TECHNICAL REPORT

ISA–TR99.00.01–2004

Security Technologies for Manufacturing and Control Systems

Approved 11 March 2004

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 Acronyms 19

4 Overview 20

5 Authentication and Authorization Technologies 21

5.1 Role-Based Authorization Tools 22

5.2 Password Authentication 24

5.3 Challenge/Response Authentication 26

5.4 Physical/Token Authentication 28

5.5 Smart Card Authentication 29

5.6 Biometric Authentication 31

5.7 Location-Based Authentication 33

5.8 Password Distribution and Management Technologies 34

5.9 Device-to-Device Authentication 34

6 Filtering/Blocking/Access Control Technologies 34

6.1 Dedicated Firewalls 34

6.2 Host-based Firewalls 38

6.3 Virtual Local Area Networks (VLANs) 40

7 Encryption Technologies and Data Validation 41

7.1 Symmetric (Secret) Key Encryption 42

Copyright 2004 ISA. All rights reserved.

7.2 Public Key Encryption and Key Distribution 45

7.3 Private Key Signatures and Digital Certificates 48

7.4 Virtual Private Networks (VPNs) 48

8 Audit, Measurement, Monitoring, and Detection Tools 53

8.1 Log Auditing Utilities 53

8.2 Virus/Malicious Code Detection 55

8.3 Intrusion Detection Systems 58

8.4 Network Vulnerability Scanners 61

8.5 Network Forensics and Analysis Tools (NFAT) 63

8.6 Host Configuration Management Tools 65

8.7 Automated Software Management Tools 65

9 Computer Software 65

9.1 Server and Workstation Operating Systems 66

9.2 Real-time and Embedded Operating Systems 68

9.3 Web and Internet Technologies 70

10 Physical Security Controls 72

10.1 Physical Protection 73

10.2 Personnel Security 76

Copyright 2004 ISA. All rights reserved.

TECHNICAL REPORT

ISA-TR99.00.02-2004

Integrating Electronic Security into the Manufacturing and Control Systems Environment

Approved 12 April 2004

Table of Contents

1 Scope 15
2 Purpose 15
3 Intended Audience 16
4 General Terms and Definitions 16
5 Background 18
6 Developing a Security Program 19
6.1 Leadership Commitment 19
6.2 Develop a Business Case 19
6.3 Develop a Charter or Scope 19
6.4 Program Tasks 20
6.5 Special Considerations for Manufacturing and Control Systems 22
6.6 Program Elements 23
6.7 Manufacturing and Control System Change Management Plan 31
6.8 The Security Lifecycle 34
6.9 Program Step Details 35
7 Define Risk Goals 36
8 Assess and Define Existing System 36
8.1 Form Cross-Functional Team 36
8.2 Pre-Risk Analysis Activities 36
8.3 Update the Screening Inventory 44
8.4 Make Preliminary Assessment of Overall Vulnerability 44
9 Conduct Risk Assessment and Gap Analysis 44
9.1 Conduct Detailed Risk Analysis Vulnerability Assessment of the Prioritized Assets 44
9.2 Prioritize Systems for Implementation Phase of Risk Mitigation Plan 55
10 Design or Select Countermeasures 55
10.1 Implement Risk Mitigation Strategies Based upon Detected Vulnerabilities 55

Copyright 2004 ISA. All rights reserved.

10.2 Address Vulnerabilities 60

10.3 Formalize Change Management Plan for the System 61

11 Procure or Build Countermeasures 61

11.1 Translate Requirements from Design Phase to Specification or Complete Construction 61

12 Define Component Test Plans 61

12.1 Decisions to Make When Planning a Test Program 61

12.2 Sufficient Testing 63

12.3 Component Test Plans 64

13 Test Countermeasures 64

14 Define Integration Test Plan 65

15 Perform Pre-Installation Integration Test 65

16 Define System Validation Test Plan 65

17 Perform Validation Test on Installed System 66

18 Finalize Operational Security Measures 66

18.1 Establish Operational Security Baseline 66

18.2 Finalize Operational Security Policy 67

18.3 Establish Management of Change (MOC) Program 67

18.4 Establish Periodic Audit Plan 67

18.5 Establish Audit Metrics 67

18.6 Establish Audit Metrics Reporting Procedure 67

18.7 Establish Compliance Requirements 68

18.8 Establish Corrective Action Procedures 68

18.9 Disaster Recovery 68

18.10 Monitoring and Logging 68

18.11 Intrusion Detection 68

18.12 Incident Response 68

18.13 Contingency Plans 69

18.14 Normal Support 69

Copyright 2004 ISA. All rights reserved.

18.15 Formalize Audit Plan for the System 69

18.16 Implement 70

19 Routine Security Reporting and Analysis 70

20 Periodic Audit and Compliance Measures 70

21 Reevaluate Security Countermeasures 70

22 Work with Suppliers and Consultants 70

22.1 System Suppliers 71

22.2 Consultants 71

22.3 Integrators 71

22.4 User Groups 71

23 Participate in Industry Forums and Development Programs 72

23.1 ISA—The Instrumentation, Systems, and Automation Society 72

23.2 U.S. National Institute of Standards and Technology (NIST) 72

23.3 North American Electric Reliability Council (NERC) 72

23.4 Chemical Industry Data Exchange (CIDX) 72

23.5 Institute of Electrical and Electronics Engineers (IEEE) 72

23.6 International Electrotechnical Commission (IEC) 72

23.7 International Council on Large Electric Systems (CIGRE) 73

23.8 U.S. Department of Energy National SCADA Test Bed Program 73

23.9 Process Control System Cyber Security Forum (PCSRF) 73

24 Bibliography and References 73

Annex A — Sample Policies and Procedures Document 77

Annex B — A Sample Vulnerability Assessment Procedure 88

Annex C —Integrating Security into Supplier Practices 88

Copyright 2004 ISA. All rights reserved.

Selected ISA Technical Papers on Security Issues

Current Status of Technical Issues Concerning Cyber Security of Control Systems for Water and Wastewater Industries
Current Status of Technical and Regulatory Issues Concerning Cyber Security of Control Systems
Developing a Solid SCADA Security Strategy
How Open Systems Increase Security Risks: What You Can Do About It
Intrusion Detection and Cyber Security Monitoring of SCADA and DCS Networks
Manufacturing and Control Systems Security – ISA SP99 History, Status, and How It Can Help You
Monitoring Controller's "DNA Sequence" For System Security
The Myths and Facts Behind Cyber Security Risks for Industrial Control Systems
Network Security in the Wireless Age
Remote Method Security in a Distributed Processing Architecture Supporting Generic Security Objects
Security Issues with Distributed Web Applications
Security Issues in Internet Programming
Web Application Security Risk Assessment
Wireless Data Communications and Security in Railway Rolling Stock Applications
Wireless LAN Security: What Every Technical Professional Should Know

Government Documents on Security Issues

The Physical Protection of Critical Infrastructures and Key Assets
Critical Infrastructure: Control Systems and the Terrorist Threat
Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems
21 Steps to Improve Cyber Security of SCADA Networks
IT Security for Industrial Control Systems