility's BAS or ACS through TCP/IP. The sensory inputs received by the fire alarm panel through serial communications to a TCP/IP converter may output status conditions or actuate a contact closure or voltage output to perform preprogrammed tasks.

HVAC systems are typically integrated into fire alarm systems to stop the spread of fire. Air handling devices usually are shut down by the fire alarm system. This is done by shutting down an HVAC system or controlling its fire control duct dampers.

Security systems are also integrated into fire alarm systems to release doors and allow egress or close doors to compartmentalize the fire.

One of the BAS functions is saving energy. A good opportunity to save energy is to control lights in a facility. In light control systems, a contactor typically is inserted in the electrical circuit to the lights, and a relay is used to control the power to the lights. A BAS, which includes the software and components to perform such a task, is integrated with little difficulty.

Another integration example is to have the ESS system turn on the lights in the event an intruder is detected. Used in conjunction with the video surveillance cameras and motion sensors, such a system allows for the detection and potential recording of unauthorized activity.

Software

The functionality and reliability of an integrated system rely 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 because of the lack of in-house capabilities to make modifications to the software beyond the standard configuration. Another concern is the lack of access to the source code required for:

- Vendors to make changes to commercial off-the-shelf software platforms.
- Integrators to make changes to proprietary software platforms.

Software, continued

The development of an integrated system at the vendor level is often based on the current version of the database and operating system (OS) software available. The change from one OS 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 OS platforms.

Databases

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 (e.g., payroll, timekeeping). Selections can be based on personal preference or experience of the integrator, client, or authority having jurisdiction (AHJ).

Control and Monitoring

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.

Scalability, Resilience, and Reliability

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 also will be a deciding factor in the selection. The system should have the capability of being scaled to meet the current and future needs of the client.

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, including redundant array of independent disks systems. The implementation of these scenarios now or in the future will have a significant impact on the selection of a software platform.

End users must understand the software license they are purchasing. Some security software companies offer software based on the number of devices that must be monitored. Buying a license for 100 devices with an initial installation of 90 devices leaves little room for expansion.

 © 2012 BICSI®

System Configuration and Expandability

Planning for expandability easily can be incorporated into the design process and often will benefit the ESS designer. 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, including not providing adequate motion detection or an unaccounted tamper switch, can be costly to the ESS designer 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 ITS infrastructure to support the new hardware.

Input/Output Matrix

The completion of an input/output matrix is a vital step in determining system expansion requirements for larger complex systems. The matrix should be configured for a specific system but contain basic information, including:

- 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 (e.g., fire alarms, tamper switches, tampers).

The matrix is a useful reference for the actual loading of each processor or segment of a system. The matrix also can be configured to calculate the expansion capability of a system and any particular section as a reference for the AHJ or plan review team.

System Configuration and Expandability, continued

Maps and Icons

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 will require 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 AHJ review will determine the types of maps required and where they should be located so that they can be found during an event.

The operator can then select the icon to display the detailed map. The use of icons should be considered. The icon should readily display the status of an event or alarm and should change as the state of the associated device changes.

One common convention is that an icon is green when the device is in the normal state (armed for detection devices), yellow when placed in access, and red when in alarm. The icon also may blink prior to being acknowledged and may be a solid color after acknowledgment but prior to returning to its normal state.

Another effective tool is to assign one icon per zone, area, or building on a site so 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. The submaps are only accessed to view particular devices.

The maps should be configured so 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 requires a reconfiguration of the mapping system.

A common pitfall is to include too large a scale map for an area with few sensors but with significant expansion capability.

System Response Times

The system response times should be calculated because they are an effective tool in determining the need for additional system capacity. The goal of system response times is to determine the processing and reporting times for alarms or system requests (e.g., access to an area via a controlled door or gate).

The response times must be calculated for peak use times (e.g., shift changes). Distributed processing reduces the response times significantly, but heavily loaded systems can still experience response time issues.

 © 2012 BICSI®

System Configuration and Expandability, continued

System Expansion Capability

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, and card readers.

The future capability is how much the system can be physically expanded by adding hardware. The physical layout impacts the system expansion. The use of available inputs in another building or area may not matter if the cost of the connections (e.g., conduit, cable, labor) is significant.

The as-built expansion capability may be included in a specification and is often expressed as a percentage. Clarification may be needed if the percentage does not identify the specific criteria (e.g., percentage of inputs or card readers).

Electronic Safety and Security (ESS) Integration Process

With all of the technology and opportunities for systems to work together comes the need for specific operational and functional requirements. 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 standards and codes (refer to each chapter for individual system requirements) 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 must be defined. These general requirements can range from simple to complex. For example, a card reader system used to verify attendance with the human resources database also can turn on the office lights and the HVAC to an area of a building when an occupant arrives.

There must be a discovery period with all of the customer parties involved—the ESS designer, the contractor, and the end user. The customer should be encouraged to include all parties within their organization to participate in the discovery process. If they are not included, one small change late in the process may delay delivery, increase the cost, or impact the system.

Electronic Safety and Security (ESS) Integration Process, continued

Some of these parties include:

- Operations.
- Information technology.
- Facilities.
- Security.
- End users.
- Financial decision makers on the project.
- AHJ.

With all parties included, the group should determine which systems are to be involved and any phasing of functional requirements, if necessary. A written functional description should define the expectations of the system and describe in detail the requirements of the integrated system versus the individual systems.

The description should identify:

- Where information is to be stored.
- Which systems are primary.
- Which systems are secondary.
- If duplicate functionality is desired or required.
- Possible areas of overlap.

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 must 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 (see Chapter 3: Electronic Safety and Security Design Process) but must account for any additional requirements for integration prior to design completion. As these systems are built, any inherent flaws or newly imposed issues can be investigated and changes can be implemented to the functional description, if necessary.

It is useful to obtain references of operational systems that meet the same system requirements (or similar requirements) and request the ability to contact the end user. The limitations of any item that may impact the system functionality should be discussed. 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. System server locations, resilience, and GUI locations must all be considered when evaluating the integrated system.

 © 2012 BICSI®

Electronic Safety and Security (ESS) Integration Process, continued

If possible, consider the testing requirements and vicinity of equipment that must be tested. With a new construction project, the ability to have more freedom in the selection of equipment and implementation methodology may save:

- Space.
- Hardware.
- Equipment costs.

When legacy systems are converged, the best methods for convergence may be expensive, require additional hardware, and require system downtime during implementation.

The legacy systems must be assessed to determine their:

- Usability.
- Maintainability.
- Sustainability.

Some systems may not allow the functional requirements to be met without replacement or upgrade of equipment. Other systems may require only software updates. After each system has been documented by a detailed site survey, they can be evaluated for usability against the functional requirements.

The design of the integration must consider the amount the customer is willing to spend, the method intended for the integration, and any approvals necessary to accomplish the integration. This is particularly important when fire alarms are involved in the integrated solution.

If the system functionality cannot meet the system functional requirements, then either the functional requirements or the systems must be evaluated for change. The functional description will lead to the development of the system description, and the system description may lead to modifications to the functional description.

All parties involved must agree to the final desired system configuration and how it will impact the functional description. If a decision is made to limit functionality based on a system description decision, it should be documented, and all parties should agree to the results.

A plan for implementing a legacy system may take years and have several phases, depending on the customer's willingness to outlay the capital. Each phase of implementation should describe the functional and system requirements and obtain the necessary approvals.

As building systems become more integrated and thus more complex, a logical result is systems that are less reliable. Reliability is cumulative in a system and decreases as significant or critical components are added.

Understanding the Risks Involved with Integration

Managing Risk

Integrated system risk management is the systematic process of identifying, analyzing, and responding to integrated system risk. It includes maximizing the probability and consequences of positive events and minimizing the probability and consequences of adverse events to system objectives.

Risk is an uncertain event or condition that has a positive or negative effect on a system objective. A risk has a cause and a consequence. Risk conditions could include aspects of the integrated system environment that may contribute to integrated system risk, including poor system components.

Risk Management Tools

Predictive maintenance tools can help to decrease system risk. An integrated system with a powerful BAS can use accurate, trended operating information to predict when equipment repairs, replacements, and services should be performed.

A single point of control reduces the:

- Complexity of multiple front ends.
- High cost of extra hardware.
- Expense of multiple training programs.

From one workstation, users can integrate all systems at multiple or remote facilities for centralized alarming and alarm routing via text message, cellular telephone, tablet, e-mail, or pager. Alarms can be sent directly to specific personnel rather than to a dispatcher, avoiding the possibility of being overlooked in a remote building until someone notices and complains.

If problems arise, an integrated system makes it possible to respond more effectively. For example, in an integrated system, the BAS/PSIM system can provide access to specific fault codes so that finite evaluations can be made to determine exactly what happened, where it happened, and why it happened so that immediate measures can be taken to correct the problem and prevent it from happening again.

 © 2012 BICSI®



Chapter 12
System Operation and Commissioning

Chapter 12 provides electronic safety and security (ESS) designers, in conjunction with security contractors and end users, with a framework to develop standardized policies and procedures.

Table of Contents

System Operation and Commissioning 12-1
Introduction 12-1
Operation 12-2
Maintenance Plan 12-5
Access Control Key Performance 12-8
Service Contracts 12-9
Emergency Response Category 12-10
Commissioning 12-12
Documentation 12-12
Cleaning 12-13
Labeling Components 12-13
Acceptance Testing Plan 12-14
System Testing 12-14
Preinstallation Testing 12-14
Preliminary Testing and Calibration 12-14
Burn-in Period 12-15
Acceptance Testing 12-15
Retesting Equipment and Systems 12-15
Client Staff Training 12-16
Warranty Period 12-16

Tables

Table 12.1 Service arrangement matrix 12-2
Table 12.2 Access control operation matrix 12-6
Table 12.3 Surveillance operation matrix 12-7
Table 12.4 Access control key performance example data (notional) 12-8
Table 12.5 Emergency response category matrix (notional) 12-10

System Operation and Commissioning

Introduction

This chapter will provide electronic safety and security (ESS) designers, in conjunction with security contractors and end users, with a framework to develop standardized policies and procedures that can reduce system breakdowns and malfunctions, thereby decreasing equipment downtime and overall inefficiencies of the ESS systems installed at their facilities.

The information required for system operation and commissioning is usually available from a variety of sources, including:

- Record drawings.
- Manufacturer equipment documentation.
- System performance specifications.
- Local ordinances.
- Industry best practices.

The policies and procedures covering the operation of the various systems and related devices should be developed by a project team drawn from various departments within the organization, including:

- Security.
- Information technology (IT).
- Facilities.
- Maintenance.
- Human resources (HR).
- A management team that sets policies, operational standards, and financial planning.

For an ESS system to remain effective, it must be properly managed and maintained. This is best achieved when all the stakeholders are fully aware of the cost to the organization if system failure results in a crime being committed.

Operation

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. It is therefore extremely 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 a knowledgeable 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 very 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.

Table 12.1 provides a typical matrix that could be generated by a project team to justify the type of service and maintenance contract that an organization could pursue to meet its ESS service requirements.

Table 12.1
Service arrangement matrix

Electronic Safety and Security (ESS) Service Type	Advantages/ Disadvantages	Organization Using Such Service
Security contractor who performs scheduled maintenance and responds to service requests.	This type of service works best when both parties understand their roles and responsibilities as defined in the contract document (e.g., educational, hospitality).	Those operating in a low-threat environment where system malfunction will not severely impact their ability to conduct business.

 © 2012 BICSI®

Operation, continued

Table 12.1, continued
Service arrangement matrix

Electronic Safety and Security (ESS) Service Type	Advantages/ Disadvantages	Organization Using Such Service
Security contractor has service personnel onsite during normal working hours to perform routine maintenance and service requests.	An advantage is consistent and fast response to servicing and maintenance issues. A disadvantage is higher cost that must be justified based on documented risk and threat assessment of the organization and facility.	Organizations operating site in a high-risk environment (location) or where their business activities are under constant threat from crime, sabotage, or espionage or where loss of company assets could severely impact overall operation (e.g., financial institutions, retail stores, research and development facilities).
In-house personnel provides all service and maintenance of ESS systems.	Uniform performance standards can be developed that reflect the organization's policies, procedures, and culture. A disadvantage is higher cost to the organization as the compensation packages for these personnel are usually part of operations or overhead charges that directly affect profit margin. Other disadvantages could be liability to the organization if system failure or malfunction results from employee oversight or neglect. Organizations considering pursuing in-house service should ensure that those employees selected are trained and equipped with up-to-date information on all the systems they are responsible for servicing. The level of service provided should exceed those offered above and should only be attempted by organizations having the strong managerial and operational structures in place to deliver exceptional service.	This service option usually is pursued by large organizations that have either a campus-style systems architecture or enterprise-wide systems dispersed across wide geographic areas or those operating high-risk/threat facilities where a security breach could have severe consequences for individuals, the organization, or the nation at large.

Operation, continued

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 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.

 © 2012 BICSI®

Maintenance Plan

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. Thisinformation 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 access control systems (ACS) 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.

Maintenance Plan, continued

Table 12.2 provides a matrix for access control operation. Table 12.3 provides a matrix for surveillance operation.

Table 12.2
Access control operation matrix

Scenarios	Interoperability	Benefits
Verifying Identification Access card issued only to individuals whose identity has been verified and authenticated from a combination of government-issued documents and biometric data.	• Provide standardized procedures for proving identity and a comprehensive identity management system. • Provide real-time verification of personnel whose identities have been vetted and cleared for entry to a secure facility. • Provide accurate information on identity of personnel requesting entry to a secure facility.	• Will allow organization to share facilities, resources, and information by increasing the acceptance of personnel credentials from one facility to another. • Critical information can be easily shared and disseminated on a real-time basis while improving the decision-making process.
Screening Screen personnel to verify the identity of personnel seeking entry to a facility.	• Access card and other biographic data on personnel can be crossmatched against the database of all employees authorized for accessing the facility. • Provides a standard screening system within which common identification credentials can be created and used to verify claimed identity. • Once a record is created in the access control center (ACC) database, it is available to other offices within the organization for future use and reference.	• Provide assurance that the credential in possession of the cardholder is authentic. • One credential should be used to authenticate access to an organization's facilities. • The use of multiple credentials should be avoided where possible.
Access and Inspection An accurate determination of one's identity is required to make sound access control decisions in a timely manner.	• A wide range of equipment and systems will be employed to authenticate identity and provide the access level established within the systems for individual users. • Provide identity credentials that can be rapidly authenticated electronically and the data collected and verified against the existing database. • Information available on one system can be easily shared, thereby providing real-time operational activities across the enterprise.	• Provide a credential whose reliability has been established by an official authentication process. • Provide electronically authenticated credential that is resistant to identity fraud, tampering, and counterfeiting. • Subsystems in an ACC can be designed to respond to information provided from other system within this interoperable network.

 © 2012 BICSI®

Maintenance Plan, continued

Table 12.3
Surveillance operation matrix

Systems/Devices	Policy/Plan Guidance	Benefits
Camera Identification Identify the camera type mounting location of all devices installed at the facility.	• Provide standardized procedures for camera operation such as video loss, camera tour, motion-activated video signal display, and camera call-up by activation from other interconnected systems (e.g., intrusion detection systems [IDS], emergency telephone). • If camera coverage extends to public spaces, provide guidance and procedures of recording of activities occurring in these spaces. • If camera coverage extends to private residences, request that the security contractor provide masking software to prevent identifiable viewing of these residences.	• This will ensure that video images viewed, recorded, and archived are consistent and with the organization's camera security plan. • This will ensure that surveillance systems are in compliance with the jurisdictions' privacy laws and regulations.
Recording Systems Identify the location of recording systems and type of recording medium in use.	• Develop guidance that defines the acceptable level of image quality, especially at sensitive areas within the facility. • Develop guidance on length of time recorded images will be stored and who will have access to these images once they are archived. • Identify the recording system compression technology in use and upgrade if needed to maximize storage capacity and minimize transmission usage. • Ensure that all recorded video on digital recorders is authenticated using an algorithm calculated into frames of video to aid in the admissibility of the digital video into a court of law.	• This ensures that recorded images will provide useful information on any future investigation that may be pursued. • The lengths of time recorded images are stored are sometimes mandated by government and other institutional bodies. • Compression and other recording technology directly affect bandwidth usage with associated cost implication if not properly managed. • Recorded video will be useless if it is inadmissible in a court of law.

Maintenance Plan, continued

Table 12.3, continued
Surveillance operation matrix

Systems/Devices	Policy/Plan Guidance	Benefits
System Power Source Identify and document how video surveillance devices are powered.	• Power to the video surveillance system should reflect the security plan. If systems are required to operate when there is outside power loss, a backup power source must be provided with seamless cutover. • Provide an approximate length of time the system will operate once the main power is lost.	• In the event of a power failure, operators will respond as trained without mass confusion from system shutdown. • This will allow operators to operate the system and start a scheduled shutdown without fear of damage to equipment or any loss of data.

Access Control Key Performance

The KPIs outlined in Table 12.4 can be developed for each system installed and should reflect the intent of the organization's security and emergency plan. The table should be reviewed on a regular basis to account for changes to an organization's business plan as well as changes in technology that could reduce the overall operating cost.

Table 12.4
Access control key performance example data (notional)

Key Performance Indicator	Threshold Level
Personnel access control	≤Three seconds to grant access to authorized users/cardholders
Vehicle access control	≥Twelve vehicles per minute scanning access card
Intrusion detection false alarm rate	≤Five false alarms per day
Video surveillance systems	Provide clear image of surveillance areas under all lighting conditions
Interoperability	Systems must operate seamlessly on a single operational platform
Systems reliability	According to customer requirements
Systems power supply	Must operate for a minimum of two hours after loss of main alternating current (ac) power source
Alert/notification	Provide precise location of security breach to allow for efficiency in response

 © 2012 BICSI®

Service Contracts

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 (SoW) eliminates misunderstandings and miscommunications.

The service contract should include the:

- Work to be performed and the frequency of said performance (e.g., weekly, monthly, quarterly).
- Price of the contract for the standard service and cost for additional services that are not part of the standard contract (e.g., after-hours or weekend response).
- Terms on which the contract can be terminated by either party.

Although different contractors may be servicing different components of the systems at the same facility, the following information should be included as an integral part of all 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 Table 12.5).
- 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 pan, tilt, and zoom [PTZ], Internet protocol [IP] or analog), housings, domes, recording devices, camera controllers, and display monitors.

Service Contracts, continued

- Uninterruptible power supply (UPS) and related power conditioning and surge protection devices.
- Electronic door locking devices, listing types (e.g., strike, magnetic lock, electrified mortise handset, shear lock).
- Communication devices (e.g., emergency telephones, two-way intercoms, one-way paging systems).
- Audible and other emergency display devices.

Emergency Response Category

The content of the emergency response category matrix in Table 12.5 should be viewed as a guide for organizations developing their own criteria for classification levels of failures.

Table 12.5
Emergency response category matrix (notional)

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 ACS and IDS may 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 efficiency of the security staff.

ACS = Access control systems
IDS = Intrusion detection systems

 © 2012 BICSI®

Emergency Response Category, continued

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.
- 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.

Commissioning

Commissioning is often one of the most neglected aspects of security system installation. A system that is properly tested and commissioned will provide the ESS designer, installer, and client with a security 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.

Documentation

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 (earthing), copper cabling, and optical fiber cabling.

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.

 © 2012 BICSI®

Documentation, continued

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, or changes (MAC) to the system.

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

Cleaning

A major task in commissioning security systems is the cleaning and removal of dust, dirt, and temporary covers. All foreign debris should be removed from the equipment and enclosures. 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.

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 MAC of an ESS system. 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-A).

Enclosures and other large components typically should have engraved plastic or metal identification plates. 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. Proper labeling will greatly reduce labor costs when the system servicing or MAC are ordered.

Acceptance Testing Plan

Clear acceptance testing guidelines should be provided in the construction specification documents. The guidelines must define the performance requirements for the ESS system. The acceptance testing plan will be used by the client during the final acceptance test as part of the turnover documentation. This 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.

Testing documentation must include full details of all commissioning tests as well as factory testing reports provided by the manufacturer with the equipment. The test plan forms and checklists should list any deficiencies and fully document the test results of each acceptance test performed. The client also documents all observed tests and creates a punch list of deficiencies that need to be corrected and retested.

System Testing

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. Equipment must be calibrated according to the manufacturer's recommendations and whenever suspected of being damaged. Calibration certification must be kept on record, and copies for each tester provided in turnover documents. Testing occurs in the stages described below.

Preinstallation Testing

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. Components (e.g., video cameras) also should be run through a quick functional test prior to installation. Preinstallation tests may reveal components that have been damaged in shipment and need to be replaced. Systems that require calibration or adjustment can be serviced in the shop instead of in the field.

Preliminary Testing and Calibration

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.

Each alarm point shall be tested for intrusion detection and video camera call-up and recording. Video cameras shall be tested for resolution, light sensitivity, focus, and where applicable, PTZ control. The graphical user interface (GUI) 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.

 © 2012 BICSI®

System Testing, continued

Burn-in Period

Prior to scheduling the final acceptance test, the commissioning technician should power up and operate each of the systems during a burn-in period. During this burn-in period, each system should be powered and 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.

Acceptance Testing

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. All access control points, intrusion detection points, video cameras, and intercom systems require testing and observation to ensure that they operate as required in the construction documents. In order to account for all lighting conditions, video cameras must be examined during the day and at night. 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. Acceptance testing is to be complete and test documentation approved by the client prior to the project completion.

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.

Client Staff Training

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.

Warranty Period

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.

Systems (e.g., IDS) might perform differently under various weather conditions and therefore should be tested to the fullest extent possible under all conditions.

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.

 © 2012 BICSI®



Appendix A
Codes, Standards, Regulations, and Organizations

Appendix A describes the codes and standards that an information technology systems (ITS) designer and installer must be aware of for the design and construction process of the ITS. Appendix A details the sources of codes and standards and lists important international, multinational/regional, and country-specific codes and standards.

Table of Contents

Introduction A-1
Construction A-2
Codes, Regulations, and Directives A-2
State Regulations A-3
Municipal/Local Regulations A-3
Special Applications A-3
Standards A-4
Standardization Efforts A-5
United States (U.S.) Standards Development A-5
International Standards Development A-5
Independent Standards-Setting Organizations A-5

International Codes and Standards A-6
International Code Council (ICC) A-6
International Organization for Standardization (ISO) A-6
International Electrotechnical Commission (IEC) A-7
International Organization for Standardization/International Electrotechnical Commission Joint Technical Committee 1 (ISO/IEC JTC1) A-7
Institute of Electrical and Electronics Engineers® (IEEE®) A-8
Project 802 . . . . . A-9
802.1 *Local Area Network* (*LAN*)/*Metropolitan Area Network* (*MAN*) *Bridging and Management* A-10
802.1 Working Projects A-11
802.3 *Part 3: Carrier Sense Multiple Access with Collision Detection* (*CSMA/CD*) *Access Method and Physical Layer Specifications* A-13
802.3 Working Projects A-15
802.11 *Wireless LAN Medium Access Control* (*MAC*) *and Physical Layer* (*PHY*) *Specifications* A-16
802.11 Working Projects A-17
802.15 *Wireless Personal Area Networks* (*WPANs*) A-18
802.16 *Broadband Wireless Metropolitan Area Networks* (*WMANs*) A-21
802.17 Resilient Packet Ring Working Group (RPRWG) A-22
802.18 Radio Regulatory Technical Advisory Group (RR-TAG) A-23
802.19 Coexistence Technical Advisory Group (TAG) A-23
802.20 Mobile Broadband Wireless Access (MBWA) Working Group A-23
802.21 Handoff/Handover Working Group A-24
802.22 Wireless Regional Area Networks (WRAN) Working Group A-25

802.23 Emergency Services Working Group A-26
P802 Handoff Executive Committee Study Group A-26
P802 Link Security Executive Committee Study Group A-26

Regional Codes and Standards A-27

Australia/New Zealand Codes and Standards A-27
Countries of the Americas Codes and Standards A-27
The Inter-American Telecommunication Commission (CITEL) A-27
European Codes and Standards A-28
Comité Européen de Normalisation Electrotechnique (CENELEC) A-28
CENELEC EN 50098 Series A-29
CENELEC EN 50173 Series A-30
CENELEC EN 50174 Series A-33
CENELEC EN 50310:2010 *Application of Equipotential Bonding and Earthing in Buildings with Information Technology Equipment* A-36
CENELEC EN 62305-1:2011 *Protection Against Lightning—Part 1 General Principles* A-37

National Codes and Standards A-38

Australian Codes and Standards A-38
Australian Communications and Media Authority (ACMA) A-38
Brazilian Codes and Standards A-38
Associacão Brasileira de Normas Técnicas (ABNT) A-38
Agência Nacional de Telecomunicações (ANATEL) A-40
Canadian Codes and Standards A-41
Standards Council of Canada (SCC) A-41
Canadian Standards Association (CSA®) A-41
National Research Council of Canada, Institute for Research in Construction (NRC-IRC) A-43
French Codes and Standards A-43
Union Technique de l'Ectricite et de la Communication (UTE) A-43
Japanese Codes and Standards A-44
Japanese Standards Association A-44
United Kingdom (UK) Codes and Standards A-44
British Standards Institution (BSI) A-44

 © 2012 BICSI®

United States (U.S.) Codes and Standards A-46
American National Standards Institute (ANSI) A-46
Americans with Disabilities Act (ADA) A-46
BICSI® A-46
Federal Communications Commission (FCC) A-47
IEEE C2-2012 *National Electrical Safety Code®* (*NESC®*) A-48
Insulated Cable Engineers Association (ICEA) A-50
National Electrical Contractors Association (NECA) A-51
National Fire Protection Association® (NFPA®) A-51
NFPA 70 *National Electrical Code®* (*NEC®*) A-52
Project Management Institute (PMI) A-56
Rural Utilities Service (RUS) A-56
Society of Cable Telecommunications Engineers (SCTE) A-57
Telecommunications Industry Association (TIA) A-58

Enforcement of United States (U.S) Building Codes, Standards, and Regulations A-62

Overview A-62
Double Requirements A-62
Local Applications of National Standards A-62
Government and Military Construction A-63
Federal Safety Health Standards A-64

Regulations and Standards for Wireless Transmission A-66

Wireless Regulations, Standards, Codes, and Organizations A-66

Wireless Standards Development Organizations A-67

Association of Radio Industries and Businesses (ARIB) A-67
European Telecommunications Standards Institute (ETSI) A-67
Federal Aviation Administration (FAA) A-68
Federal Communications Commission (FCC) A-68
Industry Canada A-68
Institute of Electrical and Electronics Engineers® (IEEE®) A-68
International Civil Aviation Organization (ICAO) A-68
International Electrotechnical Commission (IEC) A-68
International Organization for Standardization (ISO) A-68
Occupational Safety and Health Administration (OSHA) A-69
Telecommunications Industry Association (TIA) A-69
Telecommunications Technology Association (TTA) A-69
Telecommunication Technology Committee (TTC) A-69

United States (U.S.) Approval of Electrical Products and Equipment . . A-70
Product Certification A-70
Product Ratings A-70
Listed A-70
Classified A-70
Recognized A-71
Verified A-71
Test Standards A-71
Canadian Approval of Electrical Products and Equipment A-72
Product Certification A-72
European Union CE (conformité européenne) Mark A-72

Figures

Figure A.1 Conformité européenne (CE) mark A-72

Tables

Table A.1 Relationship between series EN 50174 and other design standards A-28
Table A.2 Sections of the *Canadian Electrical Code* A-42
Table A.3 Federal Communications Commission documents A-47
Table A.4 *NESC*®parts, sections, and rules applicable to telecommunications distribution requirements A-49
Table A.5 *NEC*®2011 chapters, articles, and sections that impact telecommunications installation A-53
Table A.6 Federal safety health standards A-64
Table A.7 Federal Communications Commission regulations A-67

 © 2012 BICSI®

Introduction

Nothing impacts the design and construction of a telecommunications network more than codes, standards, and regulatory acts. The information technology systems (ITS) designer and installer must be familiar with the electrical, communications, safety and building codes, standards, directives, and regulations for the nation, region, and municipality in which the design and installation work is performed. The ITS designer and installer must be aware of the critical importance of compliance with codes and standards.

In recent years, national, regional, and international standards-making bodies have joined efforts to harmonize the standards affecting information communication systems. These efforts, along with the technological developments that impact standards, codes, and regulations, maintain the dynamic nature of the documents.

Codes and standards are considered living documents because they are continually reviewed and revised. Codes, such as the *National Electrical Code*® (*NEC*®) in the United States, are typically revised every three years, and standards are revised every four to seven years, depending on the technology. The ITS designer must follow the changes in these dynamic documents.

Continuous standards harmonization efforts do not guarantee that all of the unique requirements for a specific design work area are covered. Since other disciplines (e.g., data processing, telephony, construction, architecture) are involved in the telecommunications design, the ITS designer should also be knowledgeable about these related codes, standards, and local and national regulations.

Therefore, the ITS designer must follow the rules that govern:

- Local carriers.
- Access providers (APs) and service providers (SPs).
- Telecommunications industry.
- Postal, telegraph, and telephone (PTT).

To aid ITS designers and installers, this appendix provides information on the critical codes, standards, and regulations encountered routinely in performing their duties. Information is also provided on standards that may be encountered for specific applications (e.g., outside plant, wireless), which are not necessarily included in all projects.

Construction

In the United States, Canada, and many other countries, building codes and standards regulate the construction industry. The local authority having jurisdiction (AHJ) normally enforces the codes, standards, and legal regulations for the jurisdiction.

Codes and standards encompass most, if not all, aspects of the construction industry. Installation methods and products must conform to local regulatory, code, and standards requirements.

ITS designers and installers must have a thorough knowledge of the applicable sections of these codes that affect telecommunications. Because this topic is complex, a separate section in this appendix details the various code authorities, standards committees, and reference sources.

Be aware that these codes and standards are updated regularly. It is the responsibility of the ITS designer and installer to follow the changes.

Codes, Regulations, and Directives

Codes pertain to:

- Electricity.
- Building.
- Fire.
- Other safety issues.

The purpose of codes is to ensure the:

- Practical safeguarding of persons and property from hazards.
- Quality of construction.

The *NEC*® in the United States and the *Canadian Electrical Code (CEC)* in Canada are issued to provide the criteria for minimizing the risk of electrical shock, fires, and explosions from electrical installations. Codes, when adopted by an AHJ, have the force of law and regulatory powers.

An AHJ may be a specific code authority (e.g., electrical inspector, building inspector, fire marshal). Typically, more than one AHJ will be involved on the project site because of different aspects requiring review and approval. The ITS designer and installer must meet with and comply with their specific concerns.

State, provincial, municipal, and local codes may be more restrictive than national codes and regulations and, therefore, take precedence. The order or hierarchy of code compliance should be in full conformance to local, state, and national codes.

In the European Union (EU), a set of regulations titled "Directives" take precedence. Some examples of these regulations are Construction Products Directive and Electromagnetic Compatibility Directive.

Within each country, building regulations and other government-mandated regulations are enforced.

 © 2012 BICSI®

State Regulations

At the state level in the United States, many public utility/service commissions issue their own rules in addition to monitoring tariffs. State rules are generally in accordance with FCC regulations.

The state commissions' rules and SP tariffs are available to the public. Certain sections of these rules and tariffs deal with installing telecommunications cabling and cable facilities on private and public property.

Municipal/Local Regulations

Other regulations that may affect the installation of the ITS designer's and installer's work include:

- Licensing.
- Permitting.

These may involve additional costs or fees within the state or municipality in order to meet the criteria for actual implementation of the project.

Special Applications

The ITS designer and installer must be aware of any special restrictions or conditions in specialized environments such as:

- Health care facilities.
- Manufacturing facilities.
- Chemical and industrial areas:
  - Explosion proofing.
- Emergency management areas (911).
- Earthquake prone areas:
  - Seismic restraint criteria.
  - Earthquake zone categories.

Standards

A standard is a document, developed and approved by consensus, that establishes requirements for processes, procedures, practices, or methods. Additionally, standards may be established for the selection, application, and design of materials, equipment, products, and services.

One of the purposes of a standard is to ensure a minimal level of acceptable performance. While codes and safety standards address the safety of persons and property in the installation or use of a telecommunications or other system, codes do not ensure the system functionality. Codes often reference numerous standards to ensure the minimum functional requirements of a given material or component.

Safety standards provide the criteria for safety testing of a component or system. Performance and safety standards are typically test standards. Test standards provide uniform rules for the object, methods, and acceptable results of testing. For example, in the United States, the *NEC*® requires that a cable placed in space and defined as a plenum or other air-handling space must be listed for that purpose.

This listing is given to the material that meets a specific safety test standard of minimum acceptable requirements for:

- Flammability.
- Smoke generation.
- Smoke density.
- Amount of toxic gasses generated under flame.

Other standards are not written for safety requirements, but they are written for product performance or conformance.

Standards are established as a basis to quantify, compare, measure, or specify:

- Capacity.
- Quantity.
- Content.
- Extent.
- Value.
- Quality.

As with most standards, telecommunications standards are typically voluntarily adopted. They represent industry consensus on requirements and best practices. A significant benefit of standards in the telecommunications industry is the ensured interoperability of components and systems by multiple manufacturers.

For example, if a manufacturer of network interface cards (NICs) does not adhere to standards such as IEEE 802.3, then the product may not properly function with other standards-compliant products.

 © 2012 BICSI®

Standardization Efforts

United States (U.S.) Standards Development

In 1985, the U.S. Computer Communications Industry Association (CCIA) asked the Electronic Industries Association (EIA) to develop standards for telecommunications cabling. EIA accepted the task, and the project was assigned to the Engineering Committee TR 42 (formerly TR 41.8).

In 1988, the telecommunications sector of the EIA (specifically the TR and Fiber Optics [FO] committees and subcommittees) became the Telecommunications Industry Association (TIA) under the TIA technical council. TIA conducted the standards activities through EIA until it no longer needed its sponsorship for National Standard recognition.

Many TIA standards that govern telecommunications cabling infrastructure are accredited through the American National Standards Institute (ANSI). As such, they have a broad industry acceptance throughout the United States.

Associations, such as the Alliance for Telecommunication Industry Solutions (ATIS), BICSI®, and the Society for Cable Telecommunications Engineers (SCTE), have developed standards that further define aspects of telecommunications cabling, cabling design, and cabling installation.

International Standards Development

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) jointly oversee international standardization of telecommunications cabling. These organizations form a specialized system for worldwide standardization.

National bodies that are members of ISO or IEC participate in the development of international standards through committees that deal with specific technical fields. ISO and IEC committees collaborate with other international governmental and nongovernmental organizations to develop harmonized international requirements.

In the field of information technology (IT), ISO and IEC have established a joint technical committee, which is known as ISO/IEC JTC 1.

Independent Standards-Setting Organizations

A number of independent organizations specialize in establishing, certifying, and maintaining standards. Many industry trade organizations and national and international standards-setting bodies develop standards. Some of these organizations are listed in this appendix.

International Codes and Standards

International Code Council (ICC)

The ICC was established in 1994 as a nonprofit organization committed to developing a single set of all-inclusive and coordinated national model construction codes. The ICC was founded by the International Conference of Building Officials (ICBO), Building Officials and Code Administrators International (BOCA), and Southern Building Code Congress International (SBCCI).

The mission of the ICC is to provide the highest quality codes, standards, products, and services for all concerned with the safety and performance of the built environment.

The ICC has developed and made available the following international codes and standards:

- ICC/ANSI A.117.1 – Accessible and Useable Buildings and Facilities (2009)
- ICC Performance Code™
- International Building Code®
- International Energy Conservation Code®
- International Existing Building Code®
- International Fire Code®
- International Fuel Gas Code®
- International Mechanical Code®
- International Plumbing Code®
- International Private Sewage Disposal Code®
- International Property Maintenance Code®
- International Residential Code®
- International Wildland – Urban Interface Code™
- International Zoning Code®

International Organization for Standardization (ISO)

ISO has a membership of 163 national standards bodies from countries large and small, industrialized, developing, and in transition in all regions of the world.

ISO produces documents and standards that affect telecommunications and is responsible formany standards, such as the Open Systems Interconnection (OSI) model. The OSI model provides criteria for product development that is interoperable. The ITS designer and installer should be familiar with the standardized signaling and connection interface for various network-accessing protocols.

 © 2012 BICSI®

International Electrotechnical Commission (IEC)

IEC is a leading global organization that prepares and publishes international standards for electrical, electronic, optical fiber, and related technologies. These standards serve as a basis for national standardization and as reference for drafting international tenders and contracts.

Through its members, IEC promotes international cooperation regarding electrotechnical standardization and related matters (e.g., standards, conformity assessment).

International Organization for Standardization / International Electrotechnical Commission Joint Technical Committee 1 (ISO / IEC JTC1)

In 1988, the ISO and the IEC created a Joint Technical Committee on Information Technology (ISO/IEC JTC1). ISO/IEC JTC1 produces standards that affect telecommunications.

The most relevant are:

- ISO/IEC 11801 Ed 2:2010, *Information Technology—Generic Cabling for Customer Premises*.
- ISO/IEC 14763-1:2005, *Information Technology—Implementation and Operation of Customer Premises Cabling—Part 1: Administration*.
- ISO/IEC 14763-2:2012, *Information Technology—Implementation and Operation of Customer Premises Cabling—Part 2: Planning and Installation.*
- ISO/IEC 14763-3:2009, *Information Technology—Implementation and Operation of Customer Premises Cabling—Part 3: Testing of Optical Fibre Cabling*.
- ISO/IEC 15018:2009, *Information Technology—Generic Cabling for Homes.*
- ISO/IEC 18010:2005, *Information Technology—Pathways and Spaces for Customer Premises Cabling*.
- ISO/IEC 24702:2009, *Information Technology—Generic Cabling—Industrial Premises.*
- ISO/IEC 24764 Ed 1.0:2010, *Information Technology—Generic Cabling Systems For Data Centres*.

Institute of Electrical and Electronics Engineers® (IEEE®)

IEEE® is a nonprofit, technical professional association with more than 400,000 individual members in 150 countries. IEEE is an authority in technical areas ranging from computer engineering and telecommunications to consumer electronics. IEEE has a portfolio of nearly 1300 active standards and projects under development.

The IEEE publishes many documents that affect telecommunications.
Some important standards are:

- IEEE C62.41.1™:2008, *IEEE Guide on the Surge Environment in Low-Voltage (1000 V and Less) AC Power Circuits.*
- IEEE C62.41.2™:2002, *IEEE Recommended Practice on Characterization of Surges in Low-Voltage (1000 V and Less) AC Power Circuits.*
- IEEE PC62.41.2:2002/Cor 1, *IEEE Recommended Practice on Characterization of Surges in Low-Voltage (1000 V and Less) AC Power Circuits—Corrigendum 1.*
- IEEE C62.43™:2010, *Application of Surge Protectors Used in Low-Voltage (Equal to or Less than 1000 Voltage, rms, or 1200 V, DC) Data, Communications, and Signaling Circuits.*
- IEEE C62.45™:2008, *IEEE Recommended Practice on Surge Testing for Equipment Connected to Low-Voltage (1000 V and Less) AC Power Circuits.*
- IEEE 81:1983, *IEEE Guide for Measuring Earth Resistivity, Ground Impedance, and Earth Surface Potentials of a Ground System—Part 1: Normal Measurements.*
- IEEE 142™:2007, *IEEE Recommended Practice for Grounding of Industrial and Commercial Power Systems—Green Book™.*
- IEEE 446:1995, *IEEE Recommended Practice for Emergency and Standby Power Systems for Industrial and Commercial Applications—Orange Book™.*
- IEEE 450:2010, *IEEE Recommended Practice for Maintenance, Testing, and Replacement of Vented Lead-Acid Batteries for Stationary Applications.*
- IEEE 1100:2005, *IEEE Recommended Practice for Powering and Grounding Electronic Equipment—Emerald Book™.*
- IEEE 1184:2006, *IEEE Guide for Batteries for Uninterruptible Power Supply Systems.*
- IEEE 1187:2002, *IEEE Recommended Practice for Installation Design and Installation of Valve-Regulated Lead-Acid Storage Batteries for Stationary Applications.*
- IEEE P1187:2007, *Recommended Practice for Installation Design and Installation of Valve-Regulated Lead-Acid Batteries for Stationary Applications.*

 © 2012 BICSI®

Institute of Electrical and Electronics Engineers® (IEEE®), continued

- IEEE 1188:2005, *IEEE Recommended Practice for Maintenance, Testing, and Replacement of Valve Regulated Lead-Acid (VRLA) Batteries for Stationary Applications.*
- IEEE P1188a:2010, *Recommended Practice for Maintenance, Testing, and Replacement of Valve-Regulated Lead-Acid (VRLA) Batteries for Stationary Applications—Amendment 1: Updated VRLA Maintenance Considerations.*
- IEEE 1394:2008, *IEEE Standard for a High-Performance Serial Bus.*
- IEEE P1394d:2009, *IEEE Standard for a High-Performance Serial Bus—Amendment: IEEE 1394 Single-Mode Fiber Physical Medium (PMD) Specification.*
- IEEE 1394.1:2009, *IEEE Standard for High-Performance Serial Bus Bridges.*
- IEEE 1394.3™:2008, *IEEE Standard for a High-Performance Serial Bus Peer-to-Peer Data Transport Protocol (PPDT).*

Project 802

The ITS designer and installer should be familiar with the Physical Layer signaling and connectivity for LAN standards under the IEEE Project 802.

Project 802 was organized specifically for the development of LAN and metropolitan area network (MAN) standards. The Local and Metropolitan Area Network Standards Committee (LMSC) develops LAN and MAN standards, primarily for the lowest two layers of the OSI Reference Model. The LMSC coordinates with other national and international standards groups with some standards now published by ISO as international standards. The objective of the LMSC is to develop standards that will be accepted by organizations using LANs as well as LAN hardware and software vendors. This encourages customers to ask for and manufacturers to develop standardized products, ensuring interoperability among products obtained from different vendors.

The working groups under the LMSC are identified as:

- Active—Standards published, continuing work.
- Hibernating—Standards published, but inactive. (At the time of this revision, the 802.17, Resilient Packet Ring (RPR) Working Group, and 802.20, Mobile Broadband Wireless Access (MBWA) Working Group, are currently hibernating.)
- Disbanded—Did not publish a standard.

The LMSC working groups and some of their respective standards (including drafts) within IEEE 802 are described in the following sections.

Institute of Electrical and Electronics Engineers® (IEEE®), continued

802.1 *Local Area Network (LAN) / Metropolitan Area Network (MAN) Bridging and Management*

- IEEE 802.1AB™:2009, *IEEE Standard for Local and Metropolitan Area Networks—Station and Media Access Control Connectivity Discovery.*
- IEEE 802.1D™:2004 (R2011), *IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges*.
- IEEE 802.1Q:2011, *IEEE Standard for Local and Metropolitan Area Networks—Virtual Bridged Local Area Networks*.
- IEEE 802.1Q:2005/Cor 1:2008, IEEE *Standard for Local and Metropolitan Area Networks- Virtual Bridged Local Area Networks—Amendment 07: Multiple Registration Protocol-Corrigendum 1: Corrections to the Multiple Registration Protocol.*
- IEEE 802.1Qau:2010, *IEEE Standard for Local and Metropolitan Area Networks—Virtual Bridged Local Area Networks—Amendment 13: Congestion Notification*.
- IEEE 802.1Qav:2009, *IEEE Standard for Local and Metropolitan Area Networks—Virtual Bridged Local Area Networks—Amendment 12: Forwarding and Queuing Enhancements for Time-Sensitive Streams.*
- IEEE 802.1Qaw:2009, *IEEE Standard for Local and Metropolitan Area Networks— Virtual Bridged Local Area Networks—Amendment 9: Management of Data Driven and Data Dependent Connectivity Faults.*
- IEEE 802.1X™:2010, *Standard for Local and Metropolitan Area Networks—Port-Based Network Access Control*.
- IEEE 802.1ad:2005, *IEEE Standard for Local and Metropolitan Area Networks—Virtual Bridged Local Area Networks—Amendment 4: Provider Bridge*.
- IEEE 802.1AE™:2006, *IEEE Standard for Local and Metropolitan Area Networks—Media Access Control (MAC) Security*.
- IEEE 802.1ag:2007, *IEEE Standard for Local and Metropolitan Area Networks—Virtual Bridged Local Area Networks—Amendment 5: Connectivity Fault Management.*
- IEEE 802.1ah:2008, *IEEE Standard for Local and Metropolitan Area Networks—Virtual Bridged Local Area Networks—Amendment 6: Provider Backbone Bridges*.
- IEEE P802.1aj:2009, *IEEE Draft Standard for Local and Metropolitan Area Networks—Virtual Bridged Local Area Networks—Amendment 8: Two-Port Media Access Control (MAC) Relay.*
- IEEE 802.1ak:2007, *IEEE Standard for Local and Metropolitan Area Networks—Virtual Bridged Local Area Networks—Amendment 7: Multiple Registration Protocol.*

Institute of Electrical and Electronics Engineers® (IEEE®), continued

- IEEE 802.1ap:2008, *IEEE Standard for Local and Metropolitan Area Networks—Virtual Bridged Local Area Networks—Amendment 8: Management Information Base (MIB) Definitions for VLAN Bridges.*
- IEEE 802.1AR™:2009, *IEEE Standard for Local and Metropolitan Area Networks—Secure Device Identity.*
- IEEE 802.1AX™:2008, *IEEE Standard for Local and Metropolitan Area Networks—Link Aggregation.*
- IEEE 802.1AS™:2011, *IEEE Standard for Local and Metropolitan Area Networks— Timing and Synchronization for Time-Sensitive Applications in Bridged Local Area Networks.*
- IEEE 802.1Qat:2010, *IEEE Standard for Local and Metropolitan Area Networks— Virtual Bridged Local Area Networks Amendment 14: Stream Reservation Protocol (SRP).*
- IEEE 802.1Qay:2009, *IEEE Standard for Local and Metropolitan Area Networks— Virtual Bridged Local Area Networks Amendment 10: Provider Backbone Bridge Traffic Engineering.*

802.1 Working Projects

The 802.1 working group has two active groups, Internetworking and Security, which are responsible for the following projects:

- IEEE P802.1Qaz:2009, *IEEE Draft Standard for Local and Metropolitan Area Networks—Virtual Bridged Local Area Networks Amendment: Enhanced Transmission Selection for Bandwidth Sharing Between Traffic Classes.*
- IEEE P802.1Qbb:2008, *IEEE Draft Standard for Local and Metropolitan Area Networks— Virtual Bridged Local Area Networks Amendment: Priority-based Flow Control.*
- IEEE P802.1Qbc:2009, *IEEE Draft Standard for Local and Metropolitan Area Networks— Virtual Bridged Local Area Networks Amendment: Provider Bridging—Remote Customer Service Interfaces.*
- IEEE P802.1Qbe:2009, *IEEE Draft Standard for Local and Metropolitan Area Networks— Virtual Bridged Local Area Networks Amendment: Multiple Backbone Service Instance Identifier (I-SID) Registration Protocol (MIRP).*
- IEEE P802.1Qbf:2009, *IEEE Standard for Local and Metropolitan Area Networks—Virtual Bridged Local Area Networks Amendment: Provider Backbone Bridge Traffic Engineering (PBB-TE) Infrastructure Segment Protection.*
- IEEE P802.1Qbg:2009, *Standard for Local and Metropolitan Area Networks—Virtual Bridged Local Area Networks Amendment: Edge Virtual Bridging.*
- IEEE P802.1Qbh:2009, *Standard for Local and Metropolitan Area Networks—Virtual Bridged Local Area Networks Amendment: Bridge Port Extension.*

Institute of Electrical and Electronics Engineers® (IEEE®), continued

- IEEE P802.1Qbp:2011, *IEEE Computer Society/LAN/MAN Standards Committee Title: Standard for Local and Metropolitan Area Networks—Virtual Bridged Local Area Networks Amendment: Equal Cost Multiple Paths (ECMP).*
- IEEE P802.1AC:2005, *Standard for Media Access Control (MAC) Service Definition*.
- IEEE 802.1aq:2005, *Standard for Local and Metropolitan Area Networks—Virtual Bridged Local Area Networks—Amendment 8: Shortest Path Bridging.*
- IEEE P802.1AS-2011/Cor 1:2011, *IEEE Standard for Local and Metropolitan Area Networks—Timing and Synchronization for Time-Sensitive Applications in Bridged Local Area Networks - Corrigendum 1: Technical and editorial corrections.*
- IEEE P802.1ASbt:2011, *IEEE Standard for Local and Metropolitan Area Networks—Timing and Synchronization for Time-Sensitive Applications in Bridged Local Area Networks Amendment: Enhancements and performance improvements.*
- IEEE P802.1AXbk:2010, *IEEE Standard for Local and Metropolitan Area Networks—Link Aggregation Amendment: Protocol Addressing.*
- IEEE P802.1BA:2008, *Standard for Local and Metropolitan Area Networks—Audio Video Bridging* (*AVB*) *Systems*.
- IEEE P802.1AXbq:2011, *IEEE Standard for Local and Metropolitan Area Networks—Link Aggregation Amendment: Distributed Resilient Network Interconnect.*
- IEEE P802.1BR:2011, *Standard for Local and Metropolitan Area Networks—Virtual Bridged Local Area Networks—Bridge Port Extension.*
- IEEE P802.1Q-2011/Cor 2, *IEEE Standard for Local and Metropolitan Area Networks—Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks—Corrigendum 2: Technical and Editorial Corrections.*
- IEEE P802.1Qbp:2011, *Standard for Local and Metropolitan Area Networks—Virtual Bridged Local Area Networks Amendment: Equal Cost Multiple Paths (ECMP).*
- IEEE P802.1Qbv:2012, *Standard for Local and Metropolitan Area Networks—Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks Amendment: Enhancements for Scheduled Traffic.*
- IEEE P802.1Xbx:2012, *Standard for Local and Metropolitan Area Networks Port—Based Network Access Control Amendment: MAC Security Key Agreement Protocol (MKA) Extensions.*
- IEEE P802.1AEbn: 2011, *IEEE Draft Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Security Amendment 1: Galois Counter Mode—Advanced Encryption Standard—256 (GCM-AES-256) Cipher Suite*.
- IEEE P802.1AEbw:2012, *Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Security Amendment: Extended Packet Numbering.*
- IEEE P802.1AX:2012, *Standard for Local and Metropolitan Area Networks—Link Aggregation.*
- IEEE P802.1Qbu:2012, *Standard for Local and Metropolitan Area Networks—Media Access Control (MAC) Bridges and Virtual Bridged Local Area Networks Amendment Frame Preemption.*

Institute of Electrical and Electronics Engineers® (IEEE®), continued

802.3 *Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications*

- IEEE 802.3™:2008, *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks— Specific Requirements—Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications.*
- IEEE 802.3™:2008/Cor 1:2009, *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications Corrigendum 1: Timing Considerations for PAUSE Operation.*

The IEEE 802.3 working group is responsible for developing standards and recommended practices for access control and physical signaling in the carrier sense multiple access with collision detection (CSMA/CD) form of network communications. This group specifies the Physical and Data Link Layer standards for LANs using a CSMA/CD access method and a bus topology. Such LANs include Ethernet, Fast Ethernet, Gigabit Ethernet, and 10 Gigabit Ethernet.

The 802.3 standard defines the Physical Layer implementations among a variety of physical media.

It incorporates the following previously published standards:

- IEEE 802.3x—*Specification for Full-Duplex Operation.*
- IEEE 802.3y—*Physical Layer Specifications for 100 Mb/s Operation Over Two Pairs of Category 3 or Higher Twisted-Pair Cable.*
- IEEE 802.3z—*Specification for 1000 Mb/s (Gigabit Ethernet) Operation Over Optical Fiber Cable.*
- IEEE 802.3ab—*Specification for 1000 Mb/s (Gigabit Ethernet) Operation Over Four Pairs of Category 5 or Higher Twisted-Pair Cable, Type 100BASE-T.*
- IEEE 802.3ac—*Ethernet Frame Extensions for Virtual Local Area Networks (VLANs) and Tagging On 802.3 Networks*.
- IEEE 802.3ad—*Aggregation of Multiple Link Segments.*
- IEEE 802.3ae—*10 Gb/s Operation.*
- IEEE 802.3af—*Data Terminal Equipment (DTE) Power Via Media Dependent Interface* (MDI).
- IEEE 802.3ah—*Media Access Control Parameters, Physical Layers, and Management Parameters for Subscriber Access Networks (such as Ethernet Passive Optical Network [EPON] and Ethernet over DSL).*
- IEEE 802.3ak—*Physical Layer and Management Parameters for 10 Gb/s Operation, Type 10GBASE-CX4*.
- IEEE 802.3an—*Amendment 1: Physical Layer and Management Parameters for10 Gb/s Operation, Type 10GBASE-T.*

Institute of Electrical and Electronics Engineers® (IEEE®), continued

- IEEE 802.3ap—*Amendment 4: Ethernet Operation over Electrical Backplanes.*
- IEEE 802.3aq—*Amendment 2: Physical Layer and Management Parameters for10 Gb/s Operation, Type 10GBASE-LRM.*
- IEEE 802.3as—*Amendment 3: Frame Format Extensions.*

The 802.3 working group is also responsible for the following approved amendments:

- IEEE 802.3at™:2009, *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems Local and Metropolitan Area Networks—Specific requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications Amendment 3: Data Terminal Equipment (DTE) Power via the Media Dependent Interface (MDI) Enhancements.*
- IEEE 802.3av™:2009, *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks— Specific Requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications Amendment 1: Physical Layer Specifications and Management Parameters for 10 Gb/s Passive Optical Networks.*
- IEEE 802.3at™:2009, *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications—Amendment: Data Terminal Equipment (DTE) Power Via Media Dependent Interface (MDI) Enhancements.*
- IEEE 802.3az:2010, *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications Amendment: Media Access Control Parameters, Physical Layers and Management Parameters for Energy-Efficient Ethernet.*
- IEEE 802.3ba™:2010, *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks— Specific Requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications Amendment 4: Media Access Control Parameters, Physical Layers, and Management Parameters for 40 Gb/s and 100 Gb/s Operation.*
- IEEE 802.3bc™:2009, *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications Amendment 2: Ethernet Organizationally Specific Type, Length, Value (TLVs).*

 © 2012 BICSI®

Institute of Electrical and Electronics Engineers® (IEEE®), continued

- IEEE 802.3bd™:2011, *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications—Amendment 8: MAC Control Frame for Priority-based Flow Control.*
- IEEE 802.3bf™:2011, *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—SpecificRequirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications Amendment 7: Media Access Control (MAC) Service Interface and Management Parameters to Support Time Synchronization Protocols.*
- IEEE 802.3bg™:2011, *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications Amendment 6: Physical Layer and Management Parameters for Serial 40 Gb/s Ethernet Operation Over Single Mode Fiber.*
- IEEE 802.3.1™:2011, *IEEE Standard for Management Information Base (MIB) Definitions for Ethernet.*
- IEEE 802.3-2008/Cor 1, *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks— Specific requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications Corrigendum 1: Timing Considerations for PAUSE Operation.*

802.3 Working Projects

The 802.3 working group is also responsible for the following initiatives:

- IEEE P802.3:2011, *Standards for Ethernet*.
- IEEE P802.3bj:2011, *IEEE Standard for Information Technology-Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications Amendment: Physical Layer Specifications and Management Parameters for 100 Gb/s Operation Over Backplanes and Copper Cables.*
- IEEE P802.3bk:2011, *Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications Amendment: Physical Layer Specifications and Management Parameters for Extended Ethernet Passive Optical Networks.*

Institute of Electrical and Electronics Engineers® (IEEE®), continued

802.11 *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*

- IEEE 802.11:2012, *IEEE Approved Draft Standard for Information Technology— Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.*
- IEEE 802.11k™:2008, *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between System—Local and Metropolitan Area Networks— Specific Requirement Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications—Amendment 1: Radio Resource Measurement of Wireless LANs.*
  - IEEE 802.11k is a standard for radio resource measurement. It will increase the manageability of WLANs by measuring radio and network information, which can be used by network management applications.
- IEEE 802.11n™:2009, *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications—Amendment 5: Enhancements for Higher Throughput.*
  - IEEE 802.11n is the next step in WLAN standards. The 802.11a and 802.11g standards both deliver a maximum 54 megabits per second (Mb/s). The proposed 802.11n specification, which will use the same 5 GHz frequency range as 802.11a, will raise the maximum throughput to 100 Mb/s or higher. This will improve the speed of wireless multimedia applications.
- IEEE 802.11p™:2010, *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks— Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications—Amendment 7: Wireless Access in Vehicular Environments.*
- IEEE 802.11r™:2008, *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks— Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications—Amendment 2: Fast Basic Service Set (BSS) Transition.*
- IEEE 802.11u™–2011, *IEEE Standard for Information Technology— Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications—Amendment 9: Interworking with External Networks.*
- IEEE 802.11v™:2011, *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications—Amendment 8: Wireless Network Management.*

 © 2012 BICSI®

Institute of Electrical and Electronics Engineers® (IEEE®), continued

- IEEE 802.11w™:2009, *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks— Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications—Amendment 4: Protected Management Frames.*
- IEEE 802.11y™:2008, *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications—Amendment 3: 3650-3700 MHz Operation in USA.*
- IEEE 802.11z™:2010, *IEEE Standard for Information Technology Telecommunications and Information Exchange Between Systems Local and Metropolitan Area Networks—Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 7: Extensions to Direct-Link Setup (DLS).*
- IEEE 802.11s™:2011**,** *IEEE Standard for Information Technology— Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications—Amendment 10: Mesh Networking.*

802.11 Working Projects

The 802.11 working group is also responsible for the following initiatives:

- IEEE P802.11:2008, *IEEE Draft Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*.
- IEEE P802.11aa:2008, *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks— Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) | and Physical Layer (PHY) Specifications—Amendment: MAC Enhancements for Robust Audio Video Streaming.*
- IEEE P802.11ac:2008, *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks— Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications—Amendment: Enhancements for Very High Throughput for Operation in Bands Below 6GHz.*
- IEEE P802.11ad:2008, *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks— Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications—Amendment: Enhancements for Very High Throughput in the 60 GHz Band.*

Institute of Electrical and Electronics Engineers® (IEEE®), continued

- IEEE P802.11ae:2009, *Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications—Amendment: Prioritization of Management Frames.*
- IEEE P802.11af:2009, *Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications—Amendment: TV White Spaces Operation.*
- IEEE P802.11ah:2010, *Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Amendment—Sub 1 GHz License-Exempt Operation.*
- IEEE P802.11ai:2010, *IEEE Standard for Information Technology —Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Amendment- Fast Initial Link Setup.*
- IEEE P802.11mb:2007, *Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications—Amendment: Accumulated Maintenance Changes.*

802.15 *Wireless Personal Area Networks (WPANs)*

- IEEE 802.15.1™:2005 (R2010), *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks— Specific Requirements Part 15.1: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs).*
- IEEE 802.15™.2:2003 (R2009), *IEEE Recommended Practice for Information Technology— Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements Part 15.2: Coexistence of Wireless Personal Area Networks With Other Wireless Devices Operating in Unlicensed Frequency Bands.*
- IEEE 802.15.3™:2003 (R2008), *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements Part 15.3: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for High Rate Wireless Personal Area Networks (WPANs).*
- IEEE 802.15.3b™:2005 (R2008), *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements Part 15.3: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for High Rate Wireless Personal Area Networks (WPANs)—Amendment 1: MAC Sublayer.*

 © 2012 BICSI®

Institute of Electrical and Electronics Engineers® (IEEE®), continued

- IEEE 802.15.3c™:2009, *IEEE Amendment to IEEE Standard for Information Technology— Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements Part 15.3: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for High Rate Wireless Personal Area Networks (WPANs)—Amendment 2: Millimeter Wave Based Alternative Physical Layer Extension.*
- IEEE 802.15.4:2006, *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks— Specific Requirements Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs).*
- IEEE 802.15.4a:2007, *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks— Specific Requirements Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)—Amendment 1: Add Alternate PHYs.*
- IEEE 802.15.4c:2009, *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)—Amendment 2: Alternative Physical Layer Extensionto Support One or More of the Chinese 314-316 MHz, 430-434 MHz, and 779-787 MHz Bands.*
- IEEE 802.15.4d:2009, *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)—Amendment 3: Alternative Physical Layer Extension to Support the Japanese 950 MHz Bands.*
- IEEE 802.15.5™:2009, *IEEE Recommended Practice for Information Technology— Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements Part 15.5: Mesh Topology Capability in Wireless Personal Area Networks (WPANs).*

The 802.15 working group is also responsible for the following initiatives:

- IEEE P802.15.4:2011, *Standard for Local and Metropolitan Area Networks Part 15.4: Low Rate Wireless Personal Area Networks (LR-WPANs).*
- IEEE P802.15.4:2010/Cor 1, *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (WPANs)—Corrigendum 1.*

Institute of Electrical and Electronics Engineers® (IEEE®), continued

- IEEE P802.15.4e:2011, *IEEE Standard for Local and Metropolitan Area Networks—Part 15.4: Low Rate Wireless Personal Area Networks (LR-WPANs) Amendment to the MAC Sub-Layer.*
- IEEE P802.15.4f:2011, *IEEE Standard for Local and Metropolitan Area Networks—Part 15.4: Low Rate Wireless Personal Area Networks (LR-WPANs) Amendment: Active Radio Frequency Identification (RFID) System Physical Layer (PHY).*
- IEEE P802.15.4g:2011, *IEEE Standard for Local and Metropolitan Area Networks— Part 15.4: Low Rate Wireless Personal Area Networks (LR-WPANs) Amendment: Physical Layer (PHY) Specifications for Low Data Rate Wireless Smart Metering Utility Networks.*
- IEEE P802.15.4j:2010, *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks— Specific Requirements—Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (WPANs) Amendment: Alternative Physical Layer Extension to support Medical Body Area Network (MBAN) Services Operating in the 2360-2400 MHz band.*
- IEEE P802.15.4k:2010, *IEEE Standard for Local and Metropolitan Area Networks—Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (WPANs) Amendment— Physical Layer (PHY) Specifications for Low Energy, Critical Infrastructure Monitoring Networks (LECIM).*
- IEEE P802.15.6:2007, *Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements Part 15.6: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs)—Used in or Around a Body.*
- IEEE P802.15.7:2011, *IEEE Draft Standard for Short-Range Wireless Optical Communication Using Visible Light.*
- IEEE P802.15.4m:2011, *IEEE Standard for Local and Metropolitan Area Networks Part 15.4: Low Rate Wireless Personal Area Networks (LR-WPANs) Amendment: TV White Space Between 54 MHz and 862 MHz Physical Layer.*
- IEEE P802.15.4n:2012, *Standard for Local and Metropolitan Area Networks—Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment: Physical Layer Utilizing Dedicated Medical Bands in China.*
- IEEE P802.15.4p:2012, *Standard for Local and Metropolitan Area Networks—Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment: Positive Train Control (PTC) System Physical Layer.*
- IEEE P802.15.8, 2012, *Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Peer Aware Communications (PAC).*
- IEEE P802.15.9:2011, *Recommended Practice for Transport of Key Management Protocol (KMP) Datagrams.*

Institute of Electrical and Electronics Engineers® (IEEE®), continued

802.16 *Broadband Wireless Metropolitan Area Networks(WMANs)*

- IEEE 802.16™:2009, *IEEE Standard for Local and Metropolitan Area Networks—Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems*.
- IEEE 802.16.2™:2004 (R2010), *IEEE Recommended Practice for Local and Metropolitan Area Networks—Coexistence of Fixed Broadband Wireless Access Systems*.
- IEEE 802.16/Conformance04:2006, *IEEE Standard for Conformance to IEEE* 802.16 *Part 4: Protocol Implementation Conformance Statement (PICS) Proforma for Frequencies below 11 GHz.*
  - The downside of 802.16a (commonly referred to as worldwide interoperability for microwave access [WiMAX]) is that it is a fixed access system, meaning that users must mount a dish-like antenna outside their home or office to access it. To circumvent this issue, IEEE formed a study group to develop an extension to WiMAX called 802.16e. This extension introduces nomadic capabilities that allow users to connect to a wireless Internet SP (WISP), even when they roam outside their home or business.
- IEEE 802.16h™:2010, *IEEE Standard for Local and Metropolitan Area Networks—Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems—Improved Coexistence Mechanisms for License-Exempt Operation.*
- IEEE 802.16™j:2009, *IEEE Standard for Local and Metropolitan Area Networks—Part 16: Air Interface for Broadband Wireless Access Systems—Amendment 1: Multihop Relay Specification.*
- IEEE 802.16k™:2007, *IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Bridges—Amendment 2: Bridging of IEEE 802.16.*
- IEEE 802.16m™:2011, *IEEE Standard for Local and Metropolitan Area Networks—Part 16: Air Interface for Broadband Wireless Access Systems—Amendment 3: Advanced Air Interface.*
  - The 802.16 working group is splitting the base standard into 802.16 and 802.16.1. As a result, the amendments will also be split. The working group is currently responsible for the following initiatives:
- IEEE P802.16:2011, *Standard for Air Interface for Broadband Wireless Access Systems.*
- IEEE P802.16.1:2011, *Standard for Wireless MAN—Advanced Air Interface for Broadband Wireless Access Systems.*
- IEEE P802.16.1a:2011, IEEE *Standard for Wireless MAN—Advanced Air Interface for broadband Wireless Access Systems—Amendment: Higher Reliability Networks.*
- IEEE P802.16.1b:2011, *Standard for Wireless MAN—Advanced Air Interface for Broadband Wireless Access Systems—Amendment: Enhancements to Support Machine-to-Machine Applications.*

Institute of Electrical and Electronics Engineers® (IEEE®), continued

- IEEE P802.16n:2011, *Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Broadband Wireless Access Systems Amendment: Higher Reliability Networks.*
- IEEE P802.16p:2011, *Standard for Air Interface for Broadband Wireless Access Systems— Amendment: Enhancements to Support Machine-to-Machine Applications.*

802.17 Resilient Packet Ring Working Group (RPRWG)

NOTE: This working group is currently hibernating.

The IEEE 802.17 Resilient Packet Ring Working Group (RPRWG) defines a resilient packet ring access protocol for use in local, metropolitan, and wide area networks for transfer of data packets at rates scalable to many gigabit per second (Gb/s). The standard will use the existing Physical Layer specifications and develop new specifications where appropriate.

In MANs and WANs, optical fiber rings are widely deployed. These rings are currently using protocols that are neither optimized nor scalable to the demands of packet networks, including speed of deployment, bandwidth allocation and throughput, resiliency to faults, and reduced equipment and operational costs.

- IEEE 802.17™:2011, *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements Part 17: Resilient Packet Ring (RPR) Access Method and Physical Layer Specifications*.
- IEEE 802.17a™:2004, *IEEE Standard for Local and Metropolitan Area Networks—Media Access Control (MAC) Bridges—Amendment 1: Bridging of IEEE 802.17*.
- IEEE 802.17b™:2007, *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements Part 17: Resilient Packet Ring (RPR) Access Method and Physical Layer Specifications—Amendment 1: Spatially Aware Sublayer*.
- IEEE 802.17c™:2010, *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements Part 17: Resilient Packet Ring (RPR) Access Method and Physical Layer Specifications—Amendment 2: Protected Inter-ring Connection.*

Institute of Electrical and Electronics Engineers® (IEEE®), continued

802.18 Radio Regulatory Technical Advisory Group (RR-TAG)

IEEE 802 LMSC currently has six working groups with projects on standards for radio-based systems: 802.11 (WLANs), 802.15 (WPANs), 802.16 (WMANs), 802.20 (wireless mobility), 802.21 (handoff/interoperability between networks), and 802.22 (WRANs). The task of the Radio Regulatory Technical Advisory Group (RR-TAG) is to monitor and participate in the activities of these groups.

802.19 Coexistence Technical Advisory Group (TAG)

The IEEE 802.19 Coexistence Technical Advisory Group (TAG) develops and maintains policies defining the responsibilities of 802 standards developers to address the issues of coexistence with the existing standards and other standards under development. When required, the TAG offers assessments to the Sponsor Executive Committee (SEC) regarding the degree to which standards developers have conformed to those conventions. In addition, the TAG may develop coexistence documentation of interest to the technical community outside 802.

The following is a new standard project initiated by the Mobile Broadband Wireless Access (MBWA) working group:

- IEEE P802.19.1:2009, *Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements Part 19: TV White Space Coexistence Methods.*

802.20 Mobile Broadband Wireless Access (MBWA) Working Group

NOTE: This working group is currently hibernating.

On December 11, 2002, the IEEE Standards Board approved the establishment of IEEE 802.20, the MBWA Working Group.

The mission of IEEE 802.20 is to develop the specification for an efficient packet-based air interface optimized for the transport of IP-based services. The goal is to enable worldwide deployment of affordable, ubiquitous, always on, and interoperable multi-vendor mobile broadband wireless access networks that meet the needs of business and residential end-user markets.

The project scope is the specification of Physical and media access control (MAC) Layers of an air interface for interoperable mobile broadband wireless access systems, operating in licensed bands below 3.5 GHz, optimized Internet protocol (IP) data transport, with peak data rates per user in excess of 1 Mb/s.

It supports various vehicular mobility classes up to 250 kilometers per hour (km/h) in a MAN environment and targets spectral efficiencies, sustained user data rates, and a number of active users that are all significantly higher than achieved by existing mobile systems.

Institute of Electrical and Electronics Engineers® (IEEE®), continued

The following are standard projects initiated by the MBWA working group:

- IEEE 802.20™:2008, *IEEE Standard for Local and Metropolitan Area Networks—Part 20: Air Interface for Mobile Broadband Wireless Access Systems Supporting Vehicular Mobility—Physical and Media Access Control Layer Specification*.
- IEEE 802.20.2™:2010, *IEEE Standard for Conformance to IEEE 802.20 Systems—Protocol Implementation Conformance Statement* (*PICS*) *Proforma*.
- IEEE 802.20.3™:2010, *IEEE Standard for Minimum Performance Characteristics of IEEE 802.20 Terminals and Base Stations/Access Nodes*.
- IEEE 802.20a™:2010, *IEEE Standard for Local and Metropolitan Area Networks—Part 20: Air Interface for Mobile Broadband Wireless Access Systems Supporting Vehicular Mobility–Physical and Media Access Control Layer Specification— Amendment 1: Management Information Base Enhancements and Corrigenda Items.*
- IEEE 802.20b™:2010, *IEEE Standard for Local and Metropolitan Area Networks— Virtual Bridged Local Area Networks—Amendment 15: Bridging of 802.20.*

802.21 Handoff/Handover Working Group

An 802-handover standard would be applicable to 802 wired and wireless media types. For example, a handover between 802.3 and 802.11 within a single mobile station is a plausible application of such a standard.

This standard defines extensible 802 media access independent mechanisms that enable the optimization of handover between heterogeneous 802 systems and may facilitate handover between 802 systems and non-802 (cellular) systems.

The following is a new standard project initiated by the Handoff/Handover Working Group:

- IEEE 802.21™:2008, *IEEE Standard for Local and Metropolitan Area Networks—Part 21: Media Independent Handover Services.*

The 802.21 working group is responsible for the following initiatives:

- IEEE P802.21a:2008, *Standard for Local and Metropolitan Area Networks: Media Independent Handover Services—Amendment for Security Extensions to Media Independent Handover Services and Protocol.*
- IEEE P802.21b:2009, *Standard for Media Independent Handover Services—Amendment: Handovers with Downlink Only Technologies.*
- IEEE P802.21c:2009, *Standard for Local and Metropolitan Area Networks—Part 21: Media Independent Handover Services Amendment: Optimized Single Radio Handovers.*
- IEEE P802.21d:2008, *Standard for Local and Metropolitan Area Networks: IEEE Media Independent Handover Services—Amendment: Multicast Group Management.*

 © 2012 BICSI®

Institute of Electrical and Electronics Engineers® (IEEE®), continued

802.22 Wireless Regional Area Networks (WRAN) Working Group

The Wireless Regional Area Network (WRAN) working group is responsible for policies and procedures for operation in the TV bands. WRAN will specify a cognitive air interface for fixed point-to-multipoint wireless local area networks (WLANs) that operate on unused channels in the very high frequency (VHF)/ultrahigh frequency (UHF) TV bands between 54 and 862 megahertz (MHz).

The following are new standard projects initiated by the WRAN group:

- IEEE 802.22™:2011, *Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements Part 22: Standard to Enhance Harmful Interference Protection for Low Power Licensed Devices Operating in the TV Broadcast Bands.*
- IEEE 802.22.1™:2010, *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements Part 22.1: Standard to Enhance Harmful Interference Protection for Low Power Licensed Devices Operating in TV Broadcast Bands.*

The 802.22 working group is responsible for the following initiatives:

- IEEE P802.22.2:2006, *Recommended Practice for Information Technology—Telecommunications and Information Exchange Between Systems—Wireless Regional Area Networks (WRAN)—Specific Requirements Part 22.2: Recommended Practice for the Installation and Deployment of IEEE 802.22 Systems.*
- IEEE P802.22a:2011, *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Wireless Regional Area Networks (WRAN)—Specific requirements Part 22: Cognitive Wireless RAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Policies and Procedures for Operation in the TV Bands Amendment: Management and Control Plane Interfaces and Procedures and enhancement to the Management Information Base (MIB).*
- IEEE P802.22b:2011, *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Wireless Regional Area Networks (WRAN)—Specific requirements Part 22: Cognitive Wireless RAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Policies and Procedures for Operation in the TV Bands Amendment: Enhancement for Broadband Services and Monitoring Applications.*

Institute of Electrical and Electronics Engineers® (IEEE®), continued

802.23 Emergency Services Working Group

This standard defines a media independent structure within IEEE 802 to present consistent access and data that aid in compliance to civil authority needs (e.g., VoIP 911 calls) for communications systems that include IEEE 802 networks. This standard includes a data link layer interface that provides IP-based networks citizen-to-authority emergency services capabilities using Emergency Context Resolution with Internet Technologies (ECRIT).

- IEEE P802.23:2010, *Standard for Local and Metropolitan Area Networks—Emergency Services for Internet Protocol (IP) Based Citizen to Authority Communications Status: New Standard Project.*

P802 Handoff Executive Committee Study Group

On March 14, 2003, the IEEE 802 Executive Committee approved the Handoff Executive Committee Study Group (ECSG) with a charter to:

- Consider the possibility of developing a standard specifying a common handoff framework applicable to 802 standards, wired and wireless.
- Develop a project authorization request (PAR) and five criteria for a new standard for link security that can be applied to IEEE 802 networks.
- Make a recommendation on the placement of the project within IEEE 802 and the existing working groups.

P802 Link Security Executive Committee Study Group

On November 15, 2002, the IEEE 802 Executive Committee approved the Link Security ECSG with the scope to develop link security requirements for IEEE 802 networks and a charter to:

- Evaluate link security architecture issues with the objective of identifying the broader scope that can be common to all MAC solutions.
- Develop a PAR and five criteria for a new standard for link security that can be applied to IEEE 802 networks and, in particular, to 802.3 networks.
- Make a recommendation on the placement of the project within IEEE 802 and the existing working groups.

This group is now a Study Group of the IEEE 802.1 Working Group, allowing closer cooperation between security experts in IEEE 802.

Regional Codes and Standards

Australia / New Zealand Codes and Standards

The following standards are published by Australia/New Zealand standards (AS/NZS) and are relevant to an ITS designer and installer:

- AS/NZS 3080:2009, *Telecommunications Installations—Generic Cabling for Commercial Premises*.
- AS/NZS 3084:2007, *Telecommunications Installations—Telecommunications Pathways and Spaces for Commercial Buildings*.
- AS/NZS 3085.1:2004, *Telecommunications Installations—Administration of Communications Cabling Systems—Basic Requirements*.
- AS/NZS ISO/IEC 15018:2005, *Information Technology—Generic Cabling for Homes*.
- AS/NZS ISO/IEC 61935.1: 2006, *Telecommunications Installations—Generic Cabling Systems—Specification for the Testing of Balanced Communication Cabling in accordance with ISO/IEC 11801 – Installed Wiring*.
- AS/NZS NZS ISO/IEC 61935.2: 2006, *Telecommunications Installations—Generic Cabling Systems—Specification for the Testing of Balanced Communication Cabling in accordance with ISO/IEC 11801 – Patch Cords and Work Area Cords*.

Countries of the Americas Codes and Standards

The Inter-American Telecommunication Commission (CITEL)

The Inter-American Telecommunication Commission (CITEL) was established under the auspices of the Organization of American States (OAS). It has 33 member states and 1100 associate members. It has been entrusted by the heads of state at the Summits of the Americas with specific mandates. CITEL has technical autonomy to perform its functions within the limits prescribed by the OAS Charter, its statutes, and the mandates of the General Assembly. Its objectives include facilitating and promoting the continuous development of telecommunications.

CITEL has a permanent executive committee, which consists of thirteen members, three Permanent Consultative committees, and one working group:

- Permanent Consultative Committee I (PCC I), which addresses telecommunication standardization
- Permanent Consultative Committee II (PCC II), which addresses radio communications, including broadcasting
- A steering committee
- Conference preparatory working group, whose members are all member states of the organization and associate members that represent various private telecommunication associations or companies, and permanent observers and regional and international organizations

European Codes and Standards

Comité Européen de Normalisation Electrotechnique (CENELEC)

While every country in the European Union has adopted the Comité Européen de Normalisation Electrotechnique (CENELEC) standards, there may be local standards that provide guidance or are specific to a country application for the CENELEC standards.

The organization of the CENELEC cabling-related standards is shown in Table A.1.

Table A.1
Relationship between series EN 50174 and other design standards

Building Design Phase	Cabling Design Phase	Planning Phase	Implementation Phase	Operation Phase
EN[1] 50310	**EN 50173**	**EN 50174-1**	**EN 50174-1**	**EN 50174-1**
5.2: Common bonding network (CBN) within a building 6.3: ac distribution system and bonding of the protective conductor (TN-S)	**or (and)** **EN 50098-1** **or (and)** **EN-50098-2** **or (and)** Other application standards	4: Specification considerations 5: Quality assurance 7: Cabling administration **and EN 50174-2** 4: Safety requirements 5: General installation practices for metallic and optical fiber cabling 6: Additional installation practice for metallic cabling 7: Additional installation practice for optical fiber cabling **and EN 50174-3** (for equipotential bonding)	6: Documentation 7: Cabling administration **and EN 50174-2** 4: Safety requirements 5: General installation practices for metallic and optical fiber cabling 6: Additional installation practice for metallic cabling 7: Additional installation practice for optical fiber cabling **and EN 50174-3** (for equipotential bonding)	5: Quality assurance 7: Cabling administration 8: Repair and maintenance

 © 2012 BICSI®

European Codes and Standards, continued

Table A.1, continued
Relationship between series EN 50174 and other design standards

Building Design Phase	Cabling Design Phase	Planning Phase	Implementation Phase	Operation Phase
		EN 50310 5.2: Common bonding network (CBN) within a building 6.3: ac distribution system and bonding of the protective conductor (TN-S)	**EN 50310** 5.2: Common bonding network (CBN) within a building 6.3: ac distribution system and bonding of the protective conductor (TN-S)	

[1] European Norm (EN) is sometimes preceded by "pr," meaning preliminary.

ac = Alternating current
CBN = Common bonding network
EN = European norm

CENELEC EN 50098 Series

CENELEC EN 50098-1:2003 *Customer Premises Cabling for Information Technology— Part 1: ISDN Basic Access*

This European standard defines the requirements for the design and configuration of customer premises cabling for the connection of basic access integrated services digital network (ISDN) equipment.

It also defines:

- Design requirements for ISDN basic access with point-to-point and point-to-multipoint cabling configurations.
- Minimum cabling requirements for the installation of new cabling.
- Criteria for the use of generic cabling.
- Criteria for the use of existing cabling.

This standard applies to the customer premises cabling. It describes the cabling requirements needed to transmit ISDN basic access signals as defined by ITU-T Recommendation I.430. The requirements placed on the customer premises cabling are solely those necessary to enable terminal equipment conforming to ETS 300 012-1 to operate into the network termination (NT) via configurations defined in this standard.

European Codes and Standards, continued

CENELEC EN 50098-2:1996 ***Customer Premises Cabling for Information Technology— Part 2: 2048 kb/s ISDN Primary Access and Leased Line Network Interface***

This European standard specifies the design and configuration of customer premises cabling for the connection of primary access ISDN equipment. It includes:

- Design requirements for ISDN primary access point-to-point configuration.
- Cabling requirements for the installation of new cabling.
- Criteria for the use of existing cabling.
- Implementation of ISDN primary access on generic cabling systems according to EN 50173.

This standard applies to the customer premises cabling for the transmission of ISDN primary access signals as defined by ETS 300 011. The requirements in this standard also apply to the cabling between Open Network Provision 2048 kb/s Network Interfaces and terminal equipment conforming to ETS 300 248.

CENELEC EN 50173 Series

CENELEC EN 50173 is a series of standards detailing general cabling systems for general practice and office, industrial, residential, and data centers applications.

CENELEC EN 50173-1:2011 ***Information Technology—Generic Cabling Systems—Part 1: General Requirements***

CENELEC EN 50173-1 contains those specifications that are common to generic cabling systems irrespective of the type of premises. It specifies generic balanced twisted-pair, unbalanced coaxial, singlemode, multimode, and plastic optical fiber cabling components for use within premises, which may comprise single or multiple buildings on a campus.

This European standard is optimized for premises where the maximum distance over which telecommunications services have to be distributed is 10,000 m (32,809 ft). The principles of this standard may also be applied to larger installations.

Cabling defined by this standard supports a wide range of services, including voice, data, text, image, and video. This standard specifies the:

- Structure and configuration for generic cabling.
- Cabling performance requirements.
- Implementation options.
- Applications supported by application and by media type.

Safety (e.g., electrical safety and protection, optical power, fire) and electromagnetic compatibility (EMC) requirements are outside the scope of this European standard and are covered by other standards and regulations. However, information given in this standard may be of assistance in meeting these standards and regulations or determining which cabling components are best suited for the environment in which they are to be installed.

 © 2012 BICSI®

European Codes and Standards, continued

EN 50173-2+A1:2010+A2:2011 ***Information Technology—Generic Cabling Systems—Part 2: Office Premises***

This European standard is based upon and references the requirements of EN 50173-1. This European standard contains additional requirements that are appropriate to office premises in which the maximum distance over which communications services maybe distributed is 2000 m (6562 ft). The principles of this European standard may also be applied to installations that do not fall within this range.

In addition to the requirements of EN 50173-1, this European standard specifies:

- An extended structure and configuration for generic cabling within office premises in support of a wide range of services, including voice, data, text, image, and video.
- Implementation options.

EN 50173-3: 2011 ***Information Technology—Generic Cabling Systems—Part 3: Industrial Premises***

This European standard, EN 50173-3, recognizes the benefit of generic cabling to interconnect several pieces of apparatus within industrial premises (within and between structures and buildings) and is to be read in conjunction with EN 50173-1.

This European standard provides for industrial premises:

- Users with an application-independent generic cabling system and an open market for cabling components.
- Requirements for infrastructures that support critical automation, process control, and monitoring applications in a range of industrial environments.
- Users with a flexible cabling scheme such that modifications are both easy and economical.
- Building professionals (e.g., architects) and production and control engineers with guidance, allowing the accommodation of cabling both before specific requirements are known (i.e., in the initial planning either for construction or refurbishment) and for further deployment as the requirements of specific industrial areas are defined.
- Industry and standardization bodies with a cabling system that supports current products and provides a basis for future product development and applications standardization.

European Codes and Standards, continued

EN 50173-4: 2011 ***Information Technology—Generic Cabling Systems—Part 4: Residential Premises***

This European standard specifies generic cabling in homes, which are installed to support one or more of the following groups of applications and are based upon balanced and coaxial cabling as appropriate:

- Information and Communications Technologies (ICT)
- Broadcast and Communications Technologies (BCT)
- Commands, Controls and Communications in Buildings (CCCB)

Other cabling media, used for the above applications, are not covered in this standard. Backbone cabling connecting individual homes within single premises is built according to the relevant standard (e.g., EN 50173-1, EN 50083 series).

EN 50173-5: 2011 ***Information Technology—Generic Cabling Systems—Part 5: Data Centres***

The importance of the IT cabling infrastructure is similar to that of other utilities such as heating, lighting, and electricity supplies. As with other utilities, interruptions to service can have a serious impact. Poor quality of service because of a lack of planning, use of inappropriate components, incorrect installation, poor administration, or inadequate support can threaten an organization's effectiveness.

Cabling within data centers comprises both application-specific and multipurpose networks that are mission critical to the enterprise. Generic cabling designs in accordance with the EN 50173 series have supported the development of high data rate applications based upon a defined cabling model. This European standard recognizes the benefit of generic cabling to provision multiple services and to connect large quantities of equipment within the limited space of data center premises and is to be used in conjunction with EN 50173-1.

This European standard, EN 50173-5, provides:

- Users with an application-independent generic cabling system and an open market for cabling components.
- Requirements for infrastructures that support critical applications within data centers.
- A flexible cabling scheme such that modifications are both easy and economical.
- A scalable structure to support expansion with minimum operational disruption.
- Building professionals (e.g., architects) with guidance allowing the accommodation of cabling before specific requirements are known (i.e., in the initial planning either for construction or refurbishment).
- Industry and standardization bodies with a cabling system that supports current products and provides a basis for future product development and applications standardization.

 © 2012 BICSI®

European Codes and Standards, continued

CENELEC EN 50174 Series

CENELEC EN 50174 series of standards specifies the basic requirements for the planning, implementation, and operation of IT cabling using balanced twisted-pair cabling and optical fiber cabling.

This European standard is applicable to:

- Cabling designed to support particular analog and digital telecommunications services, including voice services.
- Generic cabling systems designed in accordance with EN 50173 and intended to support a wide range of telecommunications services.

Information in this standard is intended for those involved in the procurement, installation, and operation of IT cabling.

This standard is addressed to:

- Architects, building designers, and builders.
- Main contractors.
- Designers, suppliers, installers, maintainers, and owners of IT cabling.
- Public network providers and local service providers.
- End users.

EN 50174 is applicable to certain hazardous environments, but it does not exclude additional requirements, which are applicable in specific circumstances (e.g., those defined by electrical supply and electrified railways).

CENELEC EN 50174-1:2009+A1:2011 *Information Technology—Cabling Installation—Part 1: Installation Specification and Quality Assurance*

This European standard provides guidance on the preparation and agreement of an installation specification covering the IT cabling, its accommodation, and associated building services.

It also defines installation and acceptance testing practices, enabling the agreement of a quality plan used to demonstrate conformance with the installation specification.

The importance of services delivered by IT cabling infrastructure is similar to that of utilities such as heating, lighting, and electricity supplies. As with those utilities, interruptions to service can have a serious impact. Poor quality of service because of a lack of planning, use of inappropriate components, incorrect installation, poor administration, or inadequate support can threaten an organisation's effectiveness.

European Codes and Standards, continued

There are four phases in the successful implementation of IT cabling. These are:

- Design.
- Specification—The detailed requirement for the cabling, including the planning of its accommodation and associated building services addressing specific environments (e.g., electromagnetic) together with the quality assurance requirements to be applied.
- Installation—In accordance with the requirements of the specification.
- Operation—The management of connectivity and the maintenance of transmission performance during the life of the cabling.

This European standard is in three parts and addresses the specification, installation, and operational aspects. The EN 50173 series and other application standards cover design issues.

EN 50174-1 is used during the specification phase. It addresses the:

- Installation specification, quality assurance documentation, and procedures.
- Documentation and administration.
- Operation and maintenance.

EN 50174-2 and EN 50174-3 are intended to be used by the personnel directly involved in the planning aspects of the specification phase and the installation phase. EN 50174-2 is applicable inside buildings, and EN 50174-3 is applicable outside buildings. This European standard is also relevant to:

- Architects, building designers, and builders.
- Main contractors.
- Designers, suppliers, installers, inspectors (auditors), maintainers, and owners of IT cabling.
- Public network providers and local service providers.
- End users.

The requirements and recommendations of Clause 4 are primarily for owners of premises housing IT systems. The owners may delegate selected responsibilities to designers, specifiers, operators, and maintainers of installed IT cabling.

The requirements and recommendations of Clause 5 are primarily for the installers of IT cabling.

 © 2012 BICSI®

European Codes and Standards, continued

CENELEC EN 50174-2:2009+A1:2011 *Information Technology—Cabling Installation—Part 2: Installation Planning and Practices Inside Buildings*

EN 50174-2 is concerned with the planning and installation of IT cabling using metallic cabling and optical fiber cabling inside buildings. It provides guidance as to the responsibilities of those involved and is intended to be referenced in relevant contracts.

EN 50174-2 contains requirements and recommendations relating to the installation planning and practices by defining:

- Planning strategy (road map) and guidance, depending on the application, electromagnetic environment, building infrastructure, facilities, etc.
- Planning and installation requirements for metallic and optical fiber IT cabling, depending on the application, electromagnetic environment, building infrastructure, facilities, etc.
- The practices and procedures to be adopted to ensure that the cabling is installed in accordance with the specification.

The standard excludes specific requirements applicable to other cabling systems (e.g., power cabling, coaxial cabling); however, it takes into account the effects other cabling systems may have on the installation of IT cabling (and vice versa) and gives general advice.

CENELEC EN 50174-3:2003 *Information Technology—Cabling Installation—Part 3: Installation Planning and Practices Outside Buildings*

This European standard establishes requirements for satisfactory installation and operation of IT cabling outside buildings—it is not restricted to campus areas.

This standard excludes specific requirements applicable to other cabling systems (e.g., power cabling, coaxial cabling); however, it takes into account the effects that other cabling systems may have on the installation of IT cabling (and vice versa) and gives general advice.

European Codes and Standards, continued

EN 50174-3 contains detailed requirements and guidance relating to the installation planning and practices by defining:

- Planning strategy (road map) and guidance, depending on the application and physical environment (e.g., climatic, mechanical, electromagnetic).
- Design and installation rules for metallic and optical fiber cabling, depending on the application, electromagnetic environment, and physical environment.
- Requirements on satisfactory operation of the cabling, depending on the application, electromagnetic environment, and physical environment.
- The practices and procedures to be adopted to ensure that the cabling is installed in accordance with the specification.

CENELEC EN 50310:2010 *Application of Equipotential Bonding and Earthing in Buildings with Information Technology Equipment*

This European standard specifies minimum requirements for earthing networks and connections (bonds) in buildings in which IT equipment is intended to be installed to protect that equipment and interconnecting cabling from electrical hazards.

Additionally this European standard specifies requirements and provides recommendations for earthing networks and connections (bonds) in order for the IT installation to achieve:

- Reliable signal reference.
- Adequate immunity from electromagnetic interference carried by the earthing network.

 © 2012 BICSI®

European Codes and Standards, continued

CENELEC EN 62305-1:2011 *Protection Against Lightning—Part 1 General Principles*

This part of IEC 62305 provides the general principles to be followed in the protection against lightning of:

- Structures, including their installations and contents as well as persons.
- Services connected to a structure.

The following cases are outside the scope of this standard:

- Railway systems
- Vehicles, ships, aircraft, and offshore installations
- Underground high pressure pipelines
- Pipe, power, and telecommunication lines not connected to a structure

The need for protection, the economic benefits of installing protection measures, and the selection of adequate protection measures should be determined in terms of risk management. Risk management is the subject of IEC 62305-2.

The criteria for design, installation, and maintenance of lightning protection measures are considered in three separate groups:

- The first group concerns protection measures to reduce physical damage and life hazard in a structure is given in IEC 62305-3.
- The second group concerns protection measures to reduce failures of electrical and electronic systems in a structure is given in IEC 62305-4.
- The third group concerns protection measures to reduce physical damage and failures of services connected to a structure (mainly electrical and telecommunication lines) is given in IEC 62305-5.

National Codes and Standards

Australian Codes and Standards

Australian Communications and Media Authority (ACMA)

The Australian Communications and Media Authority (ACMA) produces standards that affect telecommunications. Some of the most relevant are:

- AS/ACIF S008:2006, *Requirements for Authorised Cabling Products.*
- AS/ACIF S009:2006, *Installation Requirements for Customer Cabling (Wiring Rules).*
- HB 29:2007+A1:2010, *Communications Cabling Manual, Module 2: Communications Cabling Handbook.*

The handbook provides cabling installers with a practical field guide to allow them to cable premises for voice, data, and video. It guides them through appropriate standard requirements with cross-references to the actual standards—AS/ACIF S009:2006 and AS/NZS 3080:2003.

Brazilian Codes and Standards

Associacão Brasileira de Normas Técnicas (ABNT)

Associacão Brasileira de Normas Técnicas (ABNT) produces standards that affect telecommunications with Brazil. Some of the most relevant are:

- ABNT NBR 5410:2004, *Instalações elétricas de baixa tensão (Low Voltage Electrical Installations).*
- ABNT NBR 6814:2001, *Fios e cabos elétricos—Ensaio de resistência elétrica (Cables and Wires—Electrical Resistance Test and Measurement).*
- ABNT NBR 9130:2009, *Fios e cabos telefônicos—Ensaio de desequilíbrio resistivo (Telephone Cables and Wires—Resistance Unbalance Test).*
- ABNT NBR 9133:2011, *Cabos telefônicos—Ensaio de atenuação de sinal de transmissão—Método de ensaio (Telephone Cables—Signal Transmission Attenuation— Methods of Test).*
- ABNT NBR 13989:1997, *Cabo óptico subterrâneo—Determinação do desempenho quan do submetido ao ensaio de coeficiente de atrito estático—Método de ensaio (Underground Optical Cable—Performance Evaluation of Static Friction Coefficient—Method of Test).*
- ABNT NBR 13990:1997, *Cabo óptico subterrâneo—Determinação do desempenho quando submetido à vibração—Método de ensaio (Underground Optical Cable — Performance Evaluation under Vibration Conditions—Method of Test).*
- ABNT NBR 14103:2005, *Cabo óptico dielétrico para aplicação enterrada (Direct-buried Dielectric Optical Cable).*
- ABNT NBR 14159:2010, *Cabo óptico com núcleo geleado protegido por capa APL—Especificação* (*APL-Insulated Optical Cable Loose Tube Filled with Gel*).

 © 2012 BICSI®

Brazilian Codes and Standards, continued

- ABNT NBR 14160:2005, *Cabo óptico aéreo dielétrico auto-sustentado* (*Aerial Selfsustained Dielectric Optical Cable*).
- ABNT NBR 14161:1998, *Cabo óptico dielétrico de emergência—Especificação* (*Emergency Dielecric Optical Cable—Specification*).
- ABNT NBR 14433:2000, *Conectores montados em cordões ou cabos de fibras ópticas e adaptadores—Especificação (Optical Connectors and Adapters Assembled in Patch Cords or Optical Fiber Cables—Specification).*
- ABNT NBR 14565:2007, *Cabeamento de telecomunicações para edifícios comerciais* (*Telecommunications Cabling for Commercial Buildings*).
- ABNT NBR 14566:2004, *Cabo óptico dielétrico para aplicação subterrânea em duto e aérea espinado (Spined Dielectric Optical Cable for Underground Duct Installation—Specification).*
- ABNT NBR 14584:2000, *Cabo óptico com proteção metálica para instalações subterrâneas—Verificação da suscetibilidade a danos provocados por descarga atmosférica—Método de ensaio (Optical Cable with Metallic Protection for Underground Installations—Evaluation of Damage Caused by Atmospheric Discharge—Method of Test).*
- ABNT NBR 14589:2000, *Cabo óptico com proteção metálica para instalações subterrâneas—Determinação da capacidade de drenagem de corrente—Método de ensaio (Optical Cable with Metallic Protection for Underground Installations—Evaluation of Current Flow—Method of Test).*
- ABNT NBR 14683:2001, *Sistemas de subdutos de polietileno para telecomunicações—Parte 1: Requisitos para subduto de parede lisa (Polyethylene Innerduct Systems for Telecommunications—Part 1: Innerducts Smooth Wall Requirements).*
- ABNT NBR 14702:2001, *Emenda 2004—Cabos coaxiais flexíveis com impedância de 75 ohms—especificação (75-ohm Flexible Coaxial Cables—Specifications).*
- ABNT NBR 14702:2004, *Cabos coaxiais flexíveis com impedância de 75 ohms para redes de banda larga—especificação (75-ohm Flexible Coaxial Cables for Broadband Applications—Specification).*
- ABNT NBR 14703:2005, *Cabos de telemática de 100 Ω para redes internas estruturadas—Especificação (Telecommunications Cable for Structured Cabling, 100-ohm— Specification).*
- ABNT NBR 14705:2010, *Cabos internos de telecomunicações—classificação quanto ao retardo à propagação de chamas (Indoor Telecommunications Cable—Fire Rating Classification).*
- ABNT NBR 14770:2004, *Cabos coaxiais rígidos com impedância de 75 ohms para redes de banda larga—especificação (75-ohm Rigid Coaxial Cables for Broadband Applications—Specification).*

Brazilian Codes and Standards, continued

- ABNT NBR 14771:2007, *Cabo óptico interno—Especificação (Indoor Optical Cable— Specification).*
- ABNT NBR 14772:2006, *Cabo óptico de terminação—Especificação (Optical Cable for Connectors Termination—Specification*).
- ABNT NBR 14773:2009, *Cabo óptico dielétrico protegido contra ataque de roedores para aplicação em linhas de dutos—Especificação (Corrugated-metal Sheath Dielectric Optical Cable for Duct Systems Distribution—Specification).*
- ABNT NBR 14774:2009, *Cabo óptico dielétrico protegido contra ataque de roedores para aplicação enterrada—Especificação (Corrugated-metal Sheath Dielectric Optical Cable for Direct-buried Distribution—Specification).*
- ABNT NBR 15108:2004, *Cabo óptico com núcleo dielétrico e proteção metálica para aplicação em linhas de dutos (Dielectric Optical Cable with Metallic Protection for Duct System Installation).*
- ABNT NBR 15110:2004, *Cabo óptico com núcleo dielétrico e proteção metálica para aplicação enterrada (Optical Cable with Dielectric Core Protected by Metallic Insulated Sheath for Direct-buried Installations).*

Agência Nacional de Telecomunicações (ANATEL)

- Resolucao 242, *Regulamento para certificação e homologação de produtos para telecomunicações (Resolution 242, Regulation for Certification of Telecommunications Products).*

 © 2012 BICSI®

Canadian Codes and Standards

Standards Council of Canada (SCC)

SCC is a federal Crown corporation that serves to promote efficient and effective standardization in Canada. SCC's mission is to facilitate the development and use of national and international standards and accreditation services.

Canadian Standards Association (CSA®)

The Canadian Standards Association (CSA®) produces several documents and standards that affect telecommunications. Among the most important are:

- CSA C22.1-12, *Canadian Electrical Code (CEC), Part I, Safety Standard for Electrical Installations*.
- CSA C22.1HB-12, *CEC Handbook, An Explanation of Rules of the Canadian Electrical Code.*
- CSA T568.1-05, *Commercial Building Telecommunications Cabling Standard—Part 1: General Requirements* (Adopted ANSI/TIA/EIA-568-B.1-2001).
- CSA C22.2 No. 214-08, *Communications cables.*
- CAN/CSA-C22.2 No. 262-04, *Optical fiber Cable and Communication Cable Raceway Systems.*

Canadian Electrical Code (*CEC*)*—Part I*

The CSA sponsors, controls, and publishes the *Canadian Electrical Code, Part I*. The intent of this code is to establish safety standards for the installation and maintenance of electrical equipment, including telecommunications. Compliance with the requirements of this code and proper maintenance will ensure an essentially safe installation. The *Canadian Electrical Code, Part I,* is a voluntary code for adoption and enforcement by the provincial and territorial regulatory authorities.

All provinces and local jurisdictions have adopted the *Canadian Electrical Code, Part I,* as their standard, and some have introduced additional requirements.

The *Canadian Electrical Code, Part I,* (revised every three years) is used by:

- Fire marshals and electrical inspectors in loss prevention and safety enforcement.
- Attorneys (barristers) and insurance companies to determine liability.

ITS designers and installers must be familiar with all sections of the *Canadian Electrical Code, Part I,* when planning the installation of the telecommunications system within Canada and the Bahamas.

Table A.2 lists sections of the *Canadian Electrical Code, Part I,* that are applicable to the telecommunications distribution design.

Canadian Codes and Standards, continued

Table A.2
Sections of the *Canadian Electrical Code*

Section	Title	Contents
2	General Rules	Provides information on: • Permits. • Marking of cables. • Flame spread requirements for electrical wiring and cables.
10	Grounding and Bonding	Contains detailed bonding and grounding (earthing) information and requirements for using and identifying bonding and ground (earth) conductors.
12	Wiring Methods	Involves the requirements for installing cabling systems. It outlines: • Raceway systems. • Boxes. • Other system elements.
54	Community Antenna Distribution and Radio and Television Installations	Applies to circuits employed to distribute video, radio, and other information frequency signals.
56	Optical Fiber Cables	Contains the requirements for installing optical fiber cables.
60	Electrical Communication Systems	Contains the requirements for installing communications circuits.
82	Closed-Loop and Preclosed-Loop Power Distribution	Contains the requirements for controlling the signal between the energy controlling equipment and the utilization equipment.

 © 2012 BICSI®

Canadian Codes and Standards, continued

National Research Council of Canada, Institute for Research in Construction (NRC-IRC)

The National Research Council of Canada, Institute for Research in Construction (NRC-IRC) produces several documents and standards that affect telecommunications. Among the most important are:

- *National Building Code of Canada (NBC),* 2010.
- *National Fire Code of Canada (NFC),* 2010.
- *National Energy Code of Canada for Buildings* (*NECB*), 2011

French Codes and Standards

Union Technique de l'Ectricite et de la Communication (UTE)

The Union Technique de l'Ectricite et de la Communication (UTE) produces several documents and standards that affect telecommunications in France.

Among the most important are:

- UTE C 15-900:2006, *Guide Pratique—Cohabitation entre réseaux de communication et d'énergie—Installation des réseaux de communication (Coexistence Between Communication and Power Networks—Implementation of Communication Networks).*
- UTE C 90-480-1:2001 (NFEN 50174-1), *Technologies de l'information—Installation de câblage—Partie 1: Planification de l'assurance de la qualité (Information Technology—Cabling Installation—Part 1: Specification and Quality Assurance).*
- UTE C 90-480-2:2001 (NFEN 50174-2), *Technologies de l'information—Installation de câblage—Partie 2: Planification et pratiques d'installation à l'intérieur des bâtiments (Information Technology—Cabling Installation—Part 2: Installation Planning and Practices Inside Buildings).*
- UTE C 90-470-2:1995, *Systèmes électroniques pour les foyers domestiques et les bâtiments, HBES—Rapport technique 2—Recommandations pour l'installation professionnelle des câbles à paires torsadées—Classe 1 (Home and Building Electronic Systems [HBES]—Technical Report 2: Guidelines for the Professional Installation of Twisted-Pair Cables—Class 1).*

Japanese Codes and Standards

Japanese Standards Association

The specific standard for residential cabling in Japan is JIS X 5150:2009 (ISO/IEC 11801 Ed.2:2002+A1:2010), *Information Technology—Generic Cabling for Customer Premises.*

United Kingdom (UK) Codes and Standards

NOTE: See also European Codes and Standards for additional applicable standards within the United Kingdom (UK).

British Standards Institution (BSI)

British Standards Institution (BSI) produces standards relating to telecommunications. Some of the most relevant are:

BS 6701:2010 *Telecommunications Equipment and Telecommunications Cabling—Specification for Installation, Operation, and Maintenance*

This edition of BS 6701 extends the requirements of the BS EN 50174 series of standards to the installation, operation, administration, and maintenance of telecommunications equipment and telecommunications cabling other than cabling within the scope of the BS EN 50174 series of standards. It also specifies requirements beyond the scope of the BS EN 50174 series of standards for telecommunications equipment and all types of telecommunications cabling.

The requirements contained within Clause 4 are primarily for the installers of telecommunications equipment and telecommunications cabling.

The requirements contained within Clause 5 are primarily for owners of premises housing telecommunications systems. These owners may delegate selected responsibilities to designers, specifiers, operators, and maintainers of installed telecommunications equipment and telecommunications cabling.

BS 7671:2008+A1:2011 *Requirements for Electrical Installations—IEE Wiring Regulations*, 17th Edition

In Great Britain, electrical installations are required to comply with Statutory Regulations such as *The Electricity Safety, Quality and Continuity Regulations* 2002 (and amendments) and *The Electricity at Work Regulations* 1989 (and amendments). The regulations represent the principal legal requirements. BS 7671 (and amendments) is the national standard to which all domestic and industrial wiring must conform.

Amendment number 2 primarily concerns a fundamental change to the colors of fixed wiring cables along with some changes because of the introduction of the *Electricity Supply Quality and Continuity Regulations* and some certificate changes. The regulations are to be applied generally to electrical installations. However, in certain circumstances, these regulations may need to be supplemented by the requirements or regulations of other British or European standards.

 © 2012 BICSI®

United Kingdom (UK) Codes and Standards, continued

BS 8300:2009+A1:2010 ***Design of Buildings and Their Approaches to Meet the Needs of Disabled People—Code of Practice***

This British standard gives recommendations for the design of new buildings and their approaches to meet the needs of disabled people. This standard explains how the built environment can be designed to anticipate and overcome restrictions that prevent disabled people from making full use of premises and their surroundings. An accessible environment is one in which a disabled person can enter and make use of independently or with help from a partner or assistant.

Some facilities may be designed in such a way as to incorporate access for disabled people. In other situations, additional features such as grab rails, touch legible signs, and hearing enhancement systems may be needed. The guidance in this standard covers a wide range of impairments and the use of the built environment by disabled people who may be residents, visitors, spectators, customers, employees, or participants in sports events, performances, and conferences.

This British standard does not apply to dwellings or residential buildings designed exclusively for use by disabled people nor does it make specific recommendations relating to the use of buildings by children.

This document should be read in conjunction with building design and requirement documents and local authority guidelines.

BS 8492:2009 ***Telecommunications Equipment and Telecommunications Cabling—Code Of Practice For Fire Performance and Protection***

This British standard gives recommendations for fire performance and fire protection of all types of telecommunications equipment and telecommunications cabling. It covers:

- Designing and implementing cabling infrastructures.
- Selecting products, including materials and construction.
- Minimizing fire spread.
- Increasing safety levels for personnel and property.

This British standard details the relationship between its recommendations, the usage of premises, and fire protection measures. It is applicable to certain hazardous environments, but it does not exclude additional requirements that are applicable in particular circumstances (e.g., electrified railways, petrochemical sites, intrinsically safe areas, explosive ordnance storage facilities [bomb dumps]).

NOTE Annex A considers the fire hazard posed by the installation of telecommunications equipment and telecommunications cabling infrastructure within premises.

United States (U.S.) Codes and Standards

American National Standards Institute (ANSI)

ANSI is a private, not-for-profit organization that serves as the administrator and coordinator of the United States' private sector voluntary standardization system. ANSI's mission is to promote and facilitate voluntary consensus standards and conformity assessment systems. Although ANSI itself does not develop standards, ANSI provides a forum for numerous ANSI-accredited standards developers to develop American National Standards. A standard that has been adopted as an American National Standard typically has "ANSI" within the standard's designation.

Americans with Disabilities Act (ADA)

The Americans with Disabilities Act (ADA) of 1992 as it relates to telecommunications is covered in:

- Title IV: Telecommunications of the *Telecommunications Act*, which covers the functionality of devices for hearing and speech impaired individuals.
- Section 4.31: Telephones of the Americans with Disabilities Act (ADA) Accessibility Guidelines (ADAAG). "Accessibility Guidelines for Buildings and Facilities" covers accessibility to telephones and communications devices by the physically impaired.

Additionally, as stated in Section 255 of the *Telecommunications Act*, the industry is obligated to ensure accessibility and usability.

BICSI®

The BICSI® International Standards Program produces standards of interest to ITS designers and installers. Some of BICSI's notable standards include:

- ANSI/BICSI 001-2009, *Information Transport Systems Design Standard for K-12 Educational Institutions*.
- ANSI/BICSI 002-2011, *Data Center Design and Implementation Best Practices*.

 © 2012 BICSI®

United States (U.S.) Codes and Standards, continued

Federal Communications Commission (FCC)

At the federal level in the United States, the Federal Communications Commission (FCC) publishes numerous reports and orders that deal with specific issues, some of which are listed in this appendix. Table A.3 lists important FCC documents.

Table A.3
Federal Communications Commission documents

Document	Subject Matter
CC Docket 88-57	Defines the location of the demarcation point. The third report and order (99-405) established category 3 UTP as the minimum cable standard for simple premises cabling.
CC Docket 99-216	*The Privatization and Streamlining of Part 68 of the Commission's Rules*. Effective July 23, 2001, the Administrative Council for Terminal Attachments (ACTA) assumed operational responsibility for Part 68. ACTA was established to assume relevant responsibilities privatized by the FCC.
Fact Sheet ICB-FC-011	Connection of 1- and 2-line terminal equipment to the telephone network and installation of premises cabling.
FCC Part 15	*Radiated Emission Limits* (revised 1998) addresses electromagnetic radiation.
FCC Part 22	*Public Mobile Services* (revised 1998).
FCC Part 68	*Connection of Terminal Equipment to the Telephone Network* (1998) provides regulations for connecting premises cabling and customer-provided equipment to the regulated networks. NOTE: This is currently specified within TIA 968.
FCC Part 76	*Cable Television Service*, revised 1998.
Telecommunications Act, 1996	Established new rules for provisioning and competition in telecommunications services.

ACTA = Administrative Council for Terminal Attachments
CC = Common carrier
FCC = Federal Communications Commission
TIA = Telecommunications Industry Association
UTP = Unshielded twisted-pair

United States (U.S.) Codes and Standards, continued

IEEE C2-2012 *National Electrical Safety Code® (NESC®)*

Published by the IEEE, the *National Electrical Safety Code®* (*NESC®*) is the single most important document for safeguarding persons against electrical hazards during the installation, operation, and maintenance of electric supply and communication lines. The document contains extensive updates and critical revisions that directly impact the power utility industry.

Adopted into law by the majority of states and Public Service Commissions across the United States, *NESC* is a performance code that has been considered the authoritative source on sound electrical engineering practice for nearly 90 years.

The *NESC* covers basic provisions for the safeguarding of persons from the hazards arising from the installation, operation, or maintenance of outside plant (OSP) overhead and underground electrical supply and communication lines. It also includes work rules for the construction, maintenance, and operation of electric supply and communication lines and equipment.

The code is typically applicable to those systems and the equipment operated by utilities or similar systems and equipment of an industrial complex under the control of qualified persons. The *NESC* is also applicable to privately owned or operated complexes. This can include campus environments such as hospitals, college campuses, or industrial complexes.

The *NESC* is included in the National Institute for Standards and Technology (NIST). The *NESC* parts, sections, and rules applicable to telecommunications distribution requirements are listed in Table A.4.

 © 2012 BICSI®

United States (U.S.) Codes and Standards, continued

Table A.4
NESC® parts, sections, and rules applicable to telecommunications distribution requirements

NESC® Reference	Title
Section 1	Introduction to the *National Electrical Safety Code*®
Section 9	Grounding Methods for Electric Supply and Communications Facilities
Part 2	Safety Rules for the Installation and Maintenance of Electric Supply and Communication Lines
Section 20	Purpose, Scope, and Application of Rules
Section 21	General Requirements
Rule 215	Grounding of Circuits, Supporting Structures, and Equipment
Section 22	Relations Between Various Classes of Lines and Equipment
Rule 222	Joint Use of Structures
Rule 223	Communications Protective Requirements
Rule 224	Communication Circuits Located Within the Supply Space and Supply Circuits Located Within the Communication Space
Section 23	Clearances
Rule 230	General
Rule 230F	Fiber-Optic Cable
Rule 231	Clearances of Supporting Structures from Other Objects
Rule 232	Vertical Clearance of Wires, Conductors, Cables, and Equipment Above Ground, Roadway, Rail, or Water Surfaces
Rule 233	Clearances Between Wires, Conductors, and Cables Carried on Different Supporting Structures
Rule 234	Clearance of Wires, Conductors, Cables, and Equipment from Buildings, Bridges, Rail Cars, Swimming Pools, and Other Installations
Rule 235	Clearance for Wires, Conductors, or Cables Carried on the Same Supporting Structure
Rule 236	Climbing Space
Rule 237	Working Space
Rule 238	Vertical Clearance Between Certain Communications and Supply Facilities Located on the Same Structure
Rule 239	Clearances of Vertical and Lateral Facilities From Other Facilities and Surfaces on the Same Supporting Structure
Rule 239F	Requirements for Vertical and Lateral Communication Conductors on Communication Line Structures or Within the Communication Space on Jointly Used Structures
Rule 239H	Requirements for Vertical Communication Conductors Passing Through Supply Space on Jointly Used Structures

United States (U.S.) Codes and Standards, continued

Insulated Cable Engineers Association (ICEA)

The Insulated Cable Engineers Association (ICEA) is a wire and cable manufacturers' organization that writes telecommunications specifications for the telephone and electrical power industries.

ICEA publications are:

- Adopted in the public interest.
- Designed to:
  - Eliminate misunderstanding between the manufacturer and the user.
  - Assist users in selecting and obtaining proper products for their particular need.

ICEA standards of interest are:

- ANSI/ICEA P-61-694-1999, *Coding Guide for Copper Outside Plant and Riser Telecommunications Cables*.
- ANSI/ICEA S-80-576-2002, *Category 1 and 2 Individually Unshielded Twisted-Pair Indoor Cables for Use in Communications Wiring Systems*.
- ANSI/ICEA S-83-596-2011, *Indoor Optical Fiber Cables*.
- ANSI/ICEA S-84-608-2010, *Telecommunications Cable Filled, Polyolefin Insulated, Copper Conductor.*
- ANSI/ICEA S-85-625-2007, *Telecommunications Cable Aircore, Polyolefin Insulated, Copper Conductor Technical Requirements*.
- ANSI/ICEA S-86-634-2011, *Buried Telecommunications Wire-Filled, Polyolefin Insulated, Copper Conductor Technical Requirements*.
- ANSI/ICEA S-87-640-2011, *Optical Fiber Outside Plant Communications Cable.*
- ANSI/IEA S-89-648-2006, *Telecommunications Aerial Service Wire Technical Requirements*.
- ANSI/ICEA S-90-661-2008, *Category 3, 5, & 5e Individually Unshielded Twisted-Pair Indoor Cable for Use in General Purpose and LAN Communication Wiring Systems Technical Requirements.*
- ANSI/ICEA S-91-674-2006, *Coaxial and Coaxial/Twisted-Pair Composite Buried Service Wires Technical Requirements.*
- ANSI/ICEA S-98-688-2006, *Broadband Twisted-Pair Cable, Aircore, Polyolefin Insulated Copper Conductors Technical Requirements.*
- ANSI/ICEA S-99-689-2006, *Broadband Twisted-Pair, Cable Filled, Polyolefin Insulated Copper Conductors Technical Requirements.*

 © 2012 BICSI®

United States (U.S.) Codes and Standards, continued

- ANSI/ICEA S-101-699-2001, *Standard For Category 3 Individually Unshielded Twisted-Pair Indoor Cable For Use In General Purpose Non-LAN Telecommunications Wiring Systems Technical Requirements.*
- ICEA S-102-700-2004, *Category 6 Individually Unshielded Twisted-Pair Indoor Cables (With or Without An Overall Shield) for Use in Communication Wiring Systems Technical Requirements.*
- ICEA S-103-701-2005, *Riser Cables Technical Requirements.*
- ICEA S-104-696-2001, *Indoor-Outdoor Optical Fiber Cable.*
- ICEA S-106-703-2006, *Broadband Aerial Service Wire – Aircore, Polyolefin, Copper Conductors.*
- ICEA S-107-704-2006, *Broadband Buried Service Wire – Filled, Polyolefin Insulated, Copper Conductors.*
- ICEA S-109-709-2005, *Distribution Frame Wire Technical Requirements.*
- ICEA S-110-717-2003, *Optical Fiber Drop Cable.*

National Electrical Contractors Association (NECA)

The NECA develops and produces national installation standards. Standards of interest are:

- ANSI/NECA/BICSI 568-2006, *Standard for Installing Commercial Building Telecommunications Cabling.*
- ANSI/NECA/BICSI 607-2011, *Telecommunications Bonding and Grounding Planning and Installation Methods for Commercial Buildings.*

National Fire Protection Association® (NFPA®)

The NFPA® develops and produces fire and safety standards and codes. The following codes and standards are associated with telecommunications:

- NFPA 13, *Standard for the Installation of Sprinkler Systems,* 2010.
- NFPA 70®, *National Electrical Code®* (*NEC®*), 2011.
- NFPA 70E®, *Standard for Electrical Safety in the Workplace®*, 2012.
- NFPA 72®, *National Fire Alarm and Signaling Code®*, 2010.
- NFPA 75, *Standard for the Protection of Information Technology Equipment*, 2009.
- NFPA 76, *Standard for the Fire Protection of Telecommunications Facilities*, 2009.
- NFPA 90A, *Standard for the Installation of Air-Conditioning and Ventilating Systems*, 2009.
- NFPA 99, *Standard For Health Care Facilities,* 2012.

United States (U.S.) Codes and Standards, continued

- NFPA 101®, *Life Safety Code®*, 2012.
- NFPA 262, *Standard Method of Test for Flame Travel and Smoke of Wires and Cables for Use in Air-Handling Spaces*, 2011.
- NFPA 520, *Standard on Subterranean Spaces*, 2010.
- NFPA 730, *Guide for Premises Security*, 2011.
- NFPA 731, *Standard for the Installation of Electronic Premises Security Systems*, 2011.
- NFPA 780, *Standard for the Installation of Lightning Protection Systems*, 2011.
- NFPA 1221, *Standard for the Installation, Maintenance, and Use of Emergency Services Communications Systems*, 2010.
- NFPA 5000®, *Building Construction and Safety Code®*, 2009.

NFPA 70 *National Electrical Code® (NEC®)*

The NFPA sponsors, controls, and publishes the *NEC®* within the U.S. jurisdictional area. The *NEC®* is intended to protect people and property from electrical hazards. The *NEC®* specifies minimum provisions necessary to safeguard persons and property from electrical hazards.

In the United States, most federal, state, and local municipalities have adopted the *NEC®*, in whole or in part, as their legal electrical code. Some states or localities adopt the *NEC®* and add more stringent requirements. Local jurisdiction determines the current edition recognized and does not always adopt the latest edition.

The *NEC®*, which is revised every three years, is used by:

- Fire marshals and electrical inspectors in loss prevention and safety enforcement.
- Attorneys and insurance companies to determine liability.

In buildings that will contain the telecommunications systems, the *NEC®* requirements do not address the electrical environment for reliable and error-free operation of the installed equipment. Additional considerations beyond those necessary for safety are described in performance standards.

The following list of chapters, articles, and sections is not intended to be all-inclusive. They are a representation of those that may impact telecommunications installations. The reader is advised to read the code carefully and verify interpretations with local code enforcement officials since jurisdiction of codes is their responsibility.

The *NEC®* allows Chapter 8: Communications Systems to be separate and independent of the other chapters and articles of the code unless specifically referenced within Chapter 8. Although not all of the articles and sections listed in Table A.5 are referenced by Chapter 8, the information in these articles and sections apply to telecommunications.

 © 2012 BICSI®

United States (U.S.) Codes and Standards, continued

Table A.5
NEC® 2011 chapters, articles, and sections that impact telecommunications installation

NEC® Reference	Title
Article 90	Introduction
Section 90.1	Purpose
Section 90.2	Scope
Section 90.3	Code Arrangement
Section 90.4	Enforcement
Section 90.5	Mandatory Rules, Permissive Rules, and Explanatory Material
Section 90.7	Examination of Equipment for Safety
Section 90.8	Wiring Planning
Article 100	Definitions
Article 110	Requirements for Electrical Installations
Section 110.12	Mechanical Execution of Work
Section 110.26	Spaces About Electrical Equipment
Section 110.32	Work Space About Equipment
Section 110.33	Entrance to Enclosures and Access to Working Space
Section 110.34	Work Space and Guarding
Article 200	Use and Identification of Grounded Conductors
Article 210	Branch Circuits
Section 210.25	Branch Circuits in Buildings with More Than One Occupancy
Article 225	Outside Branch Circuits and Feeders
Section 225.14	Open-Conductor Spacings
Article 250	Grounding and Bonding
Section 250.32	Buildings or Structures Supplied by a Feeder(s) or Branch Circuit(s)
Section 250.50	Grounding Electrode System
Section 250.52	Grounding Electrodes
Section 250.53	Grounding Electrode System Installation
Section 250.60	Use of Strike Termination Devices
Section 250.70	Methods of Grounding and Bonding Conductor Connection to Electrodes
Section 250.104	Bonding of Piping Systems and Exposed Structural Steel
Article 280	Surge Arresters, Over 1 kV
Article 285	Surge-Protective Devices (SPDs), 1 kV or Less

United States (U.S.) Codes and Standards, continued

Table A.5, continued
NEC® 2011 chapters, articles, and sections that impact telecommunications installation

NEC® Reference	Title
Article 300	Wiring Methods
Section 300.1	Scope
Section 300.3	Conductors
Section 300.4	Protection Against Physical Damage
Section 300.11	Securing and Supporting
Section 300.21	Spread of Fire or Products of Combustion
Section 300.22	Wiring in Ducts Not Used for Air Handling, Fabricated Ducts for Environmental Air and Other Spaces for Environmental Air (Plenums)
Article 310	Conductors for General Wiring
Article 314	Outlet, Device, Pull, and Junction Boxes; Conduit Bodies; Fittings; and Handhole Enclosures
Article 324	Flat Conductor Cable: Type FCC
NOTE: The following Articles within Chapter 3 primarily address pathway considerations.	
Article 342	Intermediate Metal Conduit: Type IMC
Article 344	Rigid Metal Conduit: Type RMC
Article 348	Flexible Metal Conduit: Type FMC
Article 350	Liquidtight Flexible Metal Conduit: Type LFMC
Article 352	Rigid Polyvinyl Chloride Conduit: Type PVC
Article 356	Liquidtight Flexible Nonmetallic Conduit: Type LFNC
Article 358	Electrical Metallic Tubing: Type EMT
Article 360	Flexible Metallic Tubing: Type FMT
Article 362	Electrical Nonmetallic Tubing: Type ENT
Article 366	Auxiliary Gutters
Article 372	Cellular Concrete Floor Raceways
Article 374	Cellular Metal Floor Raceways
Article 376	Metal Wireways
Article 378	Nonmetallic Wireways
Article 386	Surface Metal Raceways

 © 2012 BICSI®

United States (U.S.) Codes and Standards, continued

Table A.5, continued
NEC® 2011 chapters, articles, and sections that impact telecommunications installation

NEC® Reference	Title
Article 388	Surface Nonmetallic Raceways
Article 390	Underfloor Raceways
Article 392	Cable Trays
Article 400	Flexible Cords and Cables
Article 500	Hazardous (Classified) Locations, Classes I, II, and III, Divisions 1 and 2
Article 605	Office Furnishings (Consisting of Lighting Accessories and Wired Partitions)
Article 640	Audio Signal Processing, Amplification, and Reproduction Equipment
Article 645	Information Technology Equipment
Article 647	Sensitive Electronic Equipment
Article 701	Legally Required Standby Systems
Article 720	Circuits and Equipment Operating at Less Than 50 Volts
Article 725	Class 1, Class 2, and Class 3 Remote-Control, Signaling, and Power-Limited Circuits
Article 760	Fire Alarm Systems
Article 770	Optical Fiber Cables and Raceways
Article 800	Communications Circuits
Article 810	Radio and Television Equipment
Article 820	Community Antenna Television and Radio Distribution Systems
Article 830	Network-Powered Broadband Communications Systems
Article 840	Premises-Powered Broadband Communications Systems

EMT = Electrical metallic tubing
ENT = Electrical nonmetallic tubing
FCC = Flat conductor cable
FMC = Flexible metal conduit
FMT = Flexible metallic tubing
IMC = Intermediate metal conduit
kV = Kilovolt
LFMC = Liquidtight flexible metal conduit
LFNC = Liquidtight flexible nonmetal conduit
PVC = Polyvinyl chloride
RMC = Rigid metal conduit
SPD = Surge-protective devices

United States (U.S.) Codes and Standards, continued

Project Management Institute (PMI)

The Project Management Institute (PMI) is a not-for-profit organization that advances the project management profession through globally recognized standards and certifications, collaborative communities, an extensive research program, and professional development opportunities.

- ANSI/PMI 99-001, *A Guide to the Project Management Body of Knowledge (PMBOK Guide) - Fourth Edition*, 2008.

Rural Utilities Service (RUS)

The Rural Utilities Service (RUS) is an agency of the U.S. Department of Agriculture, which provides documents and specifications for telecommunications within rural areas of the United States.

Some key documents include:

- Bulletin 1751F-630, *Design of Aerial Plant,* 1996.
- Bulletin 1751F-635, *Aerial Plant Construction*, 1995.
- Bulletin 1751F-640, *Design of Buried Plant-Physical Considerations,* 1995.
- Bulletin 1751F-641, *Construction of Buried Plant,* 1995.
- Bulletin 1751F-642, *Construction Route Planning of Buried Plant,* 1995.
- Bulletin 1751F-643, *Underground Plant Design,* 2002.
- Bulletin 1751F-644, *Underground Plant Construction,* 2002.
- Bulletin 1751F-650, *Aerial Plant Guying and Anchoring,* 1996.
- Bulletin 1751F-815, *Electrical Protection of Outside Plant,* 1995.
- Bulletin 1753F-204, *REA Specification for Aerial Service Wires (PE-7),* 1996.
- Bulletin 1753F-205, *REA Specification for Filled Telephone Cables (PE-39),* 1993.
- Bulletin 1753F-206, *REA Specification for Filled Buried Wire (PE-86),* 1993.
- Bulletin 1753F-208, *REA Specification for Filled Telephone Cables with Expanded Insulation (PE-89),* 1993.
- Bulletin 1753F-601a*, Minimum Performance Specification For Fiber Optic Cables (For Backbone, Feeder, and Distribution Plant) (PE-90a),* 2009.
- Bulletin 1753F-601b, *Minimum Performance Specification For Fiber Optic Cables* (*Subscriber Drop Cables*), *2009*.

 © 2012 BICSI®

United States (U.S.) Codes and Standards, continued

Society of Cable Telecommunications Engineers (SCTE)

SCTE produces documents and standards relating to broadband telecommunication cable systems. Some important standards are:

- ANSI/SCTE 15-2006, *Specification for Trunk, Feeder, and Distribution Coaxial Cable.*
- ANSI/SCTE 47-2007, *Test Method for Coaxial Cable Attenuation.*
- ANSI/SCTE 60-2010, *Test Method For Interface Moisture Migration Double Ended.*
- ANSI/SCTE 71-2008, *Specification for Braided, 75—Coaxial, Multi-Purpose Cable.*
- ANSI/SCTE 74-2011, *Specification for Braided 75—Flexible RF Coaxial Drop Cable.*
- ANSI/SCTE 117-2010, *Specification for Braided 75—Mini-Series Broadband Coaxial Cable*.
- ANSI/SCTE 129-2007, *Drop Passives: Bonding Blocks (without Surge Protection).*
- ANSI/SCTE 146-2008, *Outdoor "F" Female to "F" Female Inline Splice.*
- ANSI/SCTE 147-2008, *Specification for 75 Ohm, Inline Attenuators.*
- ANSI/SCTE 148-2008, *Specification for Male "F" Terminator, 75 Ohm.*
- ANSI/SCTE 151-2008, *Mechanical, Electrical, and Environmental Requirements for RF Traps and Filters.*
- ANSI/SCTE 153-2008, *Drop Passives: Splitters, Couplers and Power Inserters.*
- ANSI/SCTE 155-2008, *Indoor "F" Female to "F" Female Inline Splice.*
- ANSI/SCTE 161-2009, *Drop Amplifiers.*
- ANSI/SCTE 167-2010, *Recommended Practice for Headend Cable Color Coding.*
- ANSI/SCTE 174 2010*, Radio Frequency over Glass Fiber-to-the-Home Specification.*
- ANSI/SCTE 178 2011, *Test Method for Cable Weld Integrity.*
- SCTE 182 2011, *Broadband Compliance Guidelines for the NEC.*
- SCTE 183 2002, *Recommended Practices for Measurements on Cable Telecommunications Systems*.

United States (U.S.) Codes and Standards, continued

Telecommunications Industry Association (TIA)

TIA is accredited by ANSI to develop voluntary industry standards for a wide variety of telecommunications products.

The TIA Standards and Technology Department is composed of five divisions:

- Fiber Optics
- User Premises Equipment
- Network
- Wireless Communications
- Satellite Communications

TIA produces several documents and standards that affect telecommunications, notably the telecommunications building cabling standards, including the 568-C Series.

Among the most notable TIA documents and standards are:

- TIA-526-7 (OFSTP-7)-2002+A1:2008, *Measurement of Optical Power Loss of Installed Single-Mode Fiber Cable Plant*. This standard specifies singlemode optical loss measurement methods between two passively connected points using an optical source and power meter.
- TIA-526-14-B-2010 (OFSTP-14), *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*. This standard is used to measure the optical loss between any two passively connected points, including end terminations, of a multimode optical fiber cable plant.
  - The optical fiber cable plant, as the term is used here, may consist of optical fiber cables, connectors, mounting panels, jumper cables, and other passive components, but it may not include active components. This standard includes an encircled flux launch condition metric for measuring cable plant. Additionally, this standard includes the description of using an optical time domain reflectomer (OTDR) for total attenuation measurement and measurements of individual component loss.
- ANSI/TIA-568-C.0–2009+A1:2010+A2:2012, *Generic Telecommunications Cabling for Customer Premises*. This standard specifies requirements for generic telecommunications cabling. It specifies requirements for cabling system structure, topologies and distances, installation, performance, and testing. The purpose of this standard is to enable the planning and installation of a structured cabling system for all types of customer premises. This standard specifies a system that will support generic telecommunications cabling in a multiproduct, multi-vendor environment.

 © 2012 BICSI®

United States (U.S.) Codes and Standards, continued

- ANSI/TIA-568-C.1–2009+A1:2012, *Commercial Building Telecommunications Cabling Standard.* This standard specifies requirements for telecommunications cabling within a commercial building and between commercial buildings in a campus environment. It defines terms, specifies cabling topology, lists cabling requirements, establishes cabling distances, sets telecommunications outlet/connector configurations, and provides additional useful information. The purpose of this standard is to enable the planning and installation of a structured cabling system for commercial buildings. This standard establishes performance and technical criteria for various cabling system configurations for accessing and connecting their respective elements.
- ANSI/TIA-568-C.2–2009+A1:2010, *Balanced Twisted-Pair Telecommunications Cabling and Components Standard.* This standard specifies minimum requirements for balanced twisted-pair telecommunications cabling (e.g., channels, permanent links) and components (e.g., cable, connectors, connecting hardware, patch cords, equipment cords, work area cords, jumpers) that are used up to and including the telecommunications outlet/connector and between buildings in a campus environment. This standard also specifies field test procedures and applicable laboratory reference measurement procedures for all transmission parameters.
- ANSI/TIA-568-C.3–2009+A1:2011, *Optical Fiber Cabling Components Standard.* This standard is applicable to premises optical fiber cabling components. Specified in this standard are requirements for components such as cable, connectors, connecting hardware, and patch cords. The purpose of this standard is to specify cable and component transmission performance requirements for premises optical fiber cabling. It is intended to be used by manufacturers; however, users, designers, and installers may also find this standard useful.
- ANSI/TIA-568-C.4–2011, *Broadband Coaxial Cabling and Components Standard.* This standard is limited to coaxial cable and components related to the broadband transport industries.
- ANSI/TIA-569-C–2012, *Telecommunications Pathways and Spaces.* This standard is limited to the telecommunications aspect of commercial building design and construction, encompassing telecommunications pathways and spaces. Telecommunications pathways are designed for installation of telecommunications media, and telecommunications spaces are the rooms and areas where media is terminated and telecommunications equipment is installed. Both single- and multi-tenant buildings are recognized by this standard.
- ANSI/TIA-570-C–2012, *Residential Telecommunications Infrastructure Standard.* This document standardizes requirements for residential telecommunications cabling. These requirements are based on the facilities that are necessary for existing and emerging telecommunications services, including security, home audio, and building control cabling systems.

United States (U.S.) Codes and Standards, continued

- ANSI/TIA/EIA-598-C–2005, *Optical Fiber Cable Color Coding*. This standard specifies the recommended identification for individual fibers, fiber units, and groups of fiber units within a cable structure. The methods contained may be used to identify and locate specific fibers for the purpose of connection, termination, or testing within a communication system or for the topography of long haul, feeder route, subscriber, or distribution applications for both on-premises and OSP use. This standard also specifies the optical fiber type identification for color-coding or marking jackets for premises cables used primarily indoors.
- ANSI/TIA-606-B-2012, *Administration Standard for Commercial Telecommunications Infrastructure*. This standard specifies administration systems for commercial telecommunications infrastructure with choices of classes of administration for maintaining telecommunications infrastructure. This infrastructure may range in size from a building requiring a single telecommunications space (TS) and associated elements to many TSs and associated elements in multiple campus locations. This standard applies to administration of telecommunications infrastructure in existing, renovated, and new buildings.
- ANSI/TIA-607-B-2011, *Commercial Building Grounding (Earthing) and Bonding Requirements for Telecommunications*. The purpose of this standard is to enable the planning, design, and installation of telecommunications bonding and grounding (earthing) systems within a building with or without prior knowledge of the telecommunications systems that will subsequently be installed. This standard also provides recommendations for grounding (earthing) and customer-owned towers and antennas. This telecommunications bonding and grounding (earthing) infrastructure supports a multi-vendor, multiproduct environment as well as various system installation practices.
- ANSI/TIA-758-B–2012, *Customer-Owned Outside Plant Telecommunications Infrastructure Standard*. This document provides requirements used in the design of the telecommunication pathways and spaces, and the cabling installed between buildings or points in a customer-owned campus environment. Customer-owned campus facilities are typically termed outside plant. For the purpose of this standard, they are termed "customer-owned OSP."
- ANSI/TIA-862-A–2011, *Building Automation Systems Cabling Standard.* This document specifies a generic cabling system for building automation systems (BAS) that will support a multiproduct, multi-vendor environment. It also provides information that may be used for the design of BAS products for commercial enterprises.
- ANSI/TIA-942-A-2012, *Telecommunications Infrastructure Standard for Data Centers.* This standard specifies the minimum requirements for telecommunications infrastructure of data centers and computer rooms, including single tenant enterprise data centers and multi-tenant Internet hosting data centers. The topology proposed in this document is intended to be applicable to any size data center.

 © 2012 BICSI®

United States (U.S.) Codes and Standards, continued

- ANSI/TIA-1005-A–2012, *Telecommunications Infrastructure Standard for Industrial Premises*. This standard specifies telecommunications cabling to support industrial premises applications (e.g., voice, data, text, video, industrial and building controls, security, fire alarm, image) while allowing for exposures to wider ranges than most commercial environments (e.g., temperature, humidity, electrical noise, shock, vibration, corrosive gases, dust, liquids). This standard is to enable the planning and installation of the telecommunications cabling infrastructure within and between industrial buildings such as manufacturing facilities, laboratories, and refineries. In these industrial premises, the cabling infrastructure may be exposed to environments more hostile than in commercial buildings and where the cabling must support applications and topologies specific to industrial premises. It provides cabling requirements, cabling distances, telecommunications outlet/connector configurations, and topologies. It describes environmental classifications and provides information that is useful for designing an appropriate telecommunications infrastructure.
- ANSI/TIA-1152–2009, *Requirements for Field Test Instruments and Measurements for Balanced Twisted-Pair Cabling.* This standard includes requirements for field test instruments that are used to test balanced twisted-pair cabling as specified in the ANSI/TIA-568-C series of structured cabling standards. This standard specifies the reporting and accuracy performance requirements of field testers for balanced twisted-pair cabling measurements. Level IIe, III, and IIIe field tester requirements are specified in this standard. This standard contains methods to compare the field instrument measurements against laboratory equipment measurement specified in ANSI/TIA-568-C.2. Measurement accuracy based upon the assumptions for key performance parameters is addressed.
- ANSI/TIA-1179–2010, *Healthcare Facility Telecommunications Infrastructure Standard.* This standard specifies requirements for telecommunications infrastructure for health care facilities (e.g., hospitals, clinics). It specifies cabling, cabling topologies, and cabling distances. Additionally, pathways and spaces (e.g., sizing, location) and ancillary requirements are addressed. Telecommunications cabling specified by this standard is intended to support a wide range of health care facilities and systems. In addition to telecommunication systems, the telecommunications cabling specified by this standard is intended to support a wide range of clinical and non clinical systems (e.g., radio frequency interference, BAS, nurse call, security, access control, pharmaceutical inventory), particularly those which utilize or can utilize IP-based infrastructure.
- ANSI/TIA-1183–2012, *Test Fixtures for Balun-Less Measurements of Balanced Components and Systems.*

Enforcement of United States (U.S.) Building Codes, Standards, and Regulations

Overview

Generally, codes of state or federal regulations are enforced by the same local agency responsible for issuing building permits. In almost all communities, the local government produces ordinances establishing building codes and standards for that jurisdiction.

Some states established statutory regulations that are the minimum conditions under which any local government may permit construction to occur.

In many areas, it is the responsibility of the local fire marshal to:

- Establish local codes.
- Enforce the codes for fire protection in buildings.

Double Requirements

In some areas, compliance with more than one set of codes or regulations is required such as obtaining city and county construction permits.

Local Applications of National Standards

In almost all areas of the United States, local and state governments adopt all or major portions of the building codes. In most cases, local code-making bodies make editorial and technical modifications to the major code they adopt.

In almost all cases, a significant portion of the U.S. national fire codes is either adopted or used as a pattern by local government agencies. Significant in this standardization within the United States is the NEC®, produced as NFPA 70.

 © 2012 BICSI®

Government and Military Construction

Construction for branches of the U.S. military and Federal agencies must comply with standards established by those service branches and government agencies.

The following are a sample of such standards and practices:

- FEMA 426, Reference Manual to Mitigate Terrorist Attacks Against Buildings.
- FEMA 430, Site and Urban Design for Security - Guidance against Potential Terrorist Attacks.
- Unified Facilities Criteria, Telecommunications Building Cabling Systems Planning and Design (UFC 3-580-01).
- Unified Facilities Criteria, DOD Minimum Antiterrorism Standards for Buildings (UFC 4-010-01).
- Unified Facilities Criteria, Entry Control Facilities/Access Control Points (UFC 4-022-01).
- Unified Facilities Criteria, Selection and Application of Vehicle Barriers (UFC 4-022-02).
- Unified Facilities Criteria, Design and O&M: Mass Notification Systems (UFC 4-021-01).
- U.S. General Services Administration (GSA) “The Site Security Design Guideline Manual.”
- NIST- FIPS-201, Federal Information Processing Standards.
- Crime Prevention Through Environmental Design (CPTED).

Government and military construction are not normally subject to local government jurisdiction. However, most government and military branch standards:

- Follow the guidelines of national codes.
- Adopt the national codes in their own standards.

Federal Safety Health Standards

The federal government, through the Occupational Safety and Health Act (OSHA), enforces the safety aspects of codes and standards as they apply to employee working conditions.

The following construction-related regulations are specific to safety requirements that would apply for installation of telecommunications systems are shown in Table A.6.

Table A.6
Federal safety health standards

Specification/ Standard Number	Title	Date
29CFR1910	*Code of Federal Regulations Title 29, Labor— Part 1910: Occupational Safety and Health Standards*	2008
29CFR1910.146	*Code of Federal Regulations Title 29, Labor— Part 1910.146: Permit-Required Confined Spaces*	2008
29CFR1910.1001	*Code of Federal Regulations Title 29, Labor— Part 1910.1001: Asbestos*	2008
29CFR1910.1926	*Code of Federal Regulations Title 29, Labor— Part 1910; 1926: Safety Standards for Fall Protection in the Construction Industry*	2008

 © 2012 BICSI®

Regulations and Standards for Wireless Transmission

Wireless Regulations, Standards, Codes, and Organizations

Wireless communications has existed for more than 100 years. For that long, it has had an international quality, exemplified by Guglielmo Marconi's demonstration of a transatlantic radiotelegraphy link in 1901. A number of international and regional standards and regulations in the wireless arena have been adopted since then.

On the following pages, the major standards, regulations, and codes that influence the installation and operation of communications devices utilizing the radio spectrum are listed. The role of various organizations in the wireless space and the synergies between them are also provided.

The major areas covered include:

- Wireless standards development organizations.
- Wireless standards and technologies in the following areas:
  - Personal area network (PAN).
  - LAN.
  - Metropolitan area network (MAN).
  - Wide area network (WAN).
  - Global area network (GAN).
- Emerging wireless technologies and related standards.
- Codes and regulations.

Wireless Standards Development Organizations

Several organizations are charged with writing and setting the standards used in the various wireless technologies.

The following are the most prominent:

- Association of Radio Industries and Businesses (ARIB).
- European Telecommunications Standards Institute (ETSI).
- Federal Aviation Administration (FAA).
- Federal Communications Commission (FCC).
- Industry Canada.
- Institute of Electrical and Electronics Engineers® (IEEE®).
- International Civil Aviation Organization (ICAO).
- International Electrotechnical Commission (IEC).
- International Organization for Standardization (ISO).
- Occupational Safety and Health Administration (OSHA).
- Telecommunications Industry Association (TIA).
- Telecommunications Technology Association (TTA).
- Telecommunication Technology Committee (TTC).

Association of Radio Industries and Businesses (ARIB)

ARIB is based in Japan and conducts investigations, research and development, and consultation, and it establishes standards for the utilization of radio waves from the view of developing radio industries.

ARIB promotes the realization and popularization of new radio systems in the field of telecommunications and broadcasting.

European Telecommunications Standards Institute (ETSI)

ETSI is a nonprofit organization with a mission to produce telecommunications standards for use in Europe and beyond. ETSI unites more than 700 member organizations from 62 countries and represents administrations, network operators, manufacturers, SPs, research organizations, and users.

ETSI plays a major role in developing a wide range of standards and other technical documentation as Europe's contribution to worldwide standardization in telecommunications, broadcasting, and IT.

The prime objective of ETSI is to support global harmonization by providing a forum in which all of the key players can contribute actively.

European Telecommunications Standards Institute (ETSI), continued

ETSI is actively involved in developing standards for over 30 key technical areas, including:

- Third generation (3G) global system for mobile communications (GSM).
- High-performance radio LAN type 1 (HiperLAN/1).
- HiperLAN/2.
- Digital enhanced cordless telecommunications (DECT).
- Mobility for emergency and safety applications.
- Radio spectrum.
- Short-range devices.

Federal Aviation Administration (FAA)

The FAA cannot enforce telecommunications tower regulations as this authority lies solely with the FCC. However, to help ensure aviation safety, the FCC requires that the FAA be notified of any proposed construction or modification to a tower above 61 m (200 ft). Tower installation companies must submit their proposed projects to the FAA and request a "determination of no hazard to air navigation" in return.

Federal Communications Commission (FCC)

The FCC regulates the towers with antennas through the antenna structure registration (ASR) program. All applicable equipment must have an FCC authorization. The requirements for equipment authorization are found in Title 47 of the *Code of Federal Regulations (CFR)*. The rules cover a diverse range of subjects from FCC organization to requirements for different radio services and maximum permissible heights for antennas located near airports (see Table A.7).

Table A.7
Federal Communications Commission regulations

Specification/ Standard Number	Title	Date
47CFR22	Code of Federal Regulations Title 47, Telecommunications—Part 22: Public Mobile Services	2008
47CFR42-69	Code of Federal Regulations Title 47, Telecommunications—Parts 42–69	2008
47CFR68	Code of Federal Regulations Title 47, Telecommunications—Part 68: Connection of Terminal Equipment to the Telephone Network	2008
47CFR76	Code of Federal Regulations Title 47, Telecommunications—Part 76: Multichannel Video and Cable Television Service	2008
47CFR76.605	Code of Federal Regulations Title 47, Telecommunications—Part 76.605: Technical Standards	2008

Industry Canada

Industry Canada (IC) is the government department responsible for regulating telecommunications equipment in Canada. Section 5 of the Radiocommunication Act and Section 69.3 of the Telecommunications Act give the Minister of Industry the authority to develop technical standards and to ensure that telecommunications equipment meets these standards. The term "telecommunications equipment" is used as a generic term covering telecommunications apparatus (terminal equipment which connects directly to the public switched telephone network), radio equipment (equipment intended for, or capable of being used for, radio communication), broadcasting equipment (radio and TV equipment intended for broadcasting services) and interference-causing equipment (equipment, other than radio receivers, that causes or is capable of causing interference to radio communications).

Institute of Electrical and Electronics Engineers® (IEEE®)

The work of the IEEE 802 LMSC is of particular interest to wireless practitioners (see the IEEE section in this appendix).

International Civil Aviation Organization (ICAO)

ICAO, an agency of the United Nations, develops the principles and techniques of international air navigation and fosters the international air transport planning and development to ensure a safe and orderly growth.

The ICAO Council adopts standards and recommended practices concerning air navigation, prevention of unlawful interference, and facilitation of border-crossing procedures for international civil aviation.

In addition, it defines the protocols for air accident investigation for the transport safety authorities of the Chicago Convention signatories. The ICAO rules that impact the wireless design include the heights and markings of structures around airports required for a smooth flight operation and accident prevention.

International Electrotechnical Commission (IEC)

See the section on IEC in this appendix.

International Organization for Standardization (ISO)

See the section on ISO in this appendix.

Occupational Safety and Health Administration (OSHA)

OSHA is an agency of the U.S. Department of Labor. OSHA specifies regulations for the protection of workers who build, service, or operate wireless infrastructure towers.

Telecommunications Industry Association (TIA)

See the section on TIA in this appendix.

Telecommunications Technology Association (TTA)

TTA is an IT standards organization in Korea that develops new standards and provides services for the establishment of IT standards as well as testing and certification for IT products.

The scope of TTA activities includes telecommunications, IT, radio communications, and broadcasting. TTA has been working on over 2000 standards.

Telecommunication Technology Committee (TTC)

The purpose of this Japanese committee is to contribute to standardization efforts in the field of telecommunications by establishing protocols and standards for telecommunications networks and terminal equipment.

United States (U.S.) Approval of Electrical Products and Equipment

Product Certification

Most states or localities accept certification of electrical products by a national testing laboratory as evidence that products and materials are safe for use in that jurisdiction.

Some agencies may perform their own tests to determine acceptability for installation in their jurisdiction.

Some examples of performed tests from Underwriters Laboratories® (UL®) Inc. are:

- UL 723, *Test for Surface Burning Characteristics of Building Materials*, 2004.
- UL 1666, *Standard for Test for Flame Propagation Height of Electrical and Optical- Fiber Cables Installed Vertically in Shafts*, 2007.
- UL 1685, *Standard for Vertical-Tray Fire-Propagation and Smoke-Release Test for Electrical and Optical-Fiber Cables*, 2007.

Product Ratings

The categories used within the United States to rate products are:

- Listed.
- Classified.
- Recognized.
- Verified.

Listed

A product is listed after it successfully completes a series of mechanical, electrical, and thermal characteristics tests that simulate all reasonable, foreseeable hazards.

The listed classification is exclusive to the product for the specific applications for which it was tested and is not valid for other applications.

Classified

A product is classified after it is evaluated and passes tests for one or more of the following:

- Specific hazards only
- Performance under specified conditions
- Regulatory codes
- Other standards, including international standards

The classified rating is generally restricted to industrial or commercial products.

 © 2012 BICSI®

Product Ratings, continued

Recognized

A product is recognized after it is tested for use as a component in a listed package and passes. These component products are tested for electrical, mechanical, and thermal characteristics.

The recognized classification is a more general-purpose approval than listed because it allows a product to be certified for a category of equipment uses.

An example is insulated wire, which is recognized as appliance wiring material, a category of uses that includes:

- Data communications.
- Telecommunications.
- Instrumentation.

Verified

UL® also produces a performance verification of communications cabling with the classification of verified. Cabling manufacturers and their cabling types are listed in the UL® publication, *Performance Levels Certification Program*, for meeting the base performance criteria for the product such as category 3, 5e, and 6.

A performance verification mark allows manufacturers to demonstrate that telecommunications cabling products are certified for both safety and performance, and they comply with industry performance standards and draft standards.

The UL® performance verification mark also signifies the testing of copper and optical fiber cabling products to industry performance standards such as ANSI/TIA, ISO/IEC 11801Ed.2:2002, NEMA, and Telcordia.

It can also be applied to UL®-listed optical fiber cable verified to Telcordia specifications. The verification mark may also be applied to data transmission or optical fiber cable verified to performance specifications only.

Test Standards

The following standards, though not directly or indirectly related to cabling or transmission systems, are applicable to telecommunications:

- ASTM E84-2010, *Standard Test Method for Surface Burning Characteristics of Building Materials*.
- UL 13-2007, *Power-Limited Circuit Cables*.
- UL 444-2008, *Communications Cables*.

Canadian Approval of Electrical Products and Equipment

Product Certification

All provinces or territories accept certification of electrical products by a recognized (the Standards Council of Canada) testing laboratory to the applicable CEC Part II standard as evidence that products and materials are safe for use in that jurisdiction.

Some agencies may perform their own tests to determine acceptability for installation in their jurisdiction per CSA SPE-1000, the standard for *Model Code for the Field Evaluation of Electrical Equipment.*

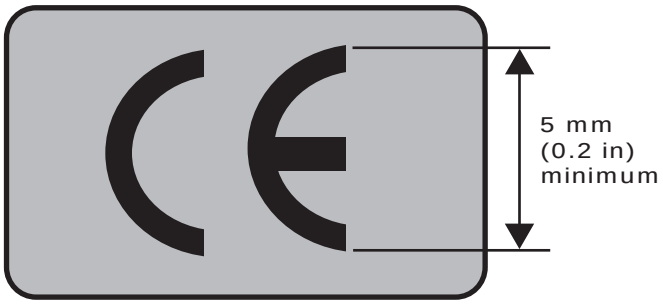
Some examples of performed tests from the CSA are:

- CSA C22.2 No. 0.3-01 (R2005), Test Methods for Electrical Wires and Cables.
- CSA C22.2 No. 214-08, Communications Cables.
- CSA C22.2 No. 232-M1998 (R2004), Optical Fiber Cables.

European Union CE (conformité européenne) Mark

For products placed on the single market in the European Economic Area (EEA), they are required to meet the applicable EU consumer safety, health, or environmental requirements. For electronic products and equipment to show that a product conforms to the EU's EMC Directive (and all applicable directives), the product must be labeled with the conformité européenne (CE) mark as shown in Figure A.1.

Figure A.1
Conformité européenne (CE) mark



in = Inches
mm = Millimeters

 © 2012 BICSI®

European Union CE (conformité européenne) Mark, continued

The CE mark may be placed on the:

- Equipment.
- Equipment packaging.
- Instructions for use guidelines.
- Guarantee certificate.

For IT equipment (e.g., computers, computer peripherals), the requirements of the CENELEC EN 55022 standard are similar to the FCC EMI requirements. CENELEC EN 55022 and its companion document, IEC CISPR-22, describe test procedures and limits similar to, but not identical to, the FCC Part 15 requirements and the ANSI/IEEE C63.4 test procedures.



Appendix B: Legal Aspects of Electronic Safety and Security Design

Appendix B examines some of the legal issues relevant to the finding or avoidance of liability.

Table of Contents

Legal Aspects of Electronic Safety and Security (ESS) Design B-1
Electronic Safety and Security (ESS) Designer's Environment B-1
Basis for Liability B-1
Legal Issues B-3
General Duties of the Electronic Safety and Security (ESS) Designer B-3
Liability in Contract B-4
Liability in Tort—Secondary Liability B-5
Limiting Legal Costs B-8
Alternative Dispute Resolution B-8
Mediation B-9
Arbitration B-9
Limiting the Electronic Safety and Security (ESS) Designer's Liability B-10

Legal Aspects of Electronic Safety and Security (ESS) Design

Electronic Safety and Security (ESS) Designer's Environment

The designers of any structure or system face a genuine threat of legal action or claim on every project they undertake.

The electronic safety and security (ESS) design may be completed by:

- Architects.
- Engineers.
- Consultants.
- Employees of the client.
- Installers (in some cases).

The ESS designer's job can include providing the client with a complete set of documents for an infrastructure that will meet the client's performance requirements and budget. The ESS designer's work can be limited to technical advice or consulting, but it often will contain plans, specifications, bill of materials, an installation plan, and a cost analysis.

ESS designers typically engage in some form of preliminary on-site survey or inspection. This is necessary because a designed or recommended system must take into account the environmental constraints in which the ESS infrastructure will be installed and operated. This would include consideration of the:

- Appropriate safeguards that may be necessary because of the layout of a particular area.
- Environment.
- Topography.
- Climate.
- Current and future types of equipment to be supported.
- Type of cable.
- Functionality of the network.
- Pathway or space over which the cable will travel.

Basis for Liability

As a general principle, liability is determined on the basis of an objective standard. This is often guided by an industry or professional standard. Courts are likely to interpret contracts or determine liability in negligence on the basis of the acceptable standard within the industry or profession.

The ESS designer's liability is defined by the published industry standards, codes, and norms. Norms may be the most problematic of the three. Norms are dynamic and usually arise in trade usage or trade custom as opposed to the standards and codes, which may have the same purpose as norms but may be less specific.

Basis for Liability, continued

The following definitions convey the general meaning of standards, codes, and norms:

- Standards are a set of minimum requirements established by a standards development organization (e.g., American National Standards Institute [ANSI], International Organization for Standardization [ISO]).
- Codes are rules specified and usually enforceable by governmental entities. These would include local building and safety codes.
- Norms may transcend state and professional regulations. They may represent the informal practices adopted by a particular discipline that are so prevalent that ESS designers may be expected to have knowledge of and adhere to them.

Sometimes, codes and standards are governed by the same organization as others but separately administered. Nevertheless, failure to adhere to these standards, codes, and norms gives rise to legal liability.

The ESS designer should recognize that each case will vary according to its facts and environment. A court has the authority to decide whether a particular standard, code, or norm that is applicable in one context is irrelevant in another. Therefore, ESS designers should use all of the available legal means to protect themselves from liability as early in the project as possible and set a suitable context and environment in which the work will be performed.

In addition to the standards, codes, and norms, the social environment also may impact the liability exposure of ESS designers. Recently, there has been a proliferation of claims against design professionals. Courts have been willing to ignore privity requirements and find design professionals liable to third parties for their actions or omissions. Privity is a legal principle that is peculiar to contract law. It means that only the parties to the contract are able to sue and be sued. This appendix will examine some of the legal issues relevant to the finding and avoidance of liability.

The ESS designer has an additional consideration that is not necessarily associated with other designers. This occurs because most of the design is intended to protect life and property and to provide a safe environment for employees as well as individuals conducting business at the facility. This may require protection starting at the building and extending to the perimeter, including the fence line and points of entry. When this happens or is likely to occur, it is important that the ESS designer clearly define the necessary ESS system best suited to deliver the capabilities and functionalities required by the client or its agents.

 © 2012 BICSI®

Legal Issues

General Duties of the Electronic Safety and Security (ESS) Designer

Like all professionals, ESS designers are required to exercise due care and skill in carrying out their discipline. To reiterate the statement previously made in this appendix, the parameters within which the duty is optimally exercised are determined by the environment and context in which the ESS designer works.

The single most important duty of an ESS designer is to engage in risk assessment and management. The methods of risk assessment and management figure prominently in any determination of legal liability. The assessor must determine what the public's expectation of an ESS designer is and against what standards those expectations will be measured. In such context, contracts can best assist the ESS designer in avoiding, or at least minimizing, the primary liability. An equally important issue is how the ESS designer may avoid secondary liability.

The ESS designer may be found primarily or secondarily liable in the tort of negligence for any loss or damage resulting from a faulty design. The ESS designer has a number of duties related to this issue. The ESS designer must have the basic technical competency acquired through formal education, in-service training or on-the-job experience, certifications/designations/registrations, and the knowledge of current developments in the discipline. Yielding to the professional skills of other persons (e.g., scientific, financial, business, and legal professionals) as required is also important.

Many professional liability claims stem from nontechnical aspects of design practice—the acceptance of onerous contract terms and conditions, poor communication, careless selection of projects, failure to engage in risk assessment and management, failure to record all significant decisions and changes, and lax fee-collection practices.

The ESS designer has a duty to know, observe, and maintain the rules of professional conduct that apply to the profession. In the case of a licensed professional, these rules are generally regulated or enforced by a licensing agency. The licensing agency typically has the power to admonish, censure, suspend, or terminate license or membership.

Regulations and codes are discussed in detail in Appendix A: Codes, Standards, Regulations, and Organizations and are not the subject of this appendix. However, they are important in the context of liability because they can form the basis of disciplinary action with remedies ranging from fines or suspensions to license revocations.

Courts are entitled to consider regulations and codes in determining whether particular contractual stipulations are fair and reasonable and whether a particular faulty design was caused by the ESS designer's negligence.

Negligence is usually determined by referring to the ESS designer's general duty to ensure public safety and welfare, whether on public or private property. This is an area in which the standards, codes, and norms interact with the general law insofar as these rules form a part of the body of law that courts may consider in making a decision on liability.

Legal Issues, continued

Liability in Contract

Liability in contract may be purely contractual or result from negligence. The liability in either case is restricted to the duties as defined in the contract between or among the parties to the contract. This is primary liability. Contracts may be oral or written. The rules of evidence relating to contractual liability are strict.

The general rule is that written contracts cannot be varied by oral or other external evidence. This is usually referred to as the four corners rule, the entire contract doctrine, or an integrated contract. This means that discussions, negotiations, and understandings accomplished prior to the execution of the contract are not admissible to vary the terms of the written document.

There are circumstances in which the court may admit evidence to show that an ambiguity exists or that other terms are incorporated by reference to other documents or discussions. With this in mind, ESS designers should incorporate all of their contract terms in writing, attaching an entire agreement or integration agreement clause. In doing so, they will ensure that no duties other than those agreed between the ESS designer and the client are imposed. This is what the court will consider to confirm the intention of the parties at the time of contracting.

However, the ESS designer should keep in mind that contracts often are premised on implied terms. These implied terms are known as warranties. A warranty will not be found to exist in all cases. Courts do not necessarily acknowledge an implied warranty that the design would be suitable for the intended purpose when appropriate assurances are missing. In such a case, the claimant has to show that the ESS designer has been aware of the circumstances and still gave an assurance or undertaking in the specific terms of the lawsuit.

NOTE: This kind of contractual liability exposes the ESS designer to third-party liability because warranty liability is not limited to negligent performance.

This is an area in which the doctrine of privity of contract has been eroded. The result is an increased exposure of the ESS designer to third-party claims.

Warranty liability is premised on representations that the work would be done in a professional manner—that it would not be defective, and it would conform to the contract documents. The warranty theory establishes a standard of performance rather than a standard of care exercised by the ESS designer and installer as the basis for liability. This liability is best understood by recognizing the changing role of the ESS designer and is more applicable where the ESS designer is a hybrid of consultant/installer, designer/installer, or an installer.

 © 2012 BICSI®

Legal Issues, continued

The distinction between the expectations of the traditional designer in the context of the separation of the five roles and the hybrid designer is that the traditional designer's work does not express or imply a warranty. Unless engaged as part of a design/build project or when employed as a project manager, the ESS designer does not warrant that the work would be carried out in a professional manner or in accordance with the specifications. Both the design/build method of construction and the role of project manager create an obligation that the finished project complies with the client's expectations. Therefore, the risk of the unknown contractually shifts from the client to the design/build firm. Consequently, in this role, the ESS designer is required to perform exactly in accordance with the contractual specifications.

The loss of protection from liability to third parties by the erosion of the "economic loss doctrine" is closely linked to the issues arising from the warranty liability. According to the economic loss doctrine, the ESS designer has no liability to the entities to which the ESS designer does not guarantee contractual privity for purely economic losses or damages.

The economic loss doctrine does not apply in all of the United States. Therefore, ESS designers need to seek appropriate legal advice to determine if the doctrine is applicable in their area. The Florida Supreme Court ruled that the economic loss doctrine originated in the context of product liability cases and, as such, "should not be invoked to bar well-established causes of action in tort, such as professional malpractice." The court thus decided that action can be brought against a professional for negligence even for purely economic damages.

In summary, the argument that there is no contractual relationship between the claimant and the ESS designer may not succeed in some courts. ESS designers therefore may find that they cannot hide behind contractual terms to escape liability. It may be tempting to question the purpose of contracts. However, the importance of clear contractual terms for work and respective risks cannot be overstated. As little as possible should be left to implication or imagination. Furthermore, ESS designers should only accept the work for which they believe they are qualified.

Liability in Tort—Secondary Liability

Although liability for negligence can arise in a contract, it is a separate and distinct head of liability. The distinction between contractual negligence and tortious negligence is that where negligence is claimed under the contract, it will be restricted to, and hence determined in accordance with, the terms of the contract.

Legal Issues, continued

Liability in tort is usually wider than the liability arising under a contract because it is premised on a general duty to exercise due care and skill. Notwithstanding the contract terms, the ESS designer may become liable to third parties for negligence. This is what is commonly referred to as secondary liability. It is based largely on expectation.

The expectation from ESS designers varies based on if, at the material time, they are consulting, designing, or installing; in fact, they may be performing all of the three tasks.

The consultant is in the business of giving professional advice; the ESS designer creates a plan and specification, and the installer implements the system according to the specifications and the plan prepared by the ESS designer. The separation of the various areas of the ESS designer's practice is for ease of analysis (bearing in mind that one person may perform all three functions).

When acting as consultants, ESS designers may be liable for negligent misstatements because they are primarily in the business of giving advice. This liability may be in contract or in tort.

ESS designers and installers may be liable for faulty designs or installations but generally not for negligent misstatements since they would be installing according to another designer's specifications. Liability may be found in a situation where the ESS designer, acting as a designer or installer, fails to design or install according to the client's specifications or fails to exercise their professional judgment to ensure that the design is suitable for the particular environment.

Negligence has five elements:

- Duty
- Foreseeability
- Breach of duty
- Causation
- Damage

The analysis usually begins by finding out who the neighbor is. This does not have a literal meaning and thus does not have to be the person next door. This inquiry sets the framework for dealing with the first element of negligence—duty. The neighbors are the category of persons who are entitled to circumvent the contract and sue ESS designers for damages. Therefore, the ESS designer owes a duty of care to this category of persons.

In several U.S. jurisdictions, it is common for third parties to sue professionals with whom they have no contractual relationship. It is the category of persons whom the ESS designer should consider subject to injury if the job is not performed properly.

Duty imposes a standard of care and skill on the ESS designer. This is measured against what is required in the profession by referring to the standards, codes, and norms that govern that profession in the public interest. This duty varies according to the context in which the ESS designer is working.

 © 2012 BICSI®

Legal Issues, continued

The term context refers to the place, time, or particular circumstances of the task that the ESS designer is required to perform. It varies based on whether they are consulting, designing, installing, or are engaged in a task for which they have no particular expertise. This explains why judges decide each case according to its particular facts even though each case is considered according to the principles of the law that governs the area of liability.

ESS designers must perform only within their areas of competence as the risk of liability for negligence increases with each deviation from their particular expertise and knowledge.

The scope of duty is limited or restricted by the concept of foreseeability. In general, a third party's opportunity to sue is restricted to whether the injury is of the kind that can reasonably and objectively be predicted to result from the ESS designer's act or omission.

In concrete terms, the ESS designers' liability is determined based on whether they knew or should have known the risk associated with choosing, for example, one ESS-specific design metric over another. The ESS designer is expected to investigate and learn if a certain type of product, system, or application is inadequate for the types of risks associated with the project environment.

Only when the injury was reasonably foreseeable is the ESS designer found liable for breach of the duty of care to a third party. The standard of reasonable conduct for the ESS designer is determined on a case-by-case basis by juries.

The assessment of whether the duty has been breached includes, but is not limited to, the following factors:

- Reasonable efforts to ascertain the physical and operational environment of the ESS design so that it can be determined whether the design would be appropriate
- Contact with architects, engineers, general contractors, other trades, information technology (IT) department, facilities department, or other entities relating to a particular location or design
- Internal procedures for determining ESS design
- Response to negative information regarding the feasibility of the design

With appropriate risk management techniques, an ESS designer may successfully avoid liability to third parties by minimizing the foreseeable risks and the class of persons to whom the duty is owed.

Assuming that a likelihood or possibility of breach exists, the injury suffered by the third party must have been caused or most likely have been caused by the ESS designer's breach. Therefore, the injured third party is required to show that it is more probable than not that the ESS designer's act or omission caused the claimed injury.

Legal Issues, continued

Having established liability, the third party must go further to demonstrate damage. The third party must also show that loss was suffered as a result of the breach. The recoverable damages can include:

- Loss of earnings.
- Loss of future earning capacity.
- Past medical expenses.
- Future medical expenses.
- Pain and suffering.
- Disfigurement.
- Permanent or temporary physical impairment.

These are classic damages in tort theory. In the context of ESS design, it appears that the courts would be challenged by quantifying the damages resulting from the loss of information.

Limiting Legal Costs

Alternative Dispute Resolution

Litigation is expensive in terms of both the legal costs and the time spent away from business to attend court, meet with the lawyers, or collate evidence. Therefore, it is often beneficial to include alternative and less expensive methods of dealing with disputes when drafting contracts.

These alternative methods are referred to under the general heading of alternative dispute resolution (ADR). The two most common forms of ADR are:

- Mediation.
- Arbitration.

The effectiveness and benefits of these processes have been the subject of reviews sponsored by the American Arbitration Association (AAA).

The global cost of civil litigation is soaring, and businesses of all sizes are opting for a wider palette of strategic dispute resolution strategies, according to a new study sponsored by the AAA. This empirical study on ADR, entitled "Dispute-Wise℠ Business Management: Improving Economic and Non-Economic Outcomes in Managing Business Conflicts," investigates the practices, attitudes, and experiences of a broad sampling of corporate legal departments from *Fortune* 1000 companies, midsize public companies, and privately held businesses in their use of nonjudicial dispute resolution.

This pioneering study on the relationship between ADR and positive corporate outcomes shows that a company may enjoy greater benefits by taking a strategic, multifaceted approach to managing the body of existing and future disputes rather than by aggressively litigating each case. It also demonstrates that companies that take this approach can effectively maximize the output of their legal staff while minimizing their legal department costs.

 © 2012 BICSI®

Limiting Legal Costs, continued

The following are some of the study findings:

- The study identified an index of eight particular traits that characterized the legal departments of dispute-savvy companies. The survey also found that a number of specific operational benefits are associated with dispute-wise business management practices for these companies. It appears a company may glean benefits (e.g., better customer and business partner relationships, lower costs, more positive employee relations) by managing effectively over time the total economic and noneconomic impact of its entire range or portfolio of issues and disputes. In addition, the survey noted interesting correlations between dispute-wise business management practices and positive economic advantages.
- "Legal departments that take a portfolio approach to resolving disputes (e.g., measuring them against each other with the goal of minimizing overall risk, cost, time spent, and resources expended) appear to garner several distinct benefits," said Richard Naimark, Senior Vice President of the AAA. "Moreover, it is clear that dispute-savvy companies monitor their key business relationships and approach dispute resolution with that strategic focus in mind" (Dispute-Wise^{SM}).

Mediation

Mediation is a nonbinding, facilitated, negotiation process. Its aim is to produce voluntary and acceptable settlement agreements between or among the parties that are involved in a dispute. Although the process starts out as nonbinding, once an agreement is reached and duly signed by the parties, it becomes binding.

A mediator is a person who is trained in dispute resolution, including negotiation techniques, and is familiar with the art of making a deal. Mediators are neutral and do not offer legal advice although they are actively engaged in the discussion process, including narrowing down the issues, offering alternatives, and directing the parties toward a settlement of the dispute.

Mediation is less expensive, in part, because preparing for the mediation, including the mediator's fees, costs less than the regular court process (e.g., filing of pleadings, disclosure of documents, attendance for depositions). Mediation offers more flexibility insofar as it is not restricted or bound by the rules of law or legal precedents. Making agreements is thus broader and less laden by the rules.

Arbitration

Arbitration is more rule-laden than mediation. In arbitration, the arbitrator is required to apply the law relating to the particular subject matter. Although having one arbitrator is not unusual, it is more common to have a panel of three arbitrators. At least one arbitrator is a lawyer, whereas the others may be drawn from among the persons familiar with the dispute's subject matter.

Limiting Legal Costs, continued

The arbitrators hear evidence in the same way as in a court of law. However, the rules of evidence are more relaxed. In addition, discovery is not as rigorous as pretrial discovery, and the more formal requirements of a trial (e.g., preparation of briefs or closing arguments) are not necessary.

To take the full advantage of ADR, it is recommended that it be included in the contract. In some state jurisdictions, apart from court proceedings, mediation is by agreement and arbitration is always by agreement.

The initial agreement makes arbitration mandatory between the parties. In the construction industry, a standard AAA clause is used.

Generating standard form AAA clauses for use by ESS designers would be useful. Merely stipulating arbitration without specific details is inadequate for giving a full effect to the intentions. The intentions may be subject to differing rules of interpretation, and therefore the process must be specified. Clauses must stipulate:

- The number of arbitrators.
- How the arbitrators would be chosen.
- Whether the decision of the arbitrators would be unanimous or by majority.

Limiting the Electronic Safety and Security (ESS) Designer's Liability

ESS designers can benefit from some of the lessons already learned by the building construction industry. Some of these liability avoidance techniques are summarized in this section.

The erosion of the doctrine of privity suggests that ESS designers have to be perceptive about the contractual arrangements or their relationship with the clients and the contractors. The construction industry has minimized this exposure by changing the manner of interaction with the builders/clients. Such interaction was achieved by first changing the relationship from a supervisory role to an inspection role. Second, the inspection role was reduced to the role of observing the work for limited purposes of:

- Ascertaining if the work was professional.
- Assessing if the work generally conformed to the contract requirements.
- Advising the client whether to pay for the work.

The single most important precautionary measure is to avoid oral agreements. Given the nature of the ESS designer's job, all contracts and amendments should be in writing.

In addition, risks can be more carefully allocated when they are fully recognized at the outset. Independent legal advice is recommended to ensure that ESS designers do not sign one-sided contracts prepared by the contractors or the clients' attorneys or contracts laden with terms that have serious implications, particularly as related to risk allocation.

 © 2012 BICSI®

Limiting the Electronic Safety and Security (ESS) Designer's Liability, continued

Fairness is a requirement on both sides so that inasmuch as unfair contractual terms should not be signed by one contract party, unfair contractual terms should not be imposed on the other contract party. Courts look with disfavor on unfair contractual terms.

An unfair contract can be as bad as having no contract at all. It is also advisable to insert provisions for early termination of the contract and for a reasonable limitation of damages consequent on early termination.

The scope of the services to be provided should be clearly defined and closely regarded. Any variation from the original terms must be put in written form after a careful analysis of the risks and costs involved or associated with the change. Warranties, indemnities, and guarantees should be avoided.

Limitations of liability are another method that can be used to allocate the risks associated with a particular project. One of the most common expressions of a limitation of liability clause is when the client and the ESS designer agree to limit the ESS designer's risk to the sum of the professional fees.

With the evolution of high-availability IT sites like data centers, the potential value of lost uptime because of consulting, design, and installation of ESS systems has increased. If a critical error is traced back to the ESS designer, the amount of the claim can be substantial. This is yet another reason to continue being educated on the legal issues arising from ESS projects.



Glossary

This glossary provides concise and current terminology that reflects the electronic safety and security (ESS) industry worldwide. It includes specific definitions from standards bodies, where appropriate, in an effort to harmonize terms within the industry.

Table of Contents

Glossary Terms **Gls-1**

Acronyms and Abbreviations **Gls-37**

Glossary Terms

A

A-weighted decibel (dBA) — An expression of the relative loudness of sounds in the air as perceived by the human ear. In the A-weighted system, the decibel values of sounds at low frequencies are reduced, compared with unweighted decibels, in which no correction is made for audio frequency. This correction is made because the human ear is less sensitive at low audio frequencies, especially below 1000 hertz (Hz) than at high audio frequencies. See also decibel, A-weighted (dBA).

above finished floor (AFF) — Standard mounting height or vertical distance (e.g., 1220 mm [48 in] AFF) for a fixture, ceiling, device, or any other object measured from the finished floor surface to the center line of the object as the measurement point.

access control — Restriction of who can interact with a resource. The resource can be restricted to individuals and assets such as an individual device (e.g., door), a building, a group of buildings, or IP-based information. The possession of access control is essential when securing important, confidential, or sensitive information and equipment.

access control card — An identification card with encoded information that, when presented to a card reader, identifies the cardholder to the access control systems (ACS), allowing the systems to determine the cardholder's entrance and exit rights.

access controller — See data gathering panel.

access control systems (ACS) — An interconnected set of controllers managing the entrance and exit of people through secure areas.

access group — A superset of information, including time zones and secured doors, that is applied toward cardholders. This information defines at what time of day and through which doors cardholders are granted access.

access level matrix — An access control systems (ACS) reference that is specific to each system for which it is being utilized. The purpose of the document is to provide a hierarchy of rights and privileges for different user groups and their associated authorized zones.

access parameter — The programmed information that defines the conditions that must be met to grant access to a secure area.

access point (AP) — The point of entry into a secure area.

acknowledgment (ACK) — A frame used in IEEE 802.11 to confirm that an error-free, data-free, frame has been received.

active card — A type of access card that is dependent upon a card reader to provide the power necessary to allow the card to transmit its data.

active multiplex system — A multiplexing system in which signaling devices (e.g., transponders) are employed to transmit status signals of each initiating device or initiating device circuit within a prescribed time interval. The lack of receipt of such a signal can be interpreted as a trouble signal.

addressable device — A fire alarm system component with discrete identification that can have its status individually identified or that is used to individually control other functions.

adverse condition — Any condition occurring in a telecommunications channel that interferes with the proper transmission or interpretation of status change signals at the supervising station.

agile reader — A reader that can read tags operating at different frequencies or using different methods of communication between the tags and readers.

air sampling-type detector — An early warning smoke detector that consists of a piping or tubing distribution network that runs from the detector to the area(s) to be protected.

alarm service — The service required following the receipt of an alarm signal.

alarm signal — Any signal resulting from the activation of an alarm event (e.g., fire alarm). An alarm signal usually results in automatic activation of visible or audible notification or signaling appliances. The purpose of an alarm signal is to indicate that immediate action is needed.

alarm system — A combination of compatible initiating devices, control panels, and indicating appliances designed and installed to produce an alarm signal in the event of fire.

alarm verification — A feature of automatic fire detection and alarm systems to reduce unwanted feature alarms wherein smoke detectors report alarm conditions for a minimum period of time, or confirm alarm conditions within a given time period after being reset, in order to be accepted as a valid alarm initiation signal.

alert tone — An attention-getting signal to alert occupants of the pending transmission of a voice message.

ambient intelligence — The presence of a digital environment that is sensitive, adaptive, and responsive to the presence of people. Ambient intelligence improves the efficiency and quality of life by creating the desired atmosphere and functionality via intelligent, personalized interconnected systems and services.

 © 2012 BICSI®

ambient sound level — The level of acoustic noise existing at a given location (e.g., room or area). Commonly expressed as background noise, ambient sound level is an objective measurement of audible sound levels in an arbitrary location under ambient conditions. The measurement is usually expressed in decibels (dB). The ambient noise level may be measured with a sound level meter and is defined as the root mean square, A-weighted, sound pressure level measured over the period of time that any person is present or a 24-hour period, whichever time period is the lesser. See also A-weighted decibel.

American National Standards Institute (ANSI) cutout — A standard or stock cutout furnished on doors and frames from the door or frame manufacturer.

Americans with Disabilities Act (ADA) — A United States federal law enacted in 1990 that guarantees equal civil rights for people with disabilities. ADA requires that alarm notification appliances used in the public mode make equivalent facilitation for people with disabilities, most often hearing impairments. This requirement often results in the use of visual signaling in combination with audible signaling.

Americans with Disabilities Act Accessibility Guidelines (ADAAG) — A set of guidelines that defines the specific methods for compliance with ADA when undertaking construction or alteration of places of public accommodation and commercial facilities in the United States of America. The first guidelines were formally published in 1991 on the first anniversary of the enactment of ADA.

analog initiating device (sensor) — An initiating device that transmits a signal indicating varying degrees of condition as contrasted with a conventional initiating device, which can only indicate an on-off condition.

annunciator — A unit containing one or more indicator lamps, alphanumeric displays, or other equivalent means in which each indication provides status information about a circuit, condition, or location.

antipassback — A method for providing one card one-way access into and out of a secure area. It prevents someone from using a card to enter a secure area and then passing that card back to another to enter that same area.

approved — Acceptable to the authority having jurisdiction (AHJ).

Architectural and Barriers Compliance Board (Access Board) — A federal agency charged with the responsibility of developing minimum guidelines and requirements standards issued under the Americans with Disabilities Act (ADA) and the Architectural Barriers Act. Established as part of the Rehabilitation Act of 1973. The Access Board is charged with ongoing development and publication of ADA Accessibility Guidelines.

asset	Anything tangible or intangible that has value.
astragal	A piece of material attached across the length of a door on the latch edge.
audible notification appliance	A notification appliance (e.g., bell, horn, speaker) that alerts by the sense of hearing.
audible signal	A sound made by one or more audible notification appliances (e.g., bells, horns, speakers) in response to the operation of any manual or automatic electronic device.
audit trail	A sequential record that accounts for all the activities of the access control systems (ACS). This record allows for the analysis of events over a given time period.
authority having jurisdiction (AHJ)	The entities (e.g., organization, office, individual) responsible for interpretation and enforcement of local building and electrical codes. This may include approving equipment, materials, an installation, or a procedure.
authorization level	A security rating that must be met before access to a secure area can be granted.
authorized passage device (authorized egress device)	A device that when activated, allows authorized persons to enter or exit monitored and controlled openings without triggering an alarm. Examples of authorized passage devices include keyed switch, card-reader, or digital code reader.
authorized service provider (ASP)	A third party cleared to work on a product still under warranty by another company without voiding the warranty.
automatic extinguishing system supervisory device	A device that responds to abnormal conditions that could affect the proper operation of an automatic sprinkler system or other fire extinguishing system(s) or suppression system(s), including, but not limited to, control valves; pressure levels; liquid agent levels and temperatures; pump power and running; engine temperature and overspeed; and room temperature.
automatic fire detector	A device designed to detect the presence of a fire signature and to initiate action. Examples include automatic fire detectors that are classified as automatic fire extinguishing or suppression system operation detector, fire-gas detector, heat detector, radiant energy-sensing fire detector, and smoke detector.
automatic fire extinguishing	A device that automatically detects the operation of a fire extinguishing or suppression system by means appropriate to the system employed.
auxiliary box	A fire alarm box that can be operated from one or more remote actuating devices.

 © 2012 BICSI®

auxiliary fire alarm system — A system connected to a municipal fire alarm system for transmitting an alarm of fire to the public fire service communications center. Fire alarms from an auxiliary fire alarm system are received at the public fire service communications center on the same equipment and by the same methods as alarms transmitted manually from municipal fire alarm boxes located on streets.

auxiliary fire alarm system, local energy type — An auxiliary system that employs a locally complete arrangement of parts, initiating devices, relays, power supply, and associated components to automatically trip a municipal transmitter or master box over electrical circuits that are electrically isolated from the municipal system circuits.

auxiliary fire alarm system, parallel telephone type — An auxiliary system connected by a municipally controlled individual circuit to the protected property to interconnect the initiating devices at the protected premises and the municipal fire alarm switchboard.

auxiliary fire alarm shunt auxiliary type — An auxiliary system electrically connected to an integral part of the system, municipal alarm system extending the municipal circuit into the protected premises to interconnect the initiating devices, which, when operated, open the municipal circuit shunted around the trip coil of the municipal transmitter or master box. The municipal transmitter or master box is then energized to start transmission without any assistance from a local source of power.

average ambient sound level — The root mean square, A-weighted, sound pressure level measured over a 24-hour period. See also A-weighted decibel and ambient sound level.

B

badge reader — See card reader.

badging software — Security software that is capable of creating a photo identification badge.

bar code card — An access control card with identification information encoded in the bar code format.

barrier — A partition, divider, or other separation that provides complete separation from adjacent compartments.

battery backup — A secondary energy source used to power devices in the event the primary energy source fails.

bell, vibrating — A bell that rings continuously as long as operating power is applied.

biased door contacts — A high-security door contact that uses a biasing magnet mounted inside the read switch part of the door contact package.

biometrics — An automated method of recognizing a person based on physiological or behavioral characteristics.

bolt position switch — A miniature switch used on or in a locking device to monitor whether the locking bolt is in the locked (projected) or unlocked (retracted) position.

box battery — A battery supplying power for an individual fire alarm box where radio signals are used for the transmission of box alarms.

breakglass box — A box with a special element that requires breaking in order to operate.

building automation and control network (BACnet®) — Developed under the auspices of the American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc. (ASHRAE), published as ANSI ASHRAE standard 135-2004, BACnet® is an industry standard protocol for building automation and control networks. BACnet defines a four-layer architecture that includes the Physical, Data Link, Network, and Application layers of the Open Systems Interconnection (OSI) Reference Model (ISO 7498).

by-wire (or x-by-wire) — A term used to describe control systems that depend on a real-time telecommunications network to connect different electronic components. Historically, these control systems relied on mechanical or hydraulic linkages, and the goal of by-wire is to replace nearly every automotive hydraulic/mechanical system with electronics. (ABI Research).

C

campus — The buildings and grounds having legal contiguous interconnection. (TIA)

candela (cd) — The International System of Units metric measure for the luminous intensity, or light output of a light or strobe.

card access — The access control systems (ACS) using encoded cards and card readers to identify card readers and determine whether access may be granted.

card encoder — A device used to encode data onto an access card.

card reader — A device that retrieves information stored on an access card or badge and transmits the information to a controller. Also called badge reader.

cardholder — An individual who has been assigned an access control card.

carrier — A transmitted signal modulated by an information source (e.g., voice or signaling impulses) on which information can be imposed by increasing the signal strength, varying the base frequency, varying the wave phase, or by other means.

carrier system — A means of conveying a number of channels over a single path by modulating each channel on a different carrier frequency and demodulating at the receiving point to restore the signals to their original form.

 © 2012 BICSI®

ceiling	The upper surface of a space, regardless of height. Areas with a suspended ceiling have two ceilings, one visible from the floor and one above the suspended ceiling.
ceiling height	The height from the continuous floor of a room to the continuous ceiling of a room or space.
ceiling surfaces, beam construction	Ceilings that have solid structural or solid nonstructural members projecting down from the ceiling surface more than 100 mm (3.94 in) and spaced more than 1 m (3.28 ft), center to center.
ceiling surfaces, girder	A support for beams or joists that runs at right angles to the beams or joists. If the top of the girder is within 100 mm (3.94 in) of the ceiling, the girder is a factor in determining the number of detectors and is to be considered a beam. If the top of the girder is more than 100 mm (3.94 in) from the ceiling, the girder is not a factor in detector location.
ceiling surfaces, solid	Ceilings that have solid structural or solid nonstructural members projecting joist construction down from the ceiling surface for a distance of more than 100 mm (3.94 in) and spaced at intervals of 1 m (3.28 ft) or less, center to center.
CE mark	A Conformité Européene mark fixed to the product itself or its packaging, instructions for use, or guarantee certificate. It indicates that the product complies with all relevant European directives that call for its application (e.g., electromagnetic compatibility directive).
cementitious	Material that, when mixed with water, looks like lightweight concrete or mortar, and can be troweled to a smooth finish.
central station	A location that remotely monitors activities that occur at a protected facility. Central stations are frequently identified as a proprietary or nonproprietary contract.
central station service	The use of a system or group of systems in which the operations of circuits and devices at a protected property are signaled to, recorded in, and supervised from a listed central station that has competent and experienced operators who, upon receipt of a signal, take such action as required by codes, standards and regulations (e.g., *NFPA 72®*). Central station service is controlled and operated by a person, firm, or corporation whose business is the furnishing of such contracted services or whose properties are the protected premises.
certification	A systematic program that uses randomly selected follow-up inspections of the certified systems installed under the program that allows the listing organization to verify that a fire alarm system complies with all the requirements of this code. A system installed under such a program is identified by the issuance of a certificate and is designated as a certificated system.

certification of personnel A formal program of related instruction and testing as provided by a recognized organization or the authority having jurisdiction (AHJ).

channel **1.** The end-to-end transmission path connecting interfaces of any two pieces of application-specific equipment. Equipment cords and work area cords are included in the channel. **2.** In frequency division multiplexing (FDM), a band in the frequency spectrum that is assigned to a specific logical connection. **3.** In time division multiplexing (TDM), a time that is assigned to a specific logical connection.

cipher lock A mechanical combination lock that is used in access control to unlock a knob or level or to actuate a set of contacts.

circuit interface A component that interfaces initiating devices or control circuits, or both; notification appliances or circuits, or both; system control outputs; and other signaling line circuits to a signaling line circuit.

closed loop secure A closed or continuous circuit or monitoring loop when a door or monitoring equipment is secure.

cloud chamber smoke detection A principle of using an air sample drawn from the protected area into a high-humidity chamber combined with a lowering of chamber pressure to create an environment in which the resultant moisture in the air condenses on any smoke particles present, forming a cloud. The cloud density is measured by a photoelectric principle. The density signal is processed and used to convey an alarm condition when it meets preset criteria.

code A rule intended to ensure safety during the installation and use of materials, components, fixtures, systems, premises, and related subjects. Codes are typically invoked and enforced through government regulation.

coded An audible or visible signal that conveys several discrete bits or units of information. Notification signal examples are numbered strokes of an impact-type appliance and numbered flashes of a visible appliance.

coded signals An audible or visual signal conveying discrete information by establishing a pattern of pulses or flashes. Coded notification signals might be numbered strokes of an impact-type appliance or numbered flashes of a visual appliance. Coded signals are often used to convey information about the specific location of a fire alarm event.

combination detector A device that either responds to more than one fire phenomenon or employs more than one operating principle to sense one of these phenomenon. Typical examples are a combination of a heat detector with a smoke detector or a combination of rate-of-rise and fixed-temperature heat detector.

combination fire alarm A manually operated box for separately transmitting a fire alarm signal and a guard's tour box distinctive guard patrol tour supervisory signal.

 © 2012 BICSI®

combination system	A fire alarm system in which components are used, in whole or in part, in common with a nonfire signaling system.
commissioning	The start-up of a safety and security system that includes testing and adjusting the systems to assure proper functioning and adherence to design criteria. Commissioning also includes the instruction of building representatives in the use of building systems.
communications channel	A circuit or path connecting a subsidiary station to a supervising station over which signals are carried.
compatibility listed	A specific listing process that applies only to two-wire devices (e.g., smoke detectors) that are designed to operate with certain control equipment.
compatible equipment	Equipment that interfaces mechanically or electrically as manufactured without field modification.
consultant	A specialist who provides services to the design team that is headed up by an architect or engineer who is under contract with the client.
contact	A conducting circuit that makes or breaks a circuit.
contact rating	The specifications or load rating of a switch. Ratings are at maximum voltage or current.
contiguous property	A single-owner or single-user protected premises on a continuous plot of ground, including any buildings thereon, that is not separated by a public thoroughfare, transportation right-of-way, property owned or used by others, or body of water not under the same ownership.
continuous duty	A device that can operate continuously with no off or rest periods.
control unit	A system component that monitors inputs and controls outputs through various types of circuits.
controller	A microprocessor-based circuit board that manages access to a secure area. The controller receives information that is used to determine through which doors and at what time cardholders are granted access to secure areas. Based on that information, the controller locks/unlocks doors, sounds alarms, and communicates its status to a host computer.
credential	An item or object that possession or knowledge of provides access to a secure space.
cross-point matrix	This system takes in a number of closed-circuit TV (CCTV) camera signals and then switches these cameras to outputs for viewing and recording. Typically, the number of inputs is higher than the quantity of outputs.

D

data gathering panel — A component of access control systems (ACS) whose primary function is to consolidate field-mounted peripheral devices and communicate bidirectionally between the system's headend software and field-mounted peripheral devices. Also referred to as access controller or intelligent field panel.

deadbolt — A bolt operated manually and nonactuated by springs. When locked, the bolt cannot be forced back. A deadbolt is operated (projected and retracted) by a key cylinder or lever handle.

dead latch — A latch in which the latch bolt is positively held in the projected position by an auxiliary mechanism.

decibel (dB) — A logarithmic unit for measuring the relative voltage, power (in watts) or strength (in voltage or current) of a signal. A decibel (db) is one tenth of a bel.

decibel, A-weighted (dBA) — A decibel measurement based on a frequency scale that closely approximates human hearing. Measurements expressed in dBA are useful because dB measurements can differ depending on output frequency (or pitch). Most sound level requirements in fire codes and standards are expressed in dBA units. See also A-weighted decibel.

delay on break — A term used to describe a mode of operation relative to timing devices. The delay begins when the initiate switch is opened (delay on break of initiate switch).

delay on energization — A term used to describe when the initiate switch is closed for application of power to the input.

delayed egress — A delayed egress device allows a 15 second delay in opening a door required by building code to be equipped with panic or fire exit hardware.

delinquency signal — A signal indicating the need for action in connection with the supervision of guards or system attendants.

derived channel — A signaling line circuit that uses the local leg of the public switched network (PSN) as an active multiplex channel while simultaneously allowing that leg's use for normal telephone communications.

detector — A device suitable for connection to a circuit that has a sensor that responds to a physical stimulus (e.g., heat, smoke).

digital alarm communicator receiver (DACR) — A component that receives signals from a digital alarm communicator transmitter. These signals contain information pertaining to the condition of the alarm system.

 © 2012 BICSI®

digital alarm communicator system (DACS) (dialer)	A system in which signals are transmitted from a digital alarm communicator transmitter (DACT) located at the protected premises through the public switched telephone network (PSTN) to a digital alarm communicator receiver so that it may seize the line to which it is connected. The seizure disconnects any private telephone equipment beyond the DACT's point of connection.
digital alarm communicator transmitter (DACT)	A component that transmits signals to a digital alarm communicator receiver. These signals contain information pertaining to the condition of the alarm system.
digital alarm radio receiver (DARR)	A system component composed of two subcomponents—one that receives and decodes radio signals and another that annunciates the decoded data. These two subcomponents can co-reside at the central station or be separated by means of a data transmission channel.
digital alarm radio system (DARS)	A system in which signals are transmitted from a digital alarm radio transmitter located at a protected premises through a radio channel to a digital alarm radio receiver.
digital alarm radio transmitter (DART)	A system component that is connected to or an integral part of a digital alarm communicator transmitter that is used to provide an alternate radio transmission channel.
Dijkstra's algorithm	This algorithm uses a combination of metric, protocol cost, and available bandwidth as part of its determination process. Routers then share this information with other neighboring routers using link state advertisements.
direct hold magnetic lock	An electric magnet is mounted to a doorframe opposite a metal plate. When energized, the lock bonds to the armature and locks the door.
display	A visual representation of output data, other than printed copy.
distributed access control	The access control systems (ACS) in which all control decisions are made at the local controllers, independent from a host computer. Local controller events are uploaded to a host computer periodically for review and storage.
door contact	A recessed or surface-mounted peripheral device that provides the access control systems (ACS) with an input that reports the status of a door or passageway that is being monitored.
door-forced alarm	An alarm generated when a door is forced open.
door held open alarm	An alarm generated when a door is held open beyond the designated period of time as programmed in the controller.
door position switch	A switch that is used to monitor whether a door is in an opened or closed position.

door switch A switch that reflects the status of the door—open or closed.

double doorway A single opening that has no intervening wall space or door trim separating the two doors.

double dwelling unit A building consisting solely of two dwelling units.

download To send information from a host computer to a controller.

dry contact A switch or relay contact that is not connected to other voltage sources.

dual control The use of two primary trunk facilities over separate routes or different methods to control one telecommunications channel.

duty cycle The percentage of "on" time or operating time a device experiences.

dwelling unit One or more rooms for the permanent use of one or more persons for eating, living, and sleeping with provisions for cooking and sanitation. A dwelling unit includes one- and two-family attached and detached dwellings, apartments, and condominiums but does not include hotel and motel rooms and guest suites, dormitories, or sleeping rooms in nursing homes.

E

egress A point of exit from a building or property.

elastomeric A characteristic of a material or substance allowing stretching and flexibility, resembling rubber or elastic.

electrical conductivity heat detector A line-type or spot-type sensing element in which resistance varies as a function of temperature.

electric latch retraction Allows doors equipped with exit devices to be operated in push-pull (dogged) mode by electrically retracting the latch bolts.

electric lockset An electrified version of a standard lockset that generally comes in two basic configurations. Available products incorporate an actuating solenoid that locks or unlocks a lockset, duplicating or replacing the function of a traditional mechanical key.

electric strike An electrified locking element that replaces a traditional door's fixed strike with an electromechanical unit that upon application (fail-secure) or removal (fail-safe) of power, a solenoid electrically activates the keeper, allowing a lock's latch bolt to pass.

electrified door release hardware A generic term for electromechanical locking hardware that is released upon an approval signal.

 © 2012 BICSI®

electromagnetic lock	An electric lock that uses an electromagnet to hold a door closed.
ember	A particle of solid material that emits radiant energy due to either its temperature or the process of combustion on its surface.
emergency voice alarm communications	An audible alarm method that uses spoken messages to alert occupants. Voice communication alarms can be used to convey specific instructions to occupants during an alarm event. Voice communication systems typically use automatic recorded messages but also provide manual override and paging capability.
encoding	The process of writing data to a card.
end-of-line device	A device used to terminate a supervised circuit.
Epilepsy Foundation of America (EFA)	An association that has had an impact on the sensitivity of photosensitive strobes and epilepsy, especially with regard to synchronization.
equivalent facilitation	The concept of making any object equally accessible or usable to persons with physical disabilities. In building and construction, equivalent facilitation is usually achieved with special accessibility features (e.g., ramps, powered door operators, visual alarm appliances).
evacuation	The withdrawal of occupants from a building.
evacuation signal	A distinctive signal intended to be recognized by the occupants as requiring evacuation of the building.
event	An occurrence at a controller (e.g., locking/unlocking a door, requesting to exit, forcing a door open) that generates a message stored in the controller.
event-based monitoring	The modern electronic safety and security (ESS) system can leverage an important principle—event-based monitoring. This principle is based on the fact that electronic systems can efficiently and effectively drive operational response (the inverse of this is operational personnel monitoring systems for trouble conditions). Event-based monitoring solutions imply a high level of integration between systems such that events from one subsystem automatically drive actions from other systems.
exit plan	A plan for the emergency evacuation of the premises.
extensible markup language (XML)	A specification developed by the World Wide Web Consortium (W3C). XML is a pared-down version of standard generalized markup language, designed especially for web documents. It allows designers to create their own customized tags, enabling the definition, transmission, validation, and interpretation of data between applications and between organizations. XML has been widely adopted for use in the integration of computing systems with automation and control systems as the underlying language behind XML web services.

F

facility code — The coded data in access control cards that identifies the location of the access control systems (ACS).

fail latched — Provides a locking device that on loss of power will latch or remain latched but does not necessarily restrict movement from the secured side.

fail locked — An electric lock that requires power to unlock. Also called fail-secure.

fail-safe door — When the power fails at that door, the door automatically unlocks, allowing exit and entrance. See also fail unlocked.

fail-safe lock — A lock that automatically unlocks a door upon loss of power. It takes power to lock a device of this type. A fail-safe lock is used for life safety applications. Also called power lock.

fail-secure door — When the power fails at a door, the door automatically locks and will not allow entrance but will continue to allow exit.

fail-secure lock — A device that automatically locks a door upon loss of power. It takes power to unlock this type of device. Also called power unlock.

fail unlocked — An electric lock that automatically unlocks with any power interruption. Also called fail-safe. See also fail-safe door.

fault — An open, ground, or short condition on any line extending from a control unit, which could prevent normal operation.

field of view — A solid cone that extends out from the detector within which the effective sensitivity of the detector is at least 50 percent of its on-axis, listed, or approved sensitivity.

fingerprint reader — A biometric reader that identifies a person based on the person's fingerprint pattern.

fire alarm code — A code that specifies when a fire alarm system is required.

fire alarm control panel (FACP) unit — A system component that receives inputs from automatic and manual fire alarm devices and might supply power to detection devices and to transponders or off-premises transmitters. The control unit might also provide transfer of power to the notification appliances and transfer of condition to relays or devices connected to the control unit. The fire alarm control unit can be a local fire alarm control unit or a master control unit. This unit may incorporate a digital alarm communication transmitter to transmit signals to a digital alarm communicator receiver.

fire alarm/evacuation signal tone generator — A device that produces a fire alarm/evacuation tone upon command.

 © 2012 BICSI®

fire alarm signal	A signal initiated by a fire alarm-initiating device (e.g., manual fire alarm box, automatic fire detector, water flow switch) in which activation is indicative of the presence of a fire or fire signature.
fire alarm standard	A standard that prescribes such requirements as the spacing and placing requirements of fire detection and alarm equipment. This addresses how a fire alarm system is to be installed, tested, inspected, maintained, and monitored.
fire alarm system	A system or portion of a combination system that consists of components and circuits arranged to monitor and annunciate the status of fire alarm or supervisory signal-initiating devices and to initiate the appropriate response to those signals.
fire command center	A principal attended or unattended location where the status of the detection, alarm communications, and control systems is displayed and from which the systems can be manually controlled.
fire-gas detector	A device that detects gases produced by a fire.
fireproof	A property of a material (e.g., masonry, block, brick, concrete, gypsum board) that does not support combustion even under accelerated conditions. No material is entirely fireproof.
fire resistance rating	The time in hours, or fraction thereof, that a material or assembly of materials will withstand the passage of flame and the transmission of heat when exposed to fire under specified conditions of test and performance criteria. (TIA)
fire safety function control device	A fire alarm system component that directly interfaces with the control system that controls the fire safety function.
fire safety functions	The building and fire control functions that are intended to increase the level of life safety for occupants or to control the spread of the harmful effects of fire.
firestop	Fire-rated materials, devices, or assembly of installed parts that are listed for the purpose of filling openings around penetrating items (e.g., cables, cable trays, conduits, ducts, pipes, support structures) to prevent the spread of fire, temperature, and gases of combustion.
fire supervisory control unit	See intermediate fire alarm.
fire warden	A building staff member or tenant trained to perform assigned duties in the event of a fire emergency.

fixed-temperature detector — A device that responds when its operating element becomes heated to a predetermined level.

flame — A body or stream of gaseous material involved in the combustion process and emitting radiant energy at specific wavelength bands determined by the combustion chemistry of the fuel. In most cases, some portion of the emitted radiant energy is visible to the human eye.

flame detector — A radiant energy-sensing fire detector that detects the radiant energy emitted by a flame.

flame detector sensitivity — The distance along the optical axis of the detector at which it can detect a fire of specified size and fuel within a given time frame.

flow switch — Monitors minor surges in water flow.

G

gateway — **1.** An internetworking service used to connect dissimilar applications running on different networks with different telecommunications protocols. Gateways normally operate at one or more of the top four layers of the Open Systems Interconnection (OSI) Reference Model. **2.** As it relates specifically to fire alarm control units, a gateway is a device that is used in the transmission of serial data (digital or analog) from the fire alarm control unit to other building system control units, equipment, or networks and/or from other building system control units to the fire alarm control unit.

general alarm — An alarm signal that is not specific to an individual device or area. General alarms are signaled throughout an entire building or area and typically result in the evacuation of occupants.

global unlock — An input that, when activated, generates a signal that unlocks doors in the access control systems (ACS).

gray scale — An image in which the value of each pixel is a single sample or a pattern of dots that is used to represent a particular shade. Displayed images of this sort are typically composed of shades of gray, varying from black at the weakest intensity to white at the strongest.

ground fault — An undesirable connection to ground in which the resistance between a conductor and ground reaches an unacceptably low level.

GS mark — A symbol of safety recognized throughout Germany and European Union countries. Any electrical, mechanical, or electromechanical product bearing the GS mark indicates that it was tested and complies with the minimum requirements of the German Equipment and Product Safety Act.

 © 2012 BICSI®

guard's tour reporting station — A device that is manually or automatically initiated to indicate the route being followed and the timing of a guard's tour.

guard's tour supervisory signal — A supervisory signal monitoring the performance of guard patrols.

H

halftone — See gray scale.

hand geometry — A biometric reader that verifies a person's identity using the variations in hand size, finger length, and finger thickness.

heat alarm — A single or multiple station alarm responsive to heat.

heat detector — A fire detector that detects either abnormally high temperature or rate of temperature rise, or both.

horn — An audible signal in which energy produces a sound by imparting motion to a flexible component that vibrates at some nominal frequency.

host computer — The central controlling computer on which access control software runs.

household fire alarm system — A system of devices that produces an alarm signal in the household for the purpose of notifying the occupants of the presence of a fire.

hunt group — A group of associated telephone lines within which an incoming call is automatically routed to an idle (not busy) telephone line for completion.

I

incipient — The early or beginning stage of a fire. The first of four stages (incipient, visible smoke, flame, and heat). Combustion particulates in the incipient stage are low in density and lower than the level of detection capabilities of conventional smoke detectors.

independent — Denotes that a device communicates with its associated control system through a wireless connection.

initiating device — A system component that originates the transmission of a change-of-state condition (e.g., in a smoke detector, manual fire alarm box, supervisory switch).

initiating device circuit (IDC) — A circuit to which automatic or manual initiating devices are connected where the signal received does not identify the individual device operated.

inrush (amperes) The current that a device requires during its initial power-up.

insertion card A card that must be inserted into a card reader for the reader to retrieve the information stored on the card.

integrated project delivery (IPD) A collaborative alliance of people, systems, business structures, and practices into a process that harnesses the talents and insights of all participants to optimize project results, increase value to the owner, reduce waste, and maximize efficiency through all phases of design, fabrication, and construction.

intelligent field panel See data gathering panel.

intelligibility For voice communications, the capability of being understood by the intended audience. Intelligibility does not imply the recognition of a particular voice. It cannot be measured with instrumentation but may be electronically simulated and measured utilizing an indexing method.

interior An area not directly connected to the perimeter walls of a building. These areas tend to require specific sensors because the protection is usually for both spaces and objects within the spaces.

interlock A system of multiple doors that control interaction. No door can be unlocked unless all other doors are secure and locked. Also known as light trap, air trap, mantrap, and sally port.

intermediate fire alarm unit A control unit used to provide area fire alarm or area fire supervisory service that, where connected to the proprietary fire alarm system, becomes a part of that system.

intermittent duty solenoid A current-carrying coil of wire that acts like a magnet when a current passes through it that is designed to be energized for short periods of time. Continuous operation may damage an intermittent duty solenoid.

intumescent The ability to expand to close gaps or voids in through-penetration openings when exposed to high-temperature conditions.

invisible That which is not visible or perceptible to the human eye. This is normally a particle smaller than 40 μm (micron) in diameter.

ionization The condition of matter when it is dissociated into ions or charged particles.

ionization smoke detection The principle of using a small amount of radioactive material to ionize the air between two differentially charged electrodes to sense the presence of smoke particles. Smoke particles entering the ionization volume decrease the conductance of the air by reducing ion mobility. The reduced conductance signal is processed and used to convey an alarm condition when it meets preset criteria.

 © 2012 BICSI®

K

keypad — An alphanumeric grid that allows a user to enter a personal identification code.

L

labeled — The equipment or materials to which has been attached a label, symbol, or other identifying mark of an organization that is acceptable to the authority having jurisdiction (AHJ) and concerned with product evaluation, that maintains periodic inspection of production of labeled equipment or materials, and by whose labeling the manufacturer indicates compliance with appropriate standards or performance in a specified manner.

laser diode — A laser for optical fiber applications, usually made from a p-n junction in a semiconductor material. Laser diodes give higher performance at higher cost than light-emitting diodes (LED). Laser diodes are commonly used with singlemode optical fiber.

leg facility — The portion of a telecommunications channel that connects not more than one protected premises to a primary or secondary trunk facility. The leg facility includes the portion of the signal transmission circuit from its point of connection with a trunk facility to the point where it is terminated within the protected premises at one or more transponders.

level ceilings — Ceilings that are level or have a slope of less than or equal to 1 in 8.

life safety network — A type of combination system that transmits fire safety control data through gateways to other building system control units.

light-emitting diode (LED) — A semiconductor diode that spontaneously emits incoherent light from the PN junction when forward current is applied. It converts information from electrical to optical form. An LED typically has a large spectral width.

line supervision — The electrical supervision of a monitoring loop to detect for tampering (a cut or shorted wire). Line supervision usually requires a terminating element at the end of the monitoring loop (e.g., resistor, diode).

line-type detector — A device in which detection is continuous along a path. Typical examples are rate-of-rise pneumatic tubing detectors, projected beam smoke detectors, and heat sensitive cable.

listed — Equipment 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 that either the equipment or material meets appropriate standards or has been tested and found suitable for a specified manner. (TIA)

loading capacity — The maximum number of discrete elements of fire alarm systems permitted to be used in a particular configuration.

local alarm — A visual or audible signaling device located at a monitored door, window, or other opening. It is used to pinpoint a violation by sounding a distinctive alarm at an opening and to frighten away the would-be intruder.

logging — Creating and storing a permanent record of events that can be reviewed, printed, and analyzed.

loss of power — A reduction of available voltage at the load below the point at which equipment can function as designed.

low-power radio transmitter — Any device that communicates with associated control/receiving equipment by low-power radio signals.

M

magnetic stripe card — An access control card with a strip of recordable magnetic material on which data is encoded.

maintenance — The repair service, including periodic inspections and tests, required to keep the fire alarm system and its component parts operative at all times. Replacement of the system or its components is necessary when they become undependable or inoperable.

mantrap — See interlock.

manual fire alarm box — A manually operated device used to initiate an alarm signal.

master box — A municipal fire alarm box that also can be operated by remote means.

master code card — An access card that grants access and exit at every card reader on the system.

master control unit (panel) — A control unit that serves the protected premises or portion of the protected premises as a local control unit and accepts input from other fire alarm control units.

mediator — A person who is trained in dispute resolution, including negotiation techniques, and is familiar with the art of making a deal. The mediator is neutral and does not offer legal advice but is actively engaged in the discussion process, including narrowing down the issues, offering alternatives, and generally directing the parties toward settling the dispute.

 © 2012 BICSI®

multi-dwelling unit (MDU) Includes apartments, townhouses, condominiums, and assisted-living facilities. These facilities may be under a single roof or consist of multiple buildings in a residential campus.

multiple station alarm A single station alarm capable of being interconnected to one or more additional alarms so that the actuation of one causes the appropriate alarm signal to operate in all interconnected alarms.

multiple station alarm device Two or more single station alarm devices that can be interconnected so that actuation of one causes all integral or separate audible alarms to operate; one single station alarm device having connections to other detectors or to a manual fire alarm box.

multiplexing (muxing) The combining of two or more communications channels into a common, high-capacity channel from which the original signals may be individually recovered.

municipal fire alarm box (street box) An enclosure housing a manually operated transmitter used to send an alarm to the public fire service communications center.

municipal fire alarm system A system of alarm-initiating devices, receiving equipment, and connecting circuits (other than a public telephone network) used to transmit alarms from street locations to the public fire service communications center.

municipal transmitter A transmitter that can only be tripped remotely that is used to send an alarm to the public fire service communications center.

muster report A report for accounting for occupants within a defined space, utilized as a tool to aid in the verification that all occupants are accounted for.

N

network A series of controllers, all connected via a telecommunications cable.

noncoded signal An audible or visible signal conveying one discrete bit of information.

noncontiguous property Owner- or user-protected premises where two or more protected premises, controlled by the same owner or user, are separated by a public thoroughfare, body of water, transportation right-of-way, or property owned or used by others.

non-fail-safe A lock or electric strike that remains locked or latched on loss of power. Same as fail-secure.

nonrequired system A supplementary fire alarm system component or group of components that is installed at the option of the owner and is not installed due to a building or fire code requirement.

nonrestorable initiating device — A device in which the sensing element is designed to be destroyed or is incapable of returning to its original state in the process of operation.

normal power — The electrical power provided by the serving utility company and distributed through the facility electrical system.

notification appliance — A fire alarm system component (e.g., bell, horn, speaker, light, text display) that provides audible, tactile, or visible outputs, or any combination thereof, designed to alert people to danger (e.g., fire alarm).

notification appliance circuit (NAC) — A fire alarm circuit used to connect and operate notification appliances to the fire alarm system.

notification zone — An area covered by notification appliances that are activated simultaneously.

nuisance alarm — Any alarm caused by mechanical failure, malfunction, improper installation, or lack of proper maintenance, or any alarm activated by a cause that cannot be determined.

O

obscuration — The effect of reducing the intensity of a light source by obscuring the source from detection or vision.

off-hook — To make connection with the public switched telephone network (PSTN) in preparation for dialing a telephone number.

on axis — The level of intensity measured on a perpendicular axis of a notification appliance (e.g., strobe light). This is often used to describe certain Underwriters Laboratories Inc.® (UL®) standard 1638 strobe lights that send their light out primarily in front of the device.

on-hook — To disconnect from the public switched telephone network (PSTN).

open area detection (protection) — The protection of an area (e.g., room, space) with detectors to provide early warning of fire.

operating mode, private — An audible or visible signaling only to those persons directly concerned with the implementation and direction of emergency action initiation and procedure in the area protected by the fire alarm system.

operating mode, public — An audible or visible signaling to occupants or inhabitants of the area protected by the fire alarm system.

operating system (OS) — The system software responsible for the direct control and management of hardware and basic system operations. The operating system (OS) also provides control of application software programs (e.g., word processing, web browsers).

 © 2012 BICSI®

other fire detectors — Devices that detect a phenomenon other than heat, smoke, flame, or gases produced by a fire.

ownership — Any property or building or its contents under legal control by the occupant, by contract, or by holding of a title or deed.

P

paging system — A system intended to page one or more persons by such means as voice over loudspeaker, coded audible signals or visible signals, or lamp annunciators.

panic bar — A push bar and latch mechanism that is installed on the secure side of an opening. When the push pad is pressed, the latch will be released and the opening will be unsecured.

parallel telephone system — A system in which an individually wired circuit is used for each fire alarm box.

pathway — **1.** A sequence of connections that provide the connectivity between devices on a network or between networks on an internetwork. **2.** The vertical and horizontal route of the telecommunications cable. **3.** A facility for the placement of telecommunications cable. (TIA)

penetration — An opening made in a firestop barrier.

perimeter area — The function of the perimeter system is to generate an alarm when the defined perimeter area is intruded upon. For effective perimeter protection, a combination of sensors is typically installed and integrated to sense, decide, and act on all attempts at unauthorized entry to the protected area.
Since the perimeter area is the first line of defense in any functional security system, it is important that the sensors specified match the environment to be protected.

permanent visual record (recording) — An immediately readable, not easily alterable, print, slash, or punch record of all occurrences of status change.

personal identification number (PIN) — A unique numeric code used to identify an individual.

photoelectric (photoelectric effect) — The property of a material to conduct electricity when light is applied to it where the amount of current can be varied depending on the frequency or intensity of the applied light.

photoelectric light obscuration smoke detection — The principle of using a light source and a photosensitive sensor onto which the principal portion of the source emissions is focused. When smoke particles enter the light path, some of the light is scattered and some is absorbed, thereby reducing the light reaching the receiving sensor. The light reduction signal is processed and used to convey an alarm condition when it meets preset criteria.

photoelectric light-scattering smoke detection — The principle of using a light source and a photosensitive sensor arranged so that the rays from the light source do not normally fall onto the photosensitive sensor. When smoke particles enter the light path, some of the light is scattered by reflection and refraction onto the sensor. The light signal is processed and used to convey an alarm condition when it meets preset criteria.

photosensitive epilepsy — A medical condition that can cause persons to experience seizures based on rapidly flickering light impulses. As a preventive measure, strobe-type notification appliances can be synchronized, so that multiple appliances do not cause overly rapid and disorienting light pulses.

physical security — 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.

piggybacking — More than one individual entering a secure area by following an authorized user into a secure area. See also tailgating.

pink noise — A noise masking system that creates an artificial sound barrier in open office environments to provide increased privacy by masking conversations.

placarded — A means to signify that the fire alarm system of a particular facility is receiving central station service by a listed central station or listed fire alarm service—a local company that is part of a systematic follow-up program under the control of an independent third-party listing organization.

plant — One or more buildings under the same ownership or control on a single property. See also campus.

pneumatic rate-of-rise tubing heat detector — A line-type detector comprising a small-diameter tubing, usually copper, that is installed on the ceiling or high on the walls throughout the protected area. The tubing is terminated in a detector unit containing diaphragms and associated contacts set to actuate at a predetermined pressure. The system is sealed except for calibrated vents that compensate for normal changes in temperature.

 © 2012 BICSI®

poisoned	The introduction and possible absorption of foreign material into the detection chamber of a fire, smoke, or other sensor causing a condition where the detecting elements are inhibited, effecting the electrical or catalytic reaction of the device.
polar	A diagrammatic method that maps a notification appliance output intensity over an angular plane, typically 180 degrees. A polar diagram can be used to illustrate notification appliance sound or light output at various locations relative to the appliance.
positive alarm sequence	An automatic sequence that results in an alarm signal, even when manually delayed for investigation, unless the system is reset.
power supply	A source of electrical operating power, including the circuits and terminations connecting it to the dependent system components.
primary battery (dry cell)	A nonrechargeable battery requiring periodic replacement.
primary trunk facility	The part of a transmission channel connecting all leg facilities to a supervising or subsidiary station.
prime contractor	The one company contractually responsible for providing central station services to a subscriber. The prime contractor can be either a listed central station or a listed fire alarm service.
private mode	The applications, situations, or incidents where a notification or signaling is intended to alert and inform only those directly involved with the response to an emergency, where trained personnel are in place to take additional measures and actions upon the notification. Such personnel may include fire fighters, security workers, and others who are familiar with the operation of the fire alarm system. Private mode visual signaling generally is not intended to compensate for hearing impairment or high ambient noise conditions.
private radio signaling	A radio system under control of the proprietary supervising station.
privity	The knowledge of something secret or private.
programmable card	A card on which data may be encoded.
projected beam-type detector	A type of photoelectric light obscuration smoke detector wherein the beam spans the protected area.
proprietary supervising station	The location to which alarm or supervisory signaling devices on proprietary fire alarm systems are connected and where personnel are in attendance at all times to supervise operation and investigate signals.

proprietary supervising station fire alarm system An installation of fire alarm systems that serves contiguous and noncontiguous properties, under one ownership, from a proprietary supervising station located at the protected property, at which trained, competent personnel are in constant attendance. This includes the proprietary supervising station; power supplies; signal-initiating devices; initiating device circuits; signal notification appliances; equipment for the automatic, permanent visual recording of signals; and equipment for initiating the operation of emergency building control services.

protected premises **1.** The physical location protected by a fire alarm system. A protected premises system sounds an alarm at the protected premises as the result of the manual operation of a fire alarm box or the operation of protection equipment or systems (e.g., water flowing in a sprinkler system, detection of smoke). 2. Provides a hierarchy of rights and privileges for different user groups and their associated authorized zones.

protected premises (local) control unit (panel) A control unit that serves the protected premises or a portion of the protected premises and indicates the alarm via notification appliances inside the protected premises.

protected premises (local) fire alarm system A protected premises system that sounds an alarm at the protected premises as the result of the manual operation of a fire alarm box or the operation of protection equipment or systems (e.g., water flowing in a sprinkler system, discharge of carbon dioxide, detection of smoke or heat).

protected system A wireless system that provides redundancy by using a transmitter combiner to connect two transceivers to an antenna for redundancy.

proximity A method of reading a card without requiring any physical contact between the card and the reading device.

proximity card A card using proximity technology to store and transmit encoded data.

public fire alarm reporting system A system of fire alarm initiating devices, receiving equipment, and connecting circuits used to transmit alarms from street locations to the communications center.

public fire alarm reporting system, type a A system in which an alarm from a fire alarm box is received and retransmitted to fire stations either manually or automatically.

public fire alarm reporting system, type b A system in which an alarm from a fire alarm box is automatically transmitted to fire stations and, if used, transmitted to supplementary alerting devices.

public fire service communications center A building or portion of the building used to house the central operating part of the fire alarm system; typically the place where the necessary testing, switching, receiving, transmitting, and power supply devices are located.

 © 2012 BICSI®

public mode The applications, situations, or incidents where a notification or signaling is intended to alert and provide adequate warning of imminent danger so that all occupants of a building can safely evacuate the premises. In public mode, notifications and signaling must therefore be unambiguous, simple, and easily recognizable by all persons with no knowledge of fire alarm systems and be able to reach all occupants of the premises.

public switched telephone network (PSTN) An assembly of telecommunications facilities and central office equipment operated jointly by authorized common carriers that provides the general public with the ability to establish telecommunications channels via discrete dialing codes. Usually accessed by telephones, key telephone systems, private branch exchange trunks, and data arrangements.

R

radiant energy-sensing fire detector A device that detects radiant energy (e.g., ultraviolet, visible, infrared) that is emitted as a product of combustion reaction and obeys the laws of optics.

radio alarm repeater station receiver (RARSR) System component that receives radio signals and resides at a repeater station that is located at a remote receiving location.

radio alarm supervising station receiver (RASSR) System component that receives data and annunciates that data at the supervising station.

radio alarm system (RAS) System in which signals are transmitted from a radio alarm transmitter located at a protected premises through a radio channel to two or more radio alarm repeater station receivers that are annunciated by a radio alarm supervising station receiver located at the central station.

radio alarm transmitter (RAT) System component at the protected premises to which initiating devices or groups of devices are connected that transmits signals indicating a status change of the initiating devices.

radio channel Band of frequencies of a width sufficient to allow its use for radio communications.

radio frequency identification device (RFID) Generic term for technologies that use radio waves to automatically identify people or objects.

rate-compensated heat detectors Devices that are designed to activate at a predetermined temperature in a space regardless of the rate at which the temperature in the space increases.

rate compensation detector A device that responds when the temperature of the air surrounding the device reaches a predetermined level, regardless of the rate of temperature rise.

rate-of-rise detector	A device that responds when the temperature rises at a rate exceeding a predetermined value.
rate-of-rise pneumatic tubing heat detector	A line-type detector consisting of small-diameter tubing and a detector unit that actuates at a predetermined pressure. The system is sealed except for calibrated vents that compensate for changes in ambient temperature.
reader	A device that receives an identification code from a card.
reader collision	When the signal from one reader can interfere with the signal from another reader where coverage overlaps.
record drawings	Drawings (as-built) that document the location of all devices, appliances, wiring sequences, wiring methods, and connections of the components of the fire alarm system as installed.
record of completion	A document that acknowledges the features of installation, operation, service, and equipment with representation by the property owner, system installer, system supplier, service organization, and the authority having jurisdiction (AHJ).
recycle time	The time needed to reset and reinstate the timing function and remain within the specified timing tolerances. Recycle time is generally specified "during timing" or "after timing."
relocation	The movement of occupants from a fire zone to a safe area within the same building.
remote alarm	A visual or audible signaling device used to signal violations at locations removed from the central control station or monitored openings. A remote alarm may be placed on a roof, in a stair tower, or in a guard station outside a building.
remote supervising station fire alarm system	A system installed to transmit alarm, supervisory, and trouble signals from one or more protected premises to a remote location where appropriate action is taken.
repeater station	The location of the equipment needed to relay signals between supervising stations, subsidiary stations, and protected premises.
request to exit (REX) signal	A signal that informs the controller that someone has requested an exit from the secure area.
request to exit (REX) switch	Utilized with access control systems (ACS), this switch is located on the secured side of a controlled door.

 © 2012 BICSI®

reset — A control function that attempts to return a system or device to its normal, nonalarm state.

restorable initiating device — A device in which the sensing element is not ordinarily destroyed in the process of operation, whose restoration can be manual or automatic.

risk — A vulnerability to or potential for loss from a threat or event.

runner — A person other than the required number of operators on duty at central, supervising, or runner stations (or otherwise in contact with these stations) available for prompt dispatching, when necessary, to the protected premises.

runner service — A service provided by a runner at the protected premises, including resetting and silencing of all equipment transmitting fire alarm or supervisory signals to an off-premises location.

S

sally port — See interlock.

satellite trunk — A circuit or path connecting a satellite to its central or proprietary supervising station.

scalability — An existing system's capability of growing to meet the customer's needs over time. Most legacy systems are not scalable, resulting in obsolescence of components or entire systems and requiring regular software and hardware replacements.

scanner — The equipment located at the telephone company wire center that monitors each local leg and relays status changes to the alarm center. Processors and associated equipment also might be included.

scattering — The deflection of light by small particles or inhomogeneities whose size is similar to or smaller than the wavelength of light.

sealant — A material that has the adhesive and cohesive properties to form a seal.

secondary trunk facility — The part of a transmission channel connecting two or more, but fewer than all, leg facilities to a primary trunk facility.

secured side — The area or side of an opening that is locked and requires a key card or other means to enter.

separate sleeping area — An area of the family living unit in which the sleeping rooms are located. Sleeping rooms separated by other use areas (e.g., kitchens, living rooms, but not bathrooms) are considered as separate sleeping areas.

shall	Frequently used in code publications, "shall" indicates a mandatory requirement.
shear lock magnetic lock	A modification of the direct hold magnetic lock that utilizes both magnetic and physical properties for locking. The electric magnet's lock body is mortised into the door's frame, and the armature is mortised into the door edge. Indentations in the armature receive protrusions in the lock body.
should	Indicates a recommendation or that which is advised but not required.
signal	A status indication communicated by electrical or other means.
signal transmission sequence	A digital alarm communicator transmitter that obtains dial tone, dials the number(s) of the digital alarm communicator receiver (DACR), obtains verification that the DACR is ready to receive signals, transmits the signals, and receives acknowledgment that the DACR has accepted that signal before disconnecting (going on-hook).
signaling line circuit (SLC)	A circuit or path between any combination of circuit interfaces, control units, or transmitters over which multiple system input signals or output signals, or both, are carried.
signaling line circuit interface	A system component that connects a signaling line circuit to any combination of initiating devices, initiating device circuits, notification appliances, notification appliance circuits, system control outputs, and other signaling line circuits.
signature verification	A biometric method using a person's signature characteristics (writing speed, pen pressure, shape of loops) to identify that person.
single dwelling unit	A building consisting solely of one dwelling unit. See also dwelling unit.
single station alarm	A detector comprising an assembly that incorporates the sensor, control components, and alarm notification appliance in one unit operated from a power source either in the unit or at the point of installation.
single station alarm device	An assembly that incorporates the detector, the control equipment, and the alarm-sounding device in one unit operated from a power supply either in the unit or at the point of installation.
site-specific software	Software that defines the specific operation and configuration of a particular system. Typically, it defines the type and quantity of hardware modules, customized labels, and specific operating features of a system.
sloping ceiling	A ceiling that has a slope of more than one in eight.

 © 2012 BICSI®

sloping peaked-type ceiling	A ceiling in which the ceiling slopes in two directions from the highest point. Curved or domed ceilings can be considered peaked, with the slope figured as the slope of the chord from the highest to lowest point.
sloping shed-type ceiling	A ceiling in which the high point is at one side, with the slope extending toward the opposite side.
S mark	A European safety mark valid throughout the European Union. Products bearing the S mark demonstrate compliance with legal European electrical safety requirements via third-party testing.
smart card	A card with a built-in integrated circuit chip. This gives the card microprocessor memory and intelligence to use for storing data.
smart environment	A smart environment employs pervasive embedded computation systems to collect sensory data from the real world, assess and evaluate the resulting information, interact with human users, and perform and facilitate alarm, decision-making, and control functions. Smart environments can exist in houses, vehicles, buildings, and campuses and include the use of telecommunications networks, sensor devices, computer hardware, and software. The word "environment" refers to the location where the employed systems collect data and operate to adapt accordingly.
smoke alarm	A single or multiple station alarm responsive to smoke.
smoke detector	A device that detects visible or invisible particles of combustion.
smooth ceiling	A ceiling surface uninterrupted by continuous projections (e.g., solid joists, beams, ducts) extending more than 101 mm (3.98 in) below the ceiling surface.
spacing	The horizontally measured dimension related to the allowable coverage of fire detectors.
spark	A moving ember.
spark/ember detector	A radiant energy-sensing fire detector that is designed to detect sparks or embers. These devices are intended to operate in dark environments and in the infrared part of the spectrum.
spark/ember detector sensitivity	The number of watts (or the fraction of a watt) of radiant power from a point source radiator, applied as a unit step signal at the wavelength of maximum detector sensitivity, necessary to produce an alarm signal from the detector within the specified response time.
spot-type detector	A device in which the detecting element is concentrated at a particular location. Typical examples are bimetallic detectors, fusible alloy detectors, certain pneumatic rate-of-rise detectors, certain smoke detectors, and thermoelectric detectors.

standby power	An electrical power provided by an on-site source for use when normal power is not available.
story	The portion of a building included between the upper surface of a floor and the upper surface of the floor or roof next above.
stratification	A phenomenon where the upward movement of smoke and gases ceases due to the loss of buoyancy.
strobe	A signaling device that produces a bright flashing high-intensity light notification. Stroboscopic lights (commonly called strobes) operate on the energy discharge theory to produce a high-intensity flash of short duration. The short bright flash is not only attention producing but also very effective in areas of low visibility. Strobe appliances come in a wide range of light intensities measured in candelas (cd). Typical strobe candela ratings are 15 cd, 30 cd, 15/75 cd, and 75 cd. Repetition rates are usually between one and five flashes per second. Strobe devices are usually marked with the word "fire" or a pictogram communicating the purpose of the device.
subscriber	A recipient of a contractual supervising station signal services. In case of multiple, noncontiguous properties having single ownership, the term refers to each protected premises or its local management.
subsidiary station	A normally unattended location that is remote from the supervising station and is linked by telecommunications channels to the supervising station. The interconnection of signals on one or more transmission channels from protected premises with telecommunications channels to the supervising station is performed at this location.
supervising station	A facility that receives signals and at which personnel are in attendance at all times to respond to these signals.
supervising station system	A supervising station system differs from a protected premises system by reporting the signals provided to the supervising station system from the protected premises system for retransmission to the designated fire protection authorities.
supervision	The continuous monitoring of the condition of the fire alarm system conductors and devices.
supervisory control and data acquisition (SCADA)	SCADA systems are used in industry and by public utilities (e.g., pipelines, electric utility grids) to monitor and control plant status and provide logging facilities that are often scattered over wide geographic areas. SCADA systems are highly configurable and traditionally use standard telephone lines to propagate their data. Public utilities are beginning to utilize these systems for the integration and transmission of voice, data, and security systems.

 © 2012 BICSI®

supervisory service — The service required to monitor performance of guard tours and the operative condition of fixed suppression systems or other systems for the protection of life and property.

supervisory signal — A signal designed to alert only facilities or maintenance personnel. Supervisory signals are used for nonemergency situations and generally are not used to activate general building notification appliances.

supervisory signal initiating device — An initiating device (e.g., valve supervisory switch, water level indicator, low air pressure switch on a dry-pipe sprinkler system) in which the change of state signals an off-normal condition and its restoration to normal of a fire protection or life safety system or a need for action in connection with guard tours, fire suppression systems or equipment, or maintenance features of related systems.

supervisory switch — A switch designed to supervise sprinkler system control valves.

supplementary — The equipment or operations not required and designated as such by the authority having jurisdiction (AHJ).

suppression system operation detector — See automatic fire extinguishing detector.

switched telephone network — An assembly of telecommunications facilities and central office equipment operated jointly by authorized service providers (ASPs) that provide the general public with the ability to establish transmission channels via discrete dialing.

system unit — The active subassemblies at the central station used for signal receiving, processing, display, or recording status change signals. A failure of one of these subassemblies causes the loss of a number of alarm signals by that unit.

T

tactile notification appliance — A notification appliance that alerts by sense of touch or vibration.

tailgating — **1.** In access control, one or more individuals entering a controlled area by using a single card. **2.** Following an authorized person into a controlled area. See also piggybacking.

telemetry — A telecommunications system designed for the automatic transmission of digital or analog data by wire, radio, or other means from remote sources to a receiving source for the recording, monitoring, and analysis of systems.

temperature resistance rating (t-rating) The time, in hours, that a firestop system will withstand a temperature test such as to raise the temperature of the unexposed surface of the firestop system by 163 °C (325 °F) above its initial temperature.

temporal code An audible pattern that is standardized to make it more universal or recognizable.

textual audible notification appliance An appliance that conveys a stream of audible information (e.g., a speaker that reproduces a voice message).

textual visible notification appliance A notification appliance that conveys a stream of visible information that displays an alphanumeric or pictorial message (e.g., annunciators, monitors, cathode ray tube, displays, printers). Textual visible notification appliances provide temporary text, permanent text, or symbols.

threat An indication of the event or the intent to do harm and/or damage.

threat analysis An evaluation of an environment, structure, or scenario for the purpose of deterring potential vulnerabilities for an unauthorized entry, removal of physical or intellectual material, or exposure to terrorist activities.

through penetration **1.** An opening in a fire barrier consisting of three items—wall or floor construction, penetrating item, and the hole or void. **2.** A continuous opening that passes through both surfaces of a fire-rated barrier. (TIA)

time zone A specified period of time in which access is allowed.

transmission channel A circuit or path connecting transmitters to supervising stations or subsidiary stations on which signals are carried.

transmitter (TX) A system component and signaling source that provides an interface between signaling line circuits, initiating device circuits, or control units and the transmission channel.

transponder A multiplex alarm transmission system functional assembly located at the protected premises.

trouble signal A signal designed to alert facilities or maintenance personnel of a system malfunction. Trouble signals are used to indicate and generally are not used to activate general building notification appliances.

turnstile An entryway that uses a mechanical device to restrict entry to one person at a time.

 © 2012 BICSI®

U

upload — To send information from the controller to the host computer.

V

vignetting — A tunnel or porthole image that is produced by using a smaller image-size format lens on a larger image-size format camera (e.g., 8 mm [0.31 in]) lens and 13 mm (1/2 in) camera). Similar to an unbordered picture, often a portrait, that shades off into the surrounding color at the edges. Conversely, one can use a larger image-size lens on a smaller image-size format camera.

visible notification appliance — An alarm appliance that alerts occupants with light.

voice intelligibility — An audible voice information that is distinguishable and understandable.

voice recognition — Identifying an individual by comparing previously stored voice recordings of key words or phrases with the same key phrases spoken at the same time access is requested.

W

wavelength — The distance between the peaks of a sinusoidal wave. All radiant energy can be described as a wave having a wavelength. Wavelength serves as the unit of measure for distinguishing between different parts of the spectrum. Wave lengths are measured in microns (µm), nanometers (nm), or angstroms (å).

wide area telephone service (WATS) — A telephone company service allowing reduced costs for certain telephone call arrangements. In WATS, 800-number service calls can be placed from anywhere in the continental United States to the called party at no cost to the calling party. Out WATS is a service whereby, for a flat-rate charge, dependent on the duration of such calls, a subscriber can make an unlimited number of calls within a prescribed area from a particular telephone terminal without the registration of individual call charges.

wireless control panel — A component that transmits/receives and processes wireless signals.

wireless mesh network — A wireless fidelity (IEEE 802.11x) network that uses a mesh network topology between wireless nodes.

wireless protection system — A system or part of a system that can transmit and receive signals without the aid of wire. It can consist of either a wireless control panel or a wireless repeater.

wireless repeater — A component used to relay signals between wireless receivers or wireless control panels, or both.

X

x-by-wire — See by-wire.

Z

zone — A defined area within the protected premises. A zone can define an area from which a signal can be received, an area to which a signal can be sent, or an area in which a form of control can be executed. A zone is created by connecting multiple fire detection devices to a common circuit. Although a zone often has a geographic connotation, a zone is a result of system wiring and not the physical placement of a device.

zone paging — The ability to send an audio signal to a specific group of loudspeakers.

 © 2012 BICSI®

Acronyms and Abbreviations

3G	third generation (wireless format)
4G	fourth generation (wireless format)
10BASE-FL	The IEEE 802.3 standard for baseband Ethernet at 10 Mb/s over two optical fibers (optional asynchronous hub).
µm	micrometer

A

A	ampere
AAA	American Arbitration Association
AACS	Advanced Access Content System
AASCI	American standard code for information interchange
ac	alternating current
AC	actual cost
ACC	access control center
ACGIH®	American Conference of Governmental Industrial Hygienists
ACK	acknowledgment
ACL	access control list
ACN	automatic crash notification
ACS	access control systems
ACWP	actual cost of work performed
A/D	analog-to-digital
ADA	Americans with Disabilities Act
ADAAG	Americans with Disabilities Act Accessibility Guidelines
ADR	alternative dispute resolution

ADSL	asymmetric digital subscriber line
A&E	architecture and engineering
AEC	architect/engineer/contractor
AEC	architecture, engineering, and construction
a/e ProNet	Architects/Engineers Professional Network
AES	advanced encryption standard
AFCESA	Air Force Civil Engineer Support Agency AFF
AFF	above finished floor
AGC	Associated General Contractors of America
AGC	automatic gain control
Ah	ampere-hour
AHJ	authority having jurisdiction
AI	analog input
AI	artificial intelligence
AIA	American Institute of Architects
AICC	Alarm Industry Communications Committee
AIT	advanced intelligent tape
ALC	automatic level control
AM	amplitude modulation
amp	ampere
ANSI	American National Standards Institute
AP	access point
API	application programming interface
ARCnet	attached resources computing network
ARP	address resolution protocol

 © 2012 BICSI®

AS2	applicability statement 2
ASA	Acoustical Society of America
ASCII	American standard code for information interchange
ASHRAE	American Society of Heating, Refrigerating, and Air-Conditioning Engineers, Inc.
ASIS	ASIS International
ASME	American Society of Mechanical Engineers International
ASP	application service provider
ASP	authorized service provider
ASTM	American Society for Testing and Materials
ATM	asynchronous transfer mode
ATM	automatic teller machine
AV	audiovisual
AVC	advanced video coding
AVDRM	*AV Design Reference Manual*
AVL	automatic vehicle location
AVMD	advanced video motion detection
AWG	American wire gauge

B

BACnet®	building automation and control network
BAS	building automation systems
BCWP	budgeted cost of work performed
BCWS	budgeted cost of work scheduled
BD	building distributor

BER bit error rate

BGP border gateway protocol

BHMA Builders' Hardware Manufacturers Association

BIM building information modeling

BIOS basic input output system

BMS building management system

BOD basis of design

BOCA Building Officials and Code Administrators International, Inc.

BOM bill of material

Btu British thermal unit

BWA broadband wireless access

C

CA construction administration

CAD computer-aided design

CAFM computer-aided facility management

CAL common application language

CAN campus area network

CATV community antenna TV

CCB Construction Criteria Base

CCD charge-coupled device

CCTV closed-circuit TV

cd candela

CD compact disc

CD construction document

 © 2012 BICSI®

CDMA	code division multiple access
CEA	Consumer Electronics Association
CEBus®	Consumer Electronics Bus
CEC®	Canadian Electrical Code®
CENELEC	Comité Européen de Normalisation
cfm	cubic foot per minute
CGI	common gateway interface
CI	circuit integrity
CIA	confidentiality, integrity, and availability
CIC	carrier identification code
CIC	CEBus® Industry Council
CIDR	classless interdomain routing
CIF	common intermediate format
CIS	common intelligibility scale
CISSP™	Certified Information Systems Security Professional
CK	compartment key
CLADI	Communications, Life Safety, and Automation Design Institute
CM	construction manager
CMOS	complementary metal-oxide semiconductor
CMP	communications plenum cable
CO	carbon monoxide
CO	central office
CO	change order
CO_2	carbon dioxide
CP	consolidation point

CPI	cost performance index
CPM	critical path method
CPP™	Certified Protection Professional
CPTED	crime prevention through environmental design
CPU	central processing unit
CR	card readers
CRAC	computer room air-conditioner
CRI	color rendition index
CRT	cathode ray tube
CSA®	Canadian Standards Association®
CSAA	Central Station Alarm Association
CSC	Construction Specifications Canada
CSI	Construction Specifications Institute

D

D/A	digital-to-analog
DACR	digital alarm communicator receiver
DACS	digital alarm communicator system
DACT	digital alarm communicator transmitter
DAMA-TDMA	demand assignment multiple access-time division multiple access
DARR	digital alarm radio receiver
DARS	digital alarm radio system
DART	digital alarm radio transmitter
DAS	direct attached storage
DAT	digital audiotape

 © 2012 BICSI®

dB	decibel
dBA	decibel adjusted for frequency
dBa	A-weighted decibel
dB(a)	A-weighted decibel
DBIA	Design-Build Institute of America
dBm	decibel milliwatt
dc	direct current
DCS	distributed control system
DD	design development
DDoS	distributed denial of service
DDNS	dynamic domain name service
DECT	digital enhanced cordless telecommunications
DHCP	dynamic host configuration protocol
DHS	Department of Homeland Security
D-ILA	direct-drive image light amplifier
DIP	dual in-line package
DLP	digital light processor
DMM	digital multimeter
DMZ	demilitarized zone
DNR	digital noise reduction
DNS	domain name system
DoD	Department of Defense
DoJ	Department of Justice
DoS	denial of service
DPDT	double-pole, double-throw

DPIC	Design Professionals Insurance Company
DPS	door position sensor
DPST	double-pole, single-throw
DRSC	dedicated short-range communications
DSL	digital subscriber line
DSP	digital signal processor
DVD	digital versatile disc
DVI-D	digital visual interface–digital
DVI-I	digital visual interface–integrated
DVMS	digital video management system
DVR	digital video recorder

E

E-to-O	electronic-to-optical
E/O	electronic-to-optical
EC	electrical contractor
EDID	extended display identification data
EEPROM	electrically erasable programmable read-only memory
EFA	Epilepsy Foundation of America
EFD	Engineering Field Division
EIA	Electronic Industries Alliance
EJCDC	Engineers Joint Contract Documents Committee
EMI	electromagnetic interference
EMT	electrical metallic tubing
EOC	emergency operations center

 © 2012 BICSI®

EOL	end-of-line
EOLR	end-of-line resistor
EPSS	emergency power supply system
ER	equipment room
ERR	equal error rate
ESS	electronic safety and security
ESSDRM	*Electronic Safety and Security Design Reference Manual*
ETSI	European Telecommunications Standards Institute
EV	earned value

F

FA	fire alarm
FACP	fire alarm control panel
FAR	false acceptance rate
FAT	functional acceptance test FBO furnished by owner
FCC	Federal Communications Commission
FDA	Food and Drug Administration
FDM	frequency division multiplexing
FEMA	Federal Emergency Management Agency
FER	failure to enroll rate
FIPS	Federal Information Processing Standard
FIT	frame interline transfer
FLS	fire-life-safety
FM	factory mutual
FM	frequency modulation

FMR	false match rate
FMRC	Factory Mutual Research Corporation
FNMR	false nonmatch rate
FRR	false rejection rate
f/s	frames per second
FS	flow switch
FSO	free space optics
FSS	Federal Supply Schedule/Service
ft	foot
FTC	failure to capture
FTP	file transfer protocol
FTS	Federal Technology Service

G

GB	gigabyte
GC	general contractor
GGMK	great grand master key
GHz	gigahertz
GIS	geographic information system
GMK	grand master key
GMP	guaranteed maximum price
GPO	Government Printing Office (U.S.)
GPS	global positioning satellite

 © 2012 BICSI®

GPS	global positioning system
GPSG	German Equipment and Product Safety Act
GSA	General Services Administration
GSM	Global System for Mobile Communications
GUI	graphical user interface

H

HD	heat detector
HD	high definition
HDMI	high-definition multimedia interface
HDMI	high-density multimode interface
HDSDI	high-definition serial digital interface
HDTV	high-definition TV
HHR	half horizontal resolution
HIDS	host-based IDS
HIPAA	Health Insurance Portability and Accountability Act
HMI	human machine interface
H_2O	water
HOV	high-occupancy vehicle
HR	human resources
HTTP	hypertext transfer protocol
HVAC	heating, ventilating, and air conditioning
Hz	Hertz

I

I/O	input/output
IACET	International Association for Continuing Education Training
IAF	International Accreditation Forum
IAFC	International Association of Fire Chiefs
IBC	International Building Code
IBNS	identity-based networking services
IC	intermediate cross-connect
ICAC®	International Certification Accreditation Council
ICBO	International Conference of Building Officials
ICC	International Code Council
ICEA	Insulated Cable Engineers Association, Inc.
ICMP	Internet control message protocol
ICS	integrated control system
ICS	International Classification for Standards
ICU	intensive care unit
IDC	initiating device circuit
IDF	intermediate distribution frame
IDS	intrusion detection systems
IEC®	International Electrotechnical Commission®
IEEE®	Institute of Electrical and Electronics Engineers, Inc.®
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IM	instant messaging

 © 2012 BICSI®

in	inch
InfoSec	information security
I/O	input/output
IP	Internet protocol
IPD	integrated project delivery
IPS	images per second
IPS	intrusion prevention system
IPSec	Internet protocol security
IPv4	Internet protocol version 4
IPv6	Internet protocol version 6
IR	infrared
IRE	Institute of Radio Engineers
IRMI	International Risk Management Institute
ISDN	integrated services digital network
ISO	International Organization for Standardization
IT	information technology
ITS	information technology systems
ITSIMM	*Information Technology Systems Installation Methods Manual*
ITU	International Telecommunication Union
IV	intravenous

J

JPEG	Joint Photographic Experts Group

K

K	Kelvin
KA	keyed alike
kB	kilobyte
kb/s	kilobit per second
KD	keyed differently
kg	kilogram
kHz	kilohertz
km	kilometer
kPa	kilopascal
KPI	key performance indicator
kW	kilowatt

L

lb	pound
lbf	pound-force
LCD	liquid crystal display
LCoS	liquid crystal on silicon
LD	laser diode
LED	light-emitting diode
LoS	line of sight
LP	low pressure
LPC	license plate capture
LPR	license plate recognition
LRE	long-reach Ethernet

 © 2012 BICSI®

M

m	meter
mA	milliampere
MAC	media access control
MAC	move, add, or change
MAN	metropolitan area network
MAPI	mail application interface
MATV	master antenna TV
MB	megabyte
Mb/s	megabits per second
MBWA	Mobile Broadband Wireless Access
MC	mechanical contractor
MDF	main distribution frame
MDU	multi-dwelling unit
MH	maintenance hole
MHz	megahertz
MIB	management information base
M-JPEG	Motion-Joint Photographic Experts Group
mm	millimeter
MOV	metal oxide varistor
MP	megapixel
MPEG	Moving Picture Experts Group
MPLS	multi-protocol label switching
MTF	modulation transfer function

N

NAC	network admission control
NAC	notification appliance circuit
NAP	network access protection
NAS	network-attached storage
NASFM	National Association of State Fire Marshals
NAVFAC	Naval Facilities Engineering Command
NBC	*National Building Code of Canada*
NBFAA	National Burglar and Fire Alarm Association
NC	normally closed
NCS	National CAD Standard
NDRM	*Network Design Reference Manual*
NEC®	*National Electrical Code®*
NEMA®	National Electrical Manufacturers Association
NESC®	*National Electrical Safety Code®*
NFIP	National Flood Insurance Program
NFPA®	National Fire Protection Association®
NIBS	National Institute of Building Sciences
NIC	network interface card
NICET	National Institute for Certification in Engineering Technologies
NIST	National Institute of Standards and Technology
nm	nanometer
NO	normally open

 © 2012 BICSI®

NOS	network operating system
NRTL	Nationally Recognized Testing Laboratory
NSCA	National Systems Contractors Association
NTSC	National Television System Committee
NVR	network video recorder

O

O-to-E	optical-to-electronic
O/E	optical-to-electronic
OAT	operational acceptance test
OBS	organization breakdown schedule
ODBC	open database connectivity
OGP	Office of Governmentwide Policy
OLE	object linking and embedding
OLED	organic light-emitting diode
OPC	object linking and embedding for process control
OS	operating system
OSHA	Occupational Safety and Health Administration
OSHPD	Office of Statewide Health Planning and Development
OSI	Open Systems Interconnection
OSP	outside plant
OSPDRM	*Outside Plant Design Reference Manual*
OS&Y	outside stem and yoke

P

P	pixel
PA	public address
PA	public announcement
PAL	phase alternation line
PAN	personal area network
PARP	proxy address resolution protocol
PASC	Pacific Area Standards Congress
PB	push button
PBS	Public Buildings Service
PBX	private branch exchange
PD	powered device
PDA	personal digital assistant
PDG	project development guide
PE	professional engineer
PERT	program evaluation review technique
PID	passive infrared detector
PIN	personal identification number
PIR	passive infrared
PIV	personal identification verification
PLC	power-line carrier
PLC	programmable logic controller
PM	phase modulation
PM	project management

 © 2012 BICSI®

PM	project manager
PMBOK®	Project Management Body of Knowledge
PMI®	Project Management Institute®
PMP®	Project Management Professional
PoE	power over Ethernet
POS	point-of-sale
POTS	plain old telephone service
p-p	peak-to-peak (signal)
PPF	pixels per foot
PRM	*The Project Resource Manual—CSI Manual of Practice*
PSE	power sourcing equipment
psi	pound-force per square inch
PSIM	physical security information management
PSP®	Physical Security Professional
PSTN	public switched telephone network
PTP	point-to-point
PTZ	pan, tilt, and zoom
PV	planned value
PVC	polyvinyl chloride

Q

QCIF	quarter common intermediate format
QoS	quality of service
QVGA	quarter video graphics array

R

R&D	research and development
RADIUS	remote authentication dial-in user service
RAID	redundant array of independent disks
RAM	random access memory
RARP	reverse address resolution protocol
RARSR	radio alarm repeater station receiver
RAS	radio alarm system
RASSR	radio alarm supervising station receiver
RAT	radio alarm transmitter
RCDD®	Registered Communications Distribution Designer
REX	request to exit
RF	radio frequency
RFI	radio frequency interference
RFI	request for information
RFI	request for interpretation
RFID	radio frequency identification
RFP	request for proposal
RFQ	request for quote
RG	radio grade
RGB	red, green, blue
RGBHV	red, green, blue, horizontal sync, vertical sync
RMS	root, mean, square
RNCM	*Residential Network Cabling Manual*

 © 2012 BICSI®

ROI	return on investment
ROM	rough order of magnitude
R/RW	read/read-write
Rx	receiver

S

s	second
SaaS	software as a service
SAN	storage area network
SAP	service access point
SAT	systems acceptance test
SBC	Standard Building Code
SBCCI	Southern Building Code Congress International
SCADA	supervisory control and data acquisition
SCS	structured cabling system
ScTP	screened twisted-pair
SD	schematic description
SD	schematic design
SD	smoke detector
SDI	serial digital interface
SDK	software development kit
SDO	standards development organization
SDSL	symmetrical digital subscriber line
SIA	Security Industry Association
SIEM	security information and event management

SIF	standard input format
SLC	signaling line circuit
SMB	server message block
SMG	server message block
SNMP	simple network management protocol
SOAP	simple object access protocol
SONET	synchronous optical network
SoR	statement of requirements
SoW	scope of work
SOX	Sarbanes-Oxley Act of 2002
SPDT	single pole, double throw
SPI	scheduled performance index
SPL	sound pressure level
SPST	single pole, single throw
SQCIF	subquarter common intermediate format
SR/WA	senior right-of-way agent
SS	safety shower
SSL	secure sockets layer
STP	shielded twisted-pair
STP	spanning tree protocol
SVGA	super video graphics array
SYN	synchronize
SXGA	super extended graphics array

 © 2012 BICSI®

T

TACACS	terminal access controller access control systems
TCAS	traffic alert and collision avoidance system
TCP	transmission control protocol
TCP/IP	transmission control protocol/Internet protocol
TDM	time division multiplexing
TDMA	time division multiple access
TDMM	*Telecommunications Distribution Methods Manual*
TIA	Telecommunications Industry Association
TLS	transport layer security
TPMA	Telecommunications Project Management Association
TR	telecommunications room
TS	tamper switch
TSA	Transportation Security Administration
TTA	Telecommunications Technology Association
TTC	Telecommunication Technology Committee
TVL	TV line
TWCS	Telecommunications Wire and Cable Standards
Tx	transmit

U

UBC	Uniform Building Code
UDP	user datagram protocol
UDS	Uniform Drawing System

UFGS	Unified Facilities Guide Specifications
UHF	ultrahigh frequency
UL®	Underwriters Laboratories Inc.®
U-NII	unlicensed national information infrastructure
UPC	universal product code
UPCS	utility power cable standards
UPS	uninterruptible power supply
USACE	United States Army Corps of Engineers
USB	universal serial bus
UTP	unshielded twisted-pair
UV	ultraviolet

⎓V

V	volt
Vac	volt alternating current
VBW	video bandwidth
VCR	videocassette recorder
Vdc	volt direct current
VE	value engineering
VGA	video graphics array
VHS	vertical helix scan
VLAN	virtual LAN

 © 2012 BICSI®

VMD	video motion detection
VoIP	voice over Internet protocol
VPN	virtual private network
VRRP	virtual router redundancy protocol
VSS	video surveillance systems
VTP	virtual terminal protocol

W

W	watt
W3C	World Wide Web Consortium
WAN	wide area network
WATS	wide area telecommunications service
WBS	work breakdown structure
WDRM	*Wireless Design Reference Manual*
WEP	wired equivalent privacy
Wi-Fi	wireless fidelity
WiMAX	worldwide interoperability for microwave access
WLAN	wireless LAN
WMAN	wireless metropolitan area network
WORM	write-once, read-many
WPAN	wireless personal area network
WWAN	wireless wide area network
WWW	World Wide Web

X

xDSL digital subscriber lines family

xDSL x digital subscriber line

XGA extended graphics array

XLR X latching resilient rubber compound

XML extensible markup language

 © 2012 BICSI®

Bibliography and Resources

Chapter 3: Electronic Safety and Security (ESS) Design Process

Construction Specifications Institute. *MasterFormat™*. Alexandria, VA: Construction Specifications Institute, 2004.

———. *SectionFormat™/PageFormat™*. Alexandria, VA: Construction Specifications Institute, 2008.

———. *The Project Resource Manual—CSI Manual of Practice*, 5th ed. New York: McGraw-Hill, 2004.

Chapter 4: Access Control Systems (ACS)

International Organization for Standardization. ISO 11784. *Radio Frequency Identification of Animals—Code Structure*. Geneva, Switzerland: International Organization for Standardization, 2010.

———. ISO 11785. *Radio Frequency Identification of Animals—Technical Concept*. Geneva, Switzerland: International Organization for Standardization, 1996.

International Organization for Standardization/International Electrotechnical Commission. ISO/IEC 10536-1. *Identification Cards—Contactless Integrated Circuit(s) Cards—Close-Coupled Cards—Part 1: Physical Characteristics*. Geneva, Switzerland: International Electrotechnical Commission, 2000.

———. ISO/IEC 14443-1. *Identification Cards—Contactless Integrated Circuit(s) Cards—Proximity Card—Part 1: Physical Characteristics*. Geneva, Switzerland: International Electrotechnical Commission, 2008.

———. ISO/IEC 15693-1. *Identification Cards—Contactless Integrated Circuit(s) Cards—Vicinity Cards—Part 1: Physical Characteristics*. Geneva, Switzerland: International Electrotechnical Commission, 2010.

———. ISO/IEC18046-1. *Information Technology—Automatic Identification and Data Capture Techniques—Radio Frequency Identification Device Performance Test Methods for System Performance*. Geneva, Switzerland: International Electrotechnical Commission, 2011.

———. ISO/IEC18046-2. *Information Technology—Automatic Identification and Data Capture Techniques—Radio Frequency Identification Device Performance Test Methods for Interrogator Performance*. Geneva, Switzerland: International Electrotechnical Commission, 2011.

———. ISO/IEC18046-3. *Information Technology—Automatic Identification and Data Capture Techniques—Radio Frequency Identification Device Performance Test Methods for Tag Performance*. Geneva, Switzerland: International Electrotechnical Commission, 2007.

———. 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*. Geneva, Switzerland: International Electrotechnical Commission, 2011.

National Fire Protection Association. NFPA 80. *Standard for Fire Doors and Other Opening Protectives*. Quincy, MA: National Fire Protection Association, 2010.

Chapter 4: Access Control Systems (ACS), continued

———. NFPA 101®. *Life Safety Code®*, 2012 ed. Quincy, MA: National Fire Protection Association, 2012.

———. NFPA 72®. *National Fire Alarm and Signaling Code*. Quincy, MA: National Fire Protection Association, 2010.

———. NFPA 730. *Guide for Premises Security*. Quincy, MA: National Fire Protection Association, 2011.

———. NFPA 731. *Standard for the Installation of Electronic Premises Security Systems*. Quincy, MA: National Fire Protection Association, 2011.

Underwriters Laboratories Inc.® UL 1034. *Burglary-Resistant Electric Locking Mechanisms*. Northbrook, IL: Underwriters Laboratories Inc., 2011.

International Code Council. *2012 International Building Code ®*. Washington, DC: International Code Council, 2012.

Chapter 5: Video Surveillance Systems (VSS)

American National Standards Institute/Security Industry Association. ANSI/SIA OSIPS-01:2008. *Open Systems Integration and Performance Standards—Framework*. Alexandria, VA: Security Industry Association, 2008.

BICSI.® *Telecommunications Distribution Methods Manual*, 12th ed. Tampa, FL: BICSI, 2009.

———. *Information Transport Systems Installation Methods Manual*, 6th ed. Tampa, FL: BICSI, 2010.

———. *Wireless Design Reference Manual*, 3rd ed. Tampa, FL: BICSI, 2008.

Electronic Industries Alliance. EIA Standard RS-232-C. *Interface Between Data Terminal Equipment and Data Communication Equipment Employing Serial Data Interchange.* Arlington, VA: Electronics Industries Alliance, 1969.

Institute of Electrical and Electronics Engineers, Inc.® IEEE 802.1X. *IEEE Standard for Local and Metropolitan Area Networks—Port-Based Network Access Control*. Piscataway, NJ: Institute of Electrical and Electronics Engineers, Inc., 2010.

———. IEEE 802.3at. *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements—Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications—Amendment 3: Data Terminal Equipment (DTE) Power via the Media Dependent Interface (MDI) Enhancements*. Piscataway, NJ: Institute of Electrical and Electronics Engineers, Inc., 2009.

International Organization for Standardization. ISO 12233. *Photography—Electronic Still-Picture Cameras—Resolution Measurements*. Geneva, Switzerland: International Organization for Standardization, 2000.

International Organization for Standardization/International Electrotechnical Commission, ISO/IEC 14496-10:2010. *Information Technology—Coding of Audio-Visual Objects—Part 10: Advanced Video Coding.* Geneva, Switzerland: International Electrotechnical Commission, 2010.

Chapter 5: Video Surveillance Systems (VSS), continued

———. ISO/IEC 15938-7:2003 +A6 2011. *Information Technology—Multimedia Content Description Interface—Part 7: Conformance Testing*. Geneva, Switzerland: International Electrotechnical Commission, 2003.

Underwriters Laboratories Inc.® UL 2044. *Standard for Commercial Closed-Circuit Television Equipment.* Northbrook, IL: Underwriters Laboratories Inc., 2008.

Chapter 6: Intrusion Detection Systems (IDS)

Institute of Electrical and Electronics Engineers, Inc.® IEEE 802.11. *IEEE Approved Draft Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*. Piscataway, NJ: Institute of Electrical and Electronics Engineers, Inc., 2012.

May, Timothy N. "Resistor Color Code Chart." Boulder, CO: University of Colorado Boulder, 2012.

National Fire Protection Association. NFPA 70. *2011 National Electrical Code®*. Quincy, MA: National Fire Protection Association, 2011.

Chapter 7: Fire Detection and Alarm Systems

American National Standards Institute. ANSI S3.41. *Audible Emergency Evacuation Signal*. Washington, DC: American National Standards Institute, 1990 (R2008).

BICSI®. *Telecommunications Distribution Methods Manual*, 12th ed. Tampa, FL: BICSI, 2009.

International Code Council. *2012 International Fire Code®*. Washington, DC: International Code Council, 2012.

International Electrotechnical Commission. IEC 60849. *Sound Systems for Emergency Purposes*, 2nd ed. Geneva, Switzerland: International Electrotechnical Commission, 1998 (R2001).

National Fire Protection Association. NFPA 1. *Uniform Fire Code*. Quincy, MA: National Fire Protection Association, 2012.

———. NFPA 13. *Standard for the Installation of Sprinkler Systems.* Quincy, MA: National Fire Protection Association, 2010.

———. NFPA 70®. *2011 National Electrical Code®*. Quincy, MA: National Fire Protection Association, 2011.

———. NFPA 72®. *National Fire Alarm and Signaling Code*. Quincy, MA: National Fire Protection Association, 2010.

Security Industry Association. SIA DC-05-1999.09. *Digital Communication Standard—Ademco® Contact ID Protocol—for Alarm System Communications*. Alexandria, VA: Security Industry Association, 1999.

Chapter 7: Fire Detection and Alarm Systems, continued

Underwriters Laboratories Inc.® UL 827. *Standard for Central-Station Alarm Services*. Northbrook, IL: Underwriters Laboratories Inc., 2008.

United States Department of Justice. Disability Section. PL 101-336. *Americans with Disabilities Act of 1990*. Washington, DC: United States Department of Justice, 1990.

Chapter 8: Notification, Communication, and Display Devices

American National Standards Institute/Telecommunications Industry Association/Electronic Industries Alliance. ANSI/TIA/EIA 606-A. *Administration Standard for Commercial Telecommunications Infrastructure.* Arlington, VA: Telecommunications Industry Association, 2002 +A1: 2008.

Ballou, Glen M. *Handbook for Sound Engineers*. Carmel, IN: Howard W. Sams & Co., 1987.

Benson, K. Blair. *Audio Engineering Handbook*. New York: McGraw-Hill Book Co., 1988.

BICSI®/InfoComm International®. *AV Design Reference Manual*, 1st ed. Tampa, FL: BICSI, 2006.

Bogen Communications, Inc. *Loudspeaker Installation Methods and Connection Techniques*. Ramsey, NJ: Bogen Communications, Inc., 1988.

Crowhurst, Norman H. *Practical PA Guidebook*. New York: John F. Rider Publisher, 1967.

Davis, Don, and Carolyn Davis. *Sound System Engineering*. Indianapolis: Howard W. Sams & Co., 1975.

Executone Information Systems. *Sound Paging System Design & Configuration*. Darien, CT: Executone, 1985.

Federal Communications Commission. *Code of Federal Regulations*, Title 47, Telecommunication, Part 68: Connection of Terminal Equipment to the Telephone Network. Revised October 1, 2007.

Giddings, Philip. *Audio System Design & Installation*. Carmel, IN: Howard W. Sams & Co., 1990.

International Electrotechnical Commission. IEC 60849. *Sound Systems for Emergency Purposes*, 2nd ed. Geneva, Switzerland: International Electrotechnical Commission, 1998 (R2001).

National Fire Protection Association. NFPA 70®. *2011 National Electrical Code®*. Quincy, MA: National Fire Protection Association, 2011.

———. NFPA 72®. *National Fire Alarm and Signaling Code*. Quincy, MA: National Fire Protection Association, 2010.

Sands, Leo G. *Sound System Installers*. Carmel, IN: Howard W. Sams & Co., 1962.

Underwriters Laboratories Inc.® UL 60950. *Safety of Information Technology Equipment,* 3rd ed. Northbrook, IL: Underwriters Laboratories Inc., 2000.

———. UL 864. *Control Units and Accessories for Fire Alarm Systems*, 9th ed. Northbrook, IL: Underwriters Laboratories Inc., 2011.

 © 2012 BICSI®

Chapter 9: Special Systems

United States Department of Justice. Disability Section. PL 101-336. *Americans with Disabilities Act of 1990*. Washington, DC: United States Department of Justice, 1990.

Austrian Electrotechnical Association. DIN VDE 0834. *Call Systems in Hospitals, Nursing Homes and Similar Institutions.* Berlin: VDE-VERLAG GmbH, 2000.

Checkpoint Systems, Inc. Web site. www.checkpointsystems.com (accessed March 14, 2012).

International Code Council. *2012 International Building Code®*. Washington, DC: International Code Council, 2012.

International Maritime Organization. Web site. www.imo.org (accessed March 14, 2012).

Lloyd, Alan. "Accounting for Staff Following an Evacuation." Web article. Continuity Central. www.continuitycentral.com/evacuation.pdf (accessed March 19, 2012).

Loss Prevention Magazine. Web site. www.lpportal.com (accessed March 14, 2012).

National Electrical Manufacturers Association. *NEMA Installation Guide for Nurse Call Systems* (R2007). Rosslyn, VA: National Electrical Manufacturers Association, 2007.

National Fire Protection Association. NFPA 70. *2011 National Electrical Code®*. Quincy, MA: National Fire Protection Association, 2011.

———. NFPA 99. *Health Care Facilities Code*, 2012 ed. Quincy, MA: National Fire Protection Association, 2012.

———. NFPA 101®. *Life Safety Code®*, 2012 ed. Quincy, MA: National Fire Protection Association, 2012.

The American Institute of Architects. *Guidelines for Design and Construction of Health Care Facilities*, 2006 ed. Washington, DC: American Institute of Architects Press, 2006.

Underwriters Laboratories Inc.® UL 1069. *Standard for Hospital Signaling and Nurse Call Equipment.* Northbrook, IL: Underwriters Laboratories Inc., 2001.

Chapter 10: Network Concepts

Information Security Forum. *2011 Standard of Good Practice for Information Security*. Web site. www.securityforum.org (accessed March 16, 2012).

Institute of Electrical and Electronics Engineers, Inc.® IEEE 802.1X. *IEEE Standard for Local and Metropolitan Area Networks—Port-Based Network Access Control.* Piscataway, NJ: Institute of Electrical and Electronics Engineers, Inc., 2010.

International Organization for Standardization/International Electrotechnical Commission. ISO/IEC 27001. *Information Technology—Security Techniques—Information Security Management Systems—Requirements.* Geneva, Switzerland: International Electrotechnical Commission, 2005.

———. ISO/IEC 27002. *Information Technology—Security Techniques—Code of Practice for Information Security Management*. Geneva, Switzerland: International Electrotechnical Commission, 2005.

Chapter 10: Network Concepts, continued

National Security Agency. *Securing Supervisory Control and Data Acquisition (SCADA) and Control Systems (CS)*. Web site. http://www.nsa.gov/ia/_files/factsheets/scada_factsheet.pdf (accessed March 16, 2012).

ASIS International. *Protection of Assets Manual*. Alexandria, VA: ASIS International, 2004.

Austrian Electrotechnical Association. DIN VDE 0834. *Call Systems in Hospitals, Nursing Homes and Similar Institutions*. Berlin: VDE-VERLAG GmbH, 2000.

BICSI®. *Network Design Reference Manual*, 7th ed. Tampa, FL: BICSI, 2009.

———. *Telecommunications Distribution Methods Manual*, 12th ed. Tampa, FL: BICSI, 2009.

Institute of Electrical and Electronics Engineers, Inc.® IEEE 802.3. *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements—Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications*. Piscataway, NJ: Institute of Electrical and Electronics Engineers, Inc., 2008.

———. IEEE 802.11. *IEEE Approved Draft Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*. Piscataway, NJ: Institute of Electrical and Electronics Engineers, Inc., 2012.

———. IEEE 802.11a. *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: High-Speed Physical Layer in the 5 GHz Band*. Piscataway, NJ: Institute of Electrical and Electronics Engineers, Inc., 1999.

———. IEEE 802.11b. *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems—Local and Metropolitan Area Networks—Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band*. Piscataway, NJ: Institute of Electrical and Electronics Engineers, Inc., 1999.

Appendix B: Legal Aspects of Electronic Safety and Security (ESS) Design

Agostini, John. "Legal Aspects and Risk Management of Design/Build Contracts." Web article. a/e ProNet, 1996. www.aepronet.org/Practice Notes/PN - Vol. 9, No. 1. May, 1996 - Legal Aspects and Risk Management of Design-Build Contracts.pdf (accessed March 16, 2012).

Dixon, Sheila A., ed. *Lessons in Professional Liability: DPIC's Loss Prevention Handbook for Design Professionals*. Monterey, CA: DPIC Companies, 1994.

Gumbiner, Kenneth J. "Alternative Dispute Resolution: There is a Better Way." Web article. a/e ProNet, 1995. www.aepronet.org/pn/vol8-no1.html (accessed March 16, 2012).

Index

A

acceptance testing 12-14
access control
  access level matrix 4-61
  application 4-4
  asset 4-60
  definition 1-5
  integration 4-59, 4-69, 11-10
  list. 10-41
  occupants 4-59
  operation matrix 12-6
  purpose. 4-1
  software 4-9
access control system
  backup power. 4-10
  biometrics. 4-52
  central equipment. 4-8
  controller 4-13, 4-45
  data entry 4-73
  database 4-67
  event recording 4-8
  failure. 4-64
  integration 4-69, 11-9
  IP based 10-15
  key performance indicators 12-8
  layout. 11-10
  levels 4-7
  notification. 4-65
  peripheral devices 4-15
  programming 4-70
  readers 4-45
  server 4-8
  structure 4-7
  user training 4-76
  verification testing 4-74
  video surveillance 5-3
  visitor management 4-12
  workstations. 4-11
ACL. . . . . .*See* access control, list
ACS. . . . . *See* access control system
air-sampling fire detection system. 7-18
alarm
  IP communicator system 7-67
  transmission equipment 7-8
analog
  communications. 4-66
  input 8-11
  recording 5-60
  to digital. 5-45
  video camera 5-12
  video system 5-8
annunciator
  intrusion detection 6-9
  panel, nurse call 9-8
  remote control, fire. 7-59
application service provider 5-76
ASP . . . . . *See* application service provider
assessment
  security. 2-3
  site 3-8
  threat 3-6
asset
  definition 2-1, 4-60
  identification 2-3
  management system. 9-12
at-risk human perimeter system 9-11
audibility
  notification appliance. 7-42
  paging system 8-9

B

badging system 4-11
balanced twisted pair. 5-48
bandwidth. 10-8
bar code card 4-50
BAS. . . . . *See* building automation system
bell. 7-36
bidding
  documents 3-39
  preparation 3-31
  process 3-32
biometric
  access control system. 4-52
  performance parameters. 4-57
  privacy 4-58
bonding. 3-15, 5-87
building automation system
  integration 11-14
  layout 11-16
burn-in period 12-15
buzzer 6-23

C

CA. . . . . .*See* construction, administration
cable
  balanced twisted-pair. 5-48
  coaxial 5-43
  optical fiber 4-66, 5-48
CAD . . . . . *See* computer-aided design
CAFM. . . . . .*See* computer-aided facility management
calibration 12-14
camera
  analog. 5-12
  film. 5-23
  image capture. 5-22
  infrared. 5-23
  IP video 5-14
  lenses 5-28

mounts 5-34
thermal 5-23
card
bar code 4-50
format 4-51
IP reader 4-45
magnetic stripe 4-50
personal identification verification 4-46
proximity 4-49
smart 4-48
Wiegand 4-50
CD . . . . . *See* document, construction
central station service 7-5
chime 7-37
coaxial cable 5-46
code
building 4-65
definition A-2
list of . . . . . Appendix A
scope of work 3-15
code call station 9-5
color rendition index 5-38
color temperature 5-36
commissioning
acceptance plan 12-14
cleaning 12-13
client staff training 12-16
documentation 12-12
labeling 12-13
system testing 12-14
communication
analog 4-66
audio systems 8-1
emergency telephone 8-5
intercom 8-3
internet protocol 6-5
IP voice system 10-19
public address 8-6
serial 4-66
telephony 6-5
telephony, cellular 6-6
wireless 6-6
compression technology 5-18
computer-aided design 3-22
computer-aided facility management 3-47
construction
administration 3-41
document 3-26
manager 3-43, 3-47
phase 3-41
submittals 3-41
team 3-43, 3-46
contact, door 4-19
contract
design bid build 3-37
design build 3-38
document 3-26
service 12-9
system maintenance 13-2
types 3-36
control trim 4-38
controller
access 4-13
coordination, design 3-23
cost
estimate 3-18
projection 3-25
credential
access control 4-7
card 4-46
privacy 4-58
radio frequency identification 4-46
CRI . . . . . *See* color rendition index

D

DACR . . . . . *See* digital alarm, communicator receiver
DACS . . . . . *See* digital alarm, communicator system
DARR . . . . . *See* digital alarm, radio receiver
DART . . . . . *See* digital alarm, radio transmitter
data mining 5-57
database
access control 4-67
conversion 4-61, 4-72
facility management 3-47
integration 11-18
software 11-18
DD . . . . . *See* design development
denial of service 10-33
design
approach 2-6
architecture & engineering 3-2
coordination 3-23
elements 3-12
final 3-31
fundamentals 1-5
implementation review 3-42
preliminary documents 3-6
process 3-1
team 3-2, 3-12, 3-35, 3-43, 3-46
verification 3-24
design development
deliverables 3-24
overview 3-19
detector
beam 7-16
duct smoke 7-17
flame 7-27
gas 7-28
glass break 6-12
heat 7-21
ionization 7-12
motion 6-11, 6-18
outdoor motion 6-17
passive infrared motion 4-16, 6-11

 © 2012 BICSI®

photoelectric . . . 7-13
photoelectric beam . . . 6-18
smoke . . . 7-11
water flow . . . 7-32
window . . . 6-12
device
audible . . . 6-22
delayed egress . . . 4-39
door status monitoring . . . 6-15
end-of-line supervision . . . 6-26
initiation . . . 6-10, 7-10, 9-3
monitoring . . . 5-67
motion detection . . . 6-11
notification . . . 6-4, 6-21, 9-7
perimeter detection . . . 6-17
peripheral . . . 4-15
specialty detection . . . 6-20
video display . . . 8-11
visual . . . 6-23
window detection . . . 6-12
wireless . . . 6-24
digital
input . . . 8-11
recording . . . 5-62
video management system . . . 5-77
video matrix . . . 5-76
video recorder . . . 5-62
video recording . . . 5-61
digital alarm
communicator receiver . . . 7-66
communicator system . . . 7-61
communicator transmitter . . . 7-62
radio receiver . . . 7-66
radio transmitter . . . 7-65
transmission channels . . . 7-63
document
bid . . . 3-39
commissioning . . . 12-12
construction . . . 3-26
contract . . . 3-26
documentation . . . 3-15, 3-18, 12-12
drawings . . . 3-20
final acceptance . . . 3-25
final specifications . . . 3-27
forms . . . 3-44
preliminary design . . . 3-6
submittals . . . 3-44
door
closer . . . 4-3, 7-55
contact . . . 4-19
fire-rated . . . 4-30
hardware . . . 4-2
hardware, electrified . . . 4-21
hold-open . . . 4-42
loop . . . 4-40
operator . . . 4-44
release button . . . 4-16
revolving . . . 4-3, 4-42
status monitoring device . . . 6-15
DoS . . . *See* denial of service
drawings
computer-aided facility management . . . 3-47
overview . . . 3-20
set systems . . . 3-21
DVMS . . . *See* digital, video management system
DVR . . . *See* digital, video recorder

E

electronic safety and security
commissioning . . . 12-12
components . . . 11-9
design fundamentals . . . 1-5
design process . . . 3-1
integration . . . 11-2
integration process . . . 11-22
knowledge areas . . . 1-3
operation . . . 12-2
supporting networks . . . 10-2
emergency response category . . . 12-10
encryption . . . 10-43
equipment
alarm transmission . . . 7-8
central, nurse call . . . 9-7
central processing . . . 4-8
ESS . . . *See* electronic safety and security
event recording . . . 4-8

F

FA . . . *See* fire alarm
FACP . . . *See* fire alarm, control unit
fail latched . . . 4-22
fail safe . . . 4-22
fail secure . . . 4-22
fire alarm
central station service . . . 7-5
classes . . . 7-3
control unit . . . 7-52
fire service box . . . 7-9
initiation device . . . 7-10
monitoring . . . 7-3
notification . . . 7-35
notification appliance circuits and pathways . . . 7-50
overview . . . 7-1
supervision . . . 7-55
trouble conditions . . . 7-56
fire alarm control unit
addressable . . . 7-54
central control panel . . . 7-52
zoned system . . . 7-53
fire alarm system
input/outputs . . . 7-57
IP hybrid . . . 10-25

proprietary supervising station system 7-7
protect premises 7-3
public reporting 7-8
remote supervising station system 7-7
supervising station 7-4
fire detection system
air-sampling 7-18
flame detector 7-27
gas detector 7-28
heat detector 7-21
pull station 7-31
fire suppression system
dry system 7-34
monitoring device 7-32
wet system 7-32
firewall 10-36
forms 3-44
frame rate 5-62
FSO . . . . . *See* wireless, free space optics

G

grounding (earthing) 3-15, 5-87

H

hardware
computer 4-9
control system 5-76
door 4-2
electrified door 4-21
electrified exit 4-18
fire rated 4-30
heat detector
combination 7-25
fixed temperature spot 7-22
rate-compensated 7-26
rate-of-rise spot 7-24
horn 7-38

I

IDS . . . . . *See* intrusion detection system
image
camera capture 5-22
capture 5-11
format 5-20
processing 5-25
resolution chart 5-39
imager 5-20
infant abduction system 9-11
infrared
camera 5-23
illumination 5-38
passive motion detector 4-16
infrastructure
network 10-9
video system 5-85
initiation device 6-10, 7-10, 9-3
input/output matrix 11-19
integrated project delivery 3-38
integration . . . . . *See* system integration
intelligibility
notification appliance 7-44
paging system 8-10
intercom 8-3
interlock 4-44
Internet protocol
access control system 10-15
addressable speaker paging system 8-7
alarm communicator system 7-67
card reader 4-45
communication 6-5
controller 4-45
ESS systems 10-2
fire alarm system, hybrid 10-25
intercom system 8-4
intrusion detection system, hybrid 10-27
network architecture 10-10
nurse call system, hybrid 10-29
paging system, end-to-end 10-21
paging system, hybrid 10-22
video camera 5-14
video deployment 5-53
video encoder 5-17
video surveillance system 10-17
video system 5-8
voice communication system 10-19
interoperability
access control 4-59
intrusion detection 6-24
video system 5-88
intrusion detection
definition 1-5
principles 6-2
intrusion detection system
annunciator 6-9
cabling 6-25
control panel 6-7
detection device 6-11
devices and sensors 11-11
digital alarm communicator system 7-61
emergency response category 12-10
end-of-line supervision 6-26
initiating device 6-10
integrated equipment 6-24
integration 11-9
Internet protocol technology 6-5
IP hybrid 10-27
keypads 6-9
network 10-41
notification device 6-21
wireless device 6-24
IP . . . . . *See* Internet protocol
IPS . . . . . *See* network, intrusion prevention system

 © 2012 BICSI®

K

key performance indicator 12-4, 12-8
keypad 6-9
KPI . . . . . *See* key performance indicator

L

labeling 12-13
latch guard 4-42
layering 2-8
layout
  access control system 11-10
  building automation system 11-16
  fire alarm system, IP hybrid 10-26
  intrusion detection system, IP hybrid 10-28
  nurse call system, IP hybrid 10-30
  paging system, end-to-end IP 10-21
  paging system, IP hybrid 10-22
  physical security information management system . . . 11-13
  video surveillance system 5-69
lenses 5-28
liability 5-4, B-1
license plate capture 5-22
lighting
  color rendition index 5-38
  color temperature 5-36
  infrared 5-38
  luminance 5-35
link loss budget 5-51
lock
  electric latch 4-36
  electric lockset 4-36
  electric strike 4-32
  electric bolt 4-37
  control trim 4-38
  functions 4-31
  types 4-31
  magnetic 4-34
  mortise 4-16
LPC . . . . . *See* license plate capture
luminance . . . . . *See* lighting

M

maintenance plan 12-5
management
  asset 9-12
  computer-aided facility 3-47
  network 10-7
  physical security information 11-11
  risk 11-24
  video system 5-77, 5-90
  visitor 4-12
mantrap . . . . . *See* interlock
matrix
  access control operation 12-6
  access level 4-61
  digital video 5-76
  emergency response category 12-10
  input/output 11-19
  responsibility 3-3
  service arrangement 12-2
  surveillance switch 5-56
  video surveillance operation 12-7
  video surveillance switch 5-56
metal oxide varistor 4-30
monitor
  devices 5-67
  fire 7-3
  location 5-68
motion detector 4-16, 6-11, 6-17, 6-18

N

NAC . . . . . *See* notification appliance, circuit
network
  access control system, IP 10-15
  administration 10-7
  architecture 10-10
  awareness training 10-44
  bandwidth 10-8
  control measures 10-36
  denial of service 10-33
  encryption 10-43
  fire alarm system, hybrid IP 10-25
  firewall 10-36
  infrastructure 10-9
  intrusion detection system 10-41
  intrusion detection system, hybrid IP 10-27
  intrusion prevention system 10-41
  management 10-7
  nurse call system, hybrid IP 10-29
  risk 10-33
  security recommendations 10-45
  security trends 10-47
  security zones 10-40
  segregation 10-44
  support 10-2
  switch 5-54
  video camera 5-91
  video recorder 5-62
  video surveillance system, IP 10-17
  voice communication, IP 10-19
noise masking system 8-10
notification
  access control 4-65
  device 8-1, 9-7
notification appliance
  audibility 7-42
  bell 7-36

chime 7-37
circuit 7-50
horn 7-38
intelligibility 7-44
performance factors 7-42
speaker 7-39
strobe 7-41
visibility 7-44
nurse call system
annunciator panel 9-8
code call station 9-5
components 9-3
hybrid IP 10-29
initiation devices 9-3
notification devices 9-7
overview 9-1
system wiring 9-9
types 9-1
wireless 9-8
NVR . . . . . *See* network, video recorder

O

Open Systems Interconnection 10-11
optical fiber
extended distances 4-66
link loss budget 5-51
video systems 5-48
OSI . . . . . *See* Open Systems Interconnection
outdoor motion detector 6-17

P

PA . . . . . *See* public address
paging system
audibility 8-9
centrally amplified 8-7
distributed amplified 8-8
IP hybrid 10-22
intelligibility 8-10
IP addressable speaker system 8-7
IP end-to-end 10-20
pan, tilt, zoom 5-11
panel
control, intrusion detection 5-7
control, fire alarm 7-52
annunciator, nurse call 9-8
panic bar 4-17
passive infrared 4-16, 6-11
passive magnetic field sensor 6-19
perimeter detection device 6-17
peripherals
access control 4-15
network 10-4
personal identification verification 4-46
photoelectric beam detector 6-18
physical security information management 11-11
PIR . . . . . *See* passive infrared
PIV . . . . . *See* personal identification verification
PoE . . . . . *See* power over Ethernet
power
alternate 5-87
backup 4-10
central control panel 7-57
distribution 4-23, 5-86
locking options 4-28
source 5-86
standby 6-7, 7-57
transfer device 4-40
power over Ethernet
network infrastructure 10-9
reader, access control 4-45
video camera 5-14
pressure switch 7-34
privacy
biometric 4-58
credential 4-46
video surveillance 5-4
project
integrated delivery 3-38
requirements 3-5
types 3-3
protected premises system 7-3
proximity card 4-49
PSIM . . . . . *See* physical security information management
PTZ . . . . . *See* pan, tilt, and zoom
public address 8-6
pull station 7-31

Q

quality of service 10-8

R

radar sensor 6-20
radio frequency identification
access control 4-46
asset management 9-12
human perimeter systems 9-11
retail tagging 9-12
system 9-10
readers
card, IP 4-45
hoteling 4-45
web-enabled 4-45
recorder
digital video 5-62
frame rate 5-62
network video 5-62
recording
analog 5-60
digital 5-61
event 4-8
relay 4-29
reliability 10-5, 11-18

 © 2012 BICSI®

request for information 3-42
request for proposal. 3-35
request to exit 4-15
resolution chart 5-39
responsibility matrix 3-3
retail tagging 9-12
REX. . . . . *See* request to exit
RFI . . . . . *See* request for information
RFID . . . . . *See* radio frequency identification
RFP . . . . . *See* request for proposal
risk
  definition 2-3
  formula. 2-2
  management. 11-24
  network 10-33

S

SaaS. . . . . *See* software as a service
schematic design 3-5
scope of work 3-13
SD . . . . . *See* schematic design
security
  assessment 2-3
  clearance 3-17
  consultant. 2-9
  definition 2-2
  design approach 2-6
  designer 2-10
  information and event management. 10-44
  installer. 2-11
  layering 2-8
  network control measures 10-36
  network recommendations. 10-45
  network zones 10-40
  physical 1-4, 1-7
  principles of 2-1
  program 2-6
  screen 6-14
  trends 1-7, 10-47
sensor
  detection. 6-3
  electric field 6-19
  microphonic 6-19
  optical fiber cable. 6-19
  passive magnetic field 6-19
  radar 6-20
  shock 6-13
service arrangement matrix. 12-2
service contract 12-9
SIEM. . . . . *See* security information and event management
siren. 6-22
site survey 3-8
smart card 4-48
smoke detector
  beam 7-16
  coverage area 7-29
  duct 7-17
  ionization. 7-12
  photoelectric. 7-13
  purpose. 7-11
software
  access control. 4-9
  database 11-18
  patching 10-43
software as a service 5-76
SoW. . . . . *See* scope of work
speakers. 6-23, 7-39, 8-7
standby power 6-7, 7-57
station
  central service 7-5
  code call. 9-5
  proprietary supervising system 7-7
  pull station 7-31
  remote supervising system. 7-7
  supervising station 7-4
  work 4-11
strobe. 6-23, 7-41
submittals 3-44
supervised care elopement prevention 9-11
supervising station system
  central station. 7-5
  proprietary 7-7
  remote 7-7
surveillance . . . . . *See* video surveillance
switch
  key 4-17
  network 5-54
  magnetic. 6-14
  magnetic, balanced. 6-17
  valve tamper. 7-33
  pressure 7-34
system
  access control. 4-1, 10-15
  administrators. 4-77
  air-sampling fire detection 7-18
  analog video. 5-8
  asset management 9-12
  at-risk human perimeter 9-11
  badging. 4-11
  building automation. 11-14
  control 10-34
  digital alarm communicator. 7-61
  digital video management 5-77
  expandability 11-19
  fire alarm 7-3, 10-25
  fire detection 7-18
  fire suppression 7-32
  human perimeter 9-11
  infant abduction 9-11
  intrusion detection 6-1, 10-27, 10-41
  intrusion prevention 10-41
  IP addressable speaker. 8-7

IP communicator alarm 7-67
maintenance 12-5
noise masking 8-10
nurse call 9-1, 9-8, 10-29
operation 12-2
operator 4-77
paging. 8-7
proprietary supervising station 7-7
protected premises 7-3
radio frequency identification 9-10
remote supervising station 7-7
supervising station 7-5
testing 12-14
training, access control 4-76
video surveillance 5-1, 10-17
voice communication 10-19
zoned 7-53
system integration
access control system. 4-59, 4-69, 11-10
building automation system 11-14
database 11-18
features. 11-2
fundamentals 11-7
input/output matrix 11-19
integrator 2-11
intrusion detection system 11-9
physical security information management 11-11
process 11-21
risk management 11-24
software 11-17
trends 1-7
user training 11-3
video surveillance system 11-11

T

telephony. 6-5
temperature
classification, heat-sensing fire detector 7-23
color 5-36
testing
acceptance 12-14
scope of work. 3-15
system 12-14
verification, access control system. 4-74
threat
assessment 3-6
categories 2-5
definition 2-3
identification 2-3
insider threat. 10-35
training
awareness 10-44
client staff. 12-16
user, access control system 4-76
user, integrated system. 11-3
transponder 7-4, 9-10
turnstile 4-3, 4-43

U

uninterruptible power supply 4-10, 5-87, 6-9. 10-9
UPS . . . . . *See* uninterruptible power supply

V

vane 7-32
video
analytics 5-57
digital management system 5-77
display device 8-11
lighting 5-35
motion detection 5-26
multichannel encoder. 5-91
over Internet protocol 5-91
processing 5-56
recorder 5-62
resolution 5-39
source 5-11
storage design 5-64
transmission 5-43
video surveillance
components 5-7
definition 1-5
function 5-3
IP system 10-17
matrix switch 5-56, 5-76
operation matrix. 12-7
privacy 5-4
system integration 11-11
system layout 5-69
trends 1-7
video system
infrastructure 5-85
interoperability. 5-88
management. 5-77, 5-80
selection 5-78
visitor management 4-12
VMD . . . . . *See* video, motion detection
voice communication system 10-19
vulnerability
model 2-4
scanner 10-42

 © 2012 BICSI®

W

warranty period 12-16
wireless
  communication 6-6
  device 6-24
  free space optics 5-52
  intercom 8-4
  nurse call system 9-8
  transmission 5-52
workstations 4-11