STANDARDS

an American National Standard

ANSI/BICSI 005-2013

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

BICSI®

ANSI/BICSI 005-2013

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

Committee Approval: March 2013
First Published: May 2013

Approved American National Standard
ANSI

BICSI®
advancing information technology systems

BICSI Standards

BICSI standards contain information deemed to be of technical value to the industry and are published at the request of the originating committee. The BICSI International Standards Program has subjected this standard to a rigorous public review and resolution of comments, which is a procedural part of the development of a BICSI standard.

BICSI reviews standards within five years of its last approval date. As necessary, standards are reaffirmed, rescinded, or revised according to submitted updates and assessment of need.

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

Copyright

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

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

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

Violators may be prosecuted.

Published by:

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

All rights reserved
Printed in U.S.A.

Notice Of Disclaimer And Limitation Of Liability

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

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

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

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

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

TABLE OF CONTENTS

1 INTRODUCTION 1
1.1 GENERAL 1
1.2 PURPOSE 1
1.3 CATEGORIES OF CRITERIA 1
2 SCOPE 1
3 REQUIRED STANDARDS AND DOCUMENTS 2
4 DEFINITIONS, ACRONYMS, ABBREVIATIONS, AND UNITS OF MEASUREMENT 4
4.1 DEFINITIONS 4
4.2 ACRONYMS AND ABBREVIATIONS 7
4.3 UNITS OF MEASUREMENT 8
5 TELECOMMUNICATIONS INFRASTRUCTURE 9
5.1 OVERVIEW 9
5.2 TOPOLOGY 9
5.2.1 Backbone and Horizontal Cabling 9
5.2.2 Other Applications and Media 9
5.3 SPACES 10
5.3.1 Equipment Rooms 10
5.3.2 Telecommunications Rooms and Telecommunications Enclosures 11
5.4 CABLING 13
5.4.1 Backbone Cabling 13
5.4.2 Horizontal Cabling 13
5.4.3 Horizontal Connection Point (HCP) 17
5.4.4 Power over Ethernet (PoE) 18
5.5 CABLING PATHWAYS 18
5.5.1 Requirements 18
5.5.2 ESS Pathway Redundancy 18
5.5.3 ESS Pathways between Telecommunications Spaces within a Building 19
5.5.4 ESS Campus Pathways Between Buildings 19
5.5.5 ESS Pathways Serving Equipment Outlets 19
5.5.6 ESS Pathway Separation from Power and EMI Sources 19
5.5.7 ESS Pathway Bonding and Grounding 20
5.5.8 Special Pathways and Spaces Considerations 20
5.5.9 Secure Areas 21
5.5.10 Enclosures, Pull Boxes and Splice Boxes 21
5.5.11 High Security Areas 21
5.6 TELECOMMUNICATIONS OUTLET/CONNECTORS 21
5.6.1 Overview 21
5.6.2 Facility Connections by Direct Attach Method 22
5.7 CABLING INSTALLATION REQUIREMENTS 23
5.7.1 Overview 23
5.7.2 Bonding and Grounding Considerations 23
5.7.3 Transmission Performance Field Testing 23
5.8 ADMINISTRATION AND DOCUMENTATION 25
5.8.1 Requirements 25
5.8.2 Recommendations 25
5.9 ESS DEVICE MOUNTING HEIGHTS 25
5.9.1 Requirements 25
5.9.2 Recommendations 25

5.10 Infrastructure for Wireless Transmission 25
5.10.1 Requirements 25
5.10.2 Additional Information 25
5.11 Coverage area planning and density 26
5.11.1 Introduction 26
5.11.2 Recommendations 26
6 INTRUSION DETECTION 27
6.1 Overview 27
6.1.1 Requirements 27
6.1.2 Recommendations 27
6.2 Sensors 27
6.2.1 Recommendations 27
6.3 Notification 28
6.3.1 Requirements 28
6.3.2 Recommendations 28
6.3.3 Additional Information 28
6.4 Control Panel 28
6.4.1 Requirements 28
6.4.2 Recommendations 29
6.5 Keypads and Annunciators 29
6.5.1 Requirements 29
6.5.2 Recommendations 29
6.6 Initiating Devices 29
6.6.1 Overview 29
6.6.2 Motion Sensors 29
6.6.3 Window Sensors 29
6.6.4 Door Status Sensors 30
6.6.5 Perimeter Sensors 30
6.7 Optional Integrated Equipment 30
6.7.1 Introduction 30
7 VIDEO SURVEILLANCE 31
7.1 Overview 31
7.2 Generation and Conformance with Use Cases 31
7.2.1 Scene Characteristics 31
7.2.2 Observation as a Primary VSS Function 32
7.2.3 Forensic Review as a Primary VSS Function 32
7.2.4 Recognition as a Primary VSS Function 33
7.2.5 Additional VSS Functions 33
7.3 Device Groups and Interoperability 34
7.3.1 Requirements 34
7.4 Device Categories 34
7.4.1 Requirements 34
7.5 Use Cases 35
7.5.1 Requirements 35
7.6 Open Network Video Interface Forum (ONVIF) Conformance 35
7.6.1 Requirements 35
7.7 Deployment Process 35
7.7.1 Requirements 35
7.7.2 Recommendations 36
7.8 Authentication of Network Video Cameras for Improved ESS Network Security 36
7.8.1 Requirements 36

8 ACCESS CONTROL 37
8.1 OVERVIEW 37
8.2 SYSTEM STRUCTURE 37
8.2.1 Overview 37
8.2.2 Central Equipment Processing (Level 1) 37
8.2.3 Computer Hardware and Software 37
8.2.4 Server 37
8.2.5 Software 38
8.2.6 Backup 38
8.2.7 Event Recording 38
8.2.8 Backup Power 38
8.2.9 Access Control Workstation 38
8.2.10 Badging System 39
8.2.11 Visitor Management 39
8.3 CONTROLLERS FOR INTELLIGENT FIELD PROCESSING (LEVEL 2) 39
8.3.1 Overview 39
8.3.2 Controller Configurations 39
8.4 PERIPHERAL DEVICES (LEVEL 3) 40
8.4.1 Overview 40
8.4.2 Power Distribution 40
8.4.3 Relays 40
8.4.4 Readers 41
8.4.5 Request to Exit (REX) Devices 41
8.4.6 Door Contacts 41
8.4.7 Electrified Door Hardware 41
8.4.8 Fail-Secure/Fail-Safe/Fail Latched 41
8.4.9 Power to Locks 42
8.5 CREDENTIALS (LEVEL 4) 43
8.5.1 Overview 43
8.5.2 Web-Enabled Access Control 43
8.5.3 IP Card Readers 43
8.5.4 IP Controllers 43
8.5.5 Communications 43
8.5.6 Analog Communications 44
8.5.7 TCP/IP or Network Communications 44
9 FIRE DETECTION AND ALARM SYSTEMS 45
9.1 OVERVIEW 45
9.2 RISK ASSESSMENT AND SAFETY PROGRAMS 45
9.2.1 Requirements 45
9.2.2 Recommendations 45
9.2.3 Additional Information 45
9.3 CLASSES OF FIRE ALARM SYSTEMS 46
9.3.1 Introduction 46
9.3.2 Requirements 46
9.3.3 Recommendations 46
9.4 INITIATION DEVICES 46
9.4.1 Introduction 46
9.4.2 Requirements 46
9.4.3 Recommendations 46
9.5 FIRE SUPPRESSION SYSTEMS AND SUPERVISION DEVICES 47
9.5.1 Introduction 47
9.5.2 Requirements 47
9.5.3 Recommendations 47
9.6 NOTIFICATION APPLIANCES 47
9.6.1 Introduction 47
9.6.2 Requirements 47

9.7 TYPES OF NOTIFICATION APPLIANCES 47
9.7.1 Introduction 47
9.7.2 Requirements 47
9.7.3 Additional Information 47
9.8 NOTIFICATION APPLIANCE CIRCUIT (NAC) 48
9.8.1 Introduction 48
9.8.2 Requirements 48
9.8.3 Recommendations 48
9.8.4 Additional Information 48
9.9 AUDIBILITY 48
9.9.1 Introduction 48
9.9.2 Requirements 49
9.9.3 Additional Information 49
9.10 INTELLIGIBILITY 49
9.10.1 Overview 49
9.11 VISIBILITY 49
9.11.1 Overview 49
9.12 CONTROL UNITS 50
9.12.1 Introduction 50
9.12.2 Requirements 50
9.12.3 Additional Information 50
9.13 SUPERVISION 51
9.13.1 Requirements 51
9.13.2 Additional Information 51
9.14 TROUBLE CONDITIONS 51
9.14.1 Overview 51
9.15 POWER SUPPLIES 51
9.15.1 Requirements 51
9.16 TRANSMITTERS 52
9.16.1 Digital Alarm Communicator Transmitter (DACT) Dialers 52
9.16.2 Digital Alarm Radio Transmitter (DART) 52
9.16.3 IP Alarm Communicator System 52
9.17 AS-BUILT DRAWINGS AND RELATED DOCUMENTATION 52
9.17.1 Requirements 52
9.17.2 Recommendations 52
10 INTEGRATED SYSTEMS 53
10.1 OVERVIEW 53
10.2 ESS INTEGRATED SERVICES, DESIGN AND INTEGRATION 53
10.2.1 Public Network Services 53
10.2.2 Design and Selection of Components 54
10.2.3 ESS Integration 54
10.3 ESS COMPONENTS 54
10.3.1 Overview 54
10.3.2 Intrusion Detection System 54
10.3.3 Access Control System 55
10.3.4 Video Surveillance System 55
10.3.5 Physical Security Information Management (PSIM) System 55
10.3.6 Sensor-Based System 55
10.3.7 Building Automation System 55
10.3.8 Location System 57
10.3.9 Global Positioning System (GPS) 57
10.3.10 Software 57

10.4 SYSTEM CONFIGURATION AND EXPANDABILITY 58
10.4.1 Overview 58
10.4.2 Input/Output Matrix 58
10.4.3 Maps and Icons 59
10.4.4 System Response Times 59
10.4.5 System Expansion Capability 59
10.5 ELECTRONIC SAFETY AND SECURITY (ESS) INTEGRATION PROCESS 59
10.5.1 Overview 59
10.5.2 Integration Process Team Members 60
10.5.3 Integration Process 60
11 RISK MANAGEMENT AND RISK ASSESSMENT 65
11.1 INTRODUCTION 65
11.2 REQUIREMENTS 65
11.3 ADDITIONAL INFORMATION 65
APPENDIX A: CABLING PATHWAYS (NORMATIVE) 67
A.1 OVERVIEW 67
A.2 TYPES OF CABLING PATHWAYS 67
A.2.1 Introduction 67
A.2.2 Cable Tray Pathways 69
A.2.3 Non-continuous Pathways 70
A.2.4 Conduit Pathways 70
A.2.5 Surface-mounted Pathways (Perimeter Raceways) 72
A.2.6 Duct Raceway Pathways 73
A.2.7 Access Floor Raceway Pathways 73
A.2.8 In-floor System Pathways 74
A.2.9 Catenary Pathways 74
A.2.10 Utility Columns (Power Poles) 74
A.3 GENERAL INSTALLATION PRACTICES 75
A.3.1 Requirements 75
A.3.2 Recommendations 75
APPENDIX B: ELECTRONIC SAFETY AND SECURITY (ESS) DESIGN FUNDAMENTALS (INFORMATIVE) 77
B.1 INTRODUCTION 77
B.2 ELEMENTS 77
B.2.1 Access Control 77
B.2.2 Intrusion Detection 77
B.2.3 Surveillance 77
B.2.4 Fire Detection and Alarm 77
B.2.5 Integrated Systems 77
B.2.6 Special Systems 77
B.2.7 Network Security 78
B.3 TYPES OF PROJECTS 78
B.4 CURRENT AND FUTURE TRENDS IN SAFETY AND SECURITY 78
B.4.1 Information Technology 78
B.4.2 Physical Security 78
B.4.3 Integration of Access Control and Building Automation Systems 78
B.4.4 Surveillance 79
B.5 ELECTRONIC SAFETY AND SECURITY SYSTEM DEVELOPMENT BASICS 79
APPENDIX C: WIRELESS TRANSMISSION (INFORMATIVE) 81
C.1 OVERVIEW 81
C.2 RADIO FREQUENCY TRANSMISSION 81
C.2.1 Introduction 81
C.3 FREE SPACE OPTICS 81
C.3.1 Introduction 81

C.4 LICENSED MICROWAVE RADIO TRANSMISSION 81
C.4.1 Overview 81
C.5 FREQUENCY SELECTION 82
C.5.1 Introduction 82
APPENDIX D: RELATED DOCUMENTS (INFORMATIVE) 83

INDEX OF FIGURES

FIGURE 1: HIERARCHICAL STAR TOPOLOGY 9
FIGURE 2: EXAMPLES OF NON-STAR TOPOLOGIES 10
FIGURE 3: OPTICAL FIBER CABLING WITH MEDIA CONVERTERS 15
FIGURE 4: CONFIGURATION EXAMPLES FOR USING HYBRID COPPER/OPTICAL FIBER CABLE TO CONNECT AN ESS DEVICE 16
FIGURE 5: EXAMPLE OF A HORIZONTAL CONNECTION POINT WITHIN A STAR TOPOLOGY 17
FIGURE 6: EXAMPLE LOCATIONS OF USER-ADMINISTERED AND FACILITY CONNECTION TELECOMMUNICATIONS OUTLETS 22
FIGURE 7: EXAMPLES OF FACILITY CONNECTIONS USING DIRECT ATTACH 22
FIGURE 8: CONFIGURATION 1: SINGLE CONNECTOR MODIFIED PERMANENT LINK SET UP FOR DIRECT ATTACH WITHOUT A CONSOLIDATION POINT 24
FIGURE 9: CONFIGURATION 2: SINGLE CONNECTOR MODIFIED PERMANENT LINK SET UP FOR DIRECT ATTACH WITH A CONSOLIDATION POINT 24
FIGURE 10: FORM A, B AND C RELAYS 40
FIGURE 11: SAMPLE PHYSICAL SECURITY INFORMATION MANAGEMENT SYSTEM 56

INDEX OF TABLES

TABLE 1: RECOMMENDED CROSS-CONNECT COLOR CODES FOR USE AT CABLING DISTRIBUTORS 11
TABLE 2: MEDIA SELECTION CRITERIA 14
TABLE 3: BALANCED TWISTED-PAIR CABLING FREQUENCY RANGE OF INTEREST AND ASSOCIATED APPLICATIONS 15
TABLE 4: TYPICAL COVERAGE AREA FOR EACH ESS LINK 26
TABLE 5: DETECTION SENSOR TECHNOLOGY AND APPLICATION 27
TABLE 6: NAC DESIGNATION REQUIREMENTS 48
TABLE 7: TYPICAL AMBIENT SOUND LEVELS BY LOCATION 49
TABLE A1: BALANCED TWISTED-PAIR CABLING BEND RADIUS AND PULLING TENSION REQUIREMENTS 68
TABLE A2: OPTICAL FIBER CABLING BEND RADIUS AND PULLING TENSION REQUIREMENTS 68
TABLE A3: MAXIMUM ALLOWABLE CABLING STACKING HEIGHT IN CABLING PATHWAYS 69