Contents

Foreword **9**

Introduction **11**

1 Scope **13**

2 Purpose **13**

3 General Terms and Definitions **14**

3.1 Definitions 14
3.2 Acronyms 18
3.3 Sources for Definitions and Abbreviations 20

4 Overview **21**

5 Authentication and Authorization Technologies **22**

5.1 Role-Based Authorization Tools 23
5.2 Password Authentication 25
5.3 Challenge/Response Authentication 29
5.4 Physical/Token Authentication 30
5.5 Smart Card Authentication 32
5.6 Biometric Authentication 34
5.7 Location-Based Authentication 36
5.8 Password Distribution and Management Technologies 37
5.9 Device-to-Device Authentication 40

6 Filtering/Blocking/Access Control Technologies **41**

6.1 Network Firewalls 42
6.2 Host-based Firewalls 46
6.3 Virtual Networks 49

7 Encryption Technologies and Data Validation **50**

7.1 Symmetric (Secret) Key Encryption 51
7.2 Public Key Encryption and Key Distribution 56

Copyright 2007 ISA. All rights reserved.

7.3 Virtual Private Networks (VPNs) 59

8 Management, Audit, Measurement, Monitoring, and Detection Tools 63

8.1 Log Auditing Utilities 64
8.2 Virus and Malicious Code Detection Systems 66
8.3 Intrusion Detection Systems 69
8.4 Vulnerability Scanners 73
8.5 Forensics and Analysis Tools (FAT) 76
8.6 Host Configuration Management Tools 79
8.7 Automated Software Management Tools 81

9 Industrial Automation and Control Systems Computer Software 84

9.1 Server and Workstation Operating Systems 84
9.2 Real-time and Embedded Operating Systems 87
9.3 Web Technologies 89

10 Physical Security Controls 91

10.1 Physical Protection 92
10.2 Personnel Security 95

Copyright 2007 ISA. All rights reserved.