

**ISA-TR99.00.02-2004**

**Integrating Electronic  
Security into the  
Manufacturing and Control  
Systems Environment**

**Approved 12 April 2004**

ISA-TR99.00.02-2004

Integrating Electronic Security into the Manufacturing and Control Systems Environment

ISBN: 1-55617-889-1

Copyright © 2004 by ISA—The Instrumentation, Systems, and Automation Society. All rights reserved. Not for resale. Printed in the United States of America. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), without the prior written permission of the Publisher.

ISA  
67 Alexander Drive  
P.O. Box 12277  
Research Triangle Park, North Carolina 27709  
USA

## Preface

This preface, as well as all footnotes and annexes, is included for information purposes and is not part of ISA-TR 99.00.02-2004.

This document has been prepared as part of the service of ISA--The Instrumentation, Systems, and Automation Society, toward a goal of uniformity in the field of instrumentation. To be of real value, this document should not be static but should be subject to periodic review. Toward this end, the Society welcomes all comments and criticisms and asks that they be addressed to the Secretary, Standards and Practices Board; ISA; 67 Alexander Drive; P. O. Box 12277; Research Triangle Park, NC 27709; Telephone (919) 549-8411; Fax (919) 549-8288; E-mail: standards@isa.org.

The ISA Standards and Practices Department is aware of the growing need for attention to the metric system of units in general, and the International System of Units (SI) in particular, in the preparation of instrumentation standards. The Department is further aware of the benefits to USA users of ISA standards of incorporating suitable references to the SI (and the metric system) in their business and professional dealings with other countries. Toward this end, this Department will endeavor to introduce SI-acceptable metric units in all new and revised standards, recommended practices, and technical reports to the greatest extent possible. *Standard for Use of the International System of Units (SI): The Modern Metric System*, published by the American Society for Testing & Materials as IEEE/ASTM SI 10-97, and future revisions, will be the reference guide for definitions, symbols, abbreviations, and conversion factors.

It is the policy of ISA to encourage and welcome the participation of all concerned individuals and interests in the development of ISA standards, recommended practices, and technical reports. Participation in the ISA standards-making process by an individual in no way constitutes endorsement by the employer of that individual, of ISA, or of any of the standards, recommended practices, and technical reports that ISA develops.

**CAUTION — ISA ADHERES TO THE POLICY OF THE AMERICAN NATIONAL STANDARDS INSTITUTE WITH REGARD TO PATENTS. IF ISA IS INFORMED OF AN EXISTING PATENT THAT IS REQUIRED FOR USE OF THE DOCUMENT, IT WILL REQUIRE THE OWNER OF THE PATENT TO EITHER GRANT A ROYALTY-FREE LICENSE FOR USE OF THE PATENT BY USERS COMPLYING WITH THE DOCUMENT OR A LICENSE ON REASONABLE TERMS AND CONDITIONS THAT ARE FREE FROM UNFAIR DISCRIMINATION.**

**EVEN IF ISA IS UNAWARE OF ANY PATENT COVERING THIS DOCUMENT, THE USER IS CAUTIONED THAT IMPLEMENTATION OF THE DOCUMENT MAY REQUIRE USE OF TECHNIQUES, PROCESSES, OR MATERIALS COVERED BY PATENT RIGHTS. ISA TAKES NO POSITION ON THE EXISTENCE OR VALIDITY OF ANY PATENT RIGHTS THAT MAY BE INVOLVED IN IMPLEMENTING THE DOCUMENT. ISA IS NOT RESPONSIBLE FOR IDENTIFYING ALL PATENTS THAT MAY REQUIRE A LICENSE BEFORE IMPLEMENTATION OF THE DOCUMENT OR FOR INVESTIGATING THE VALIDITY OR SCOPE OF ANY PATENTS BROUGHT TO ITS ATTENTION. THE USER SHOULD CAREFULLY INVESTIGATE RELEVANT PATENTS BEFORE USING THE DOCUMENT FOR THE USER'S INTENDED APPLICATION.**

**HOWEVER, ISA ASKS THAT ANYONE REVIEWING THIS DOCUMENT WHO IS AWARE OF ANY PATENTS THAT MAY IMPACT IMPLEMENTATION OF THE DOCUMENT NOTIFY THE ISA STANDARDS AND PRACTICES DEPARTMENT OF THE PATENT AND ITS OWNER.**

**ADDITIONALLY, THE USE OF THIS DOCUMENT MAY INVOLVE HAZARDOUS MATERIALS, OPERATIONS OR EQUIPMENT. THE DOCUMENT CANNOT ANTICIPATE ALL POSSIBLE APPLICATIONS OR ADDRESS ALL POSSIBLE SAFETY ISSUES ASSOCIATED WITH USE IN HAZARDOUS CONDITIONS. THE USER OF THIS DOCUMENT MUST EXERCISE SOUND**

**PROFESSIONAL JUDGMENT CONCERNING ITS USE AND APPLICABILITY UNDER THE USER'S PARTICULAR CIRCUMSTANCES. THE USER MUST ALSO CONSIDER THE APPLICABILITY OF ANY GOVERNMENTAL REGULATORY LIMITATIONS AND ESTABLISHED SAFETY AND HEALTH PRACTICES BEFORE IMPLEMENTING THIS DOCUMENT.**

The following served as voting members of ISA-SP99:

| <b>NAME</b>                                        | <b>COMPANY</b>                           |
|----------------------------------------------------|------------------------------------------|
| B. Singer, <i>Chair</i>                            | Rockwell Automation                      |
| E. Hand, <i>Vice Chair</i>                         | Kraft Foods Inc.                         |
| R. Webb, <i>Managing Director &amp; WG2 Leader</i> | Consultant                               |
| E. Byres, <i>Working Group 1 Leader</i>            | British Columbia Institute of Technology |
| M. Franz, <i>Working Group 3 Leader</i>            | Cisco Systems, Inc.                      |
| D. Teumim, <i>Working Group 7 Leader</i>           | Teumim Technical LLC                     |
| P. Baybutt                                         | Primatech Inc.                           |
| H. Beum                                            | Interface Technologies                   |
| R. Bhojani                                         | Bayer                                    |
| D. Brandl                                          | BR&L Consulting                          |
| K. Chambers                                        | GE Fanuc Automation Americas Inc.        |
| J. Christman                                       | Northrop Grumman Information Technology  |
| E. Cosman                                          | The Dow Chemical Co.                     |
| J. Dalzon                                          | ISA France                               |
| T. Davis                                           | Telvent                                  |
| R. Derynck                                         | Verano Inc.                              |
| R. Dhaliwal                                        | Allstream                                |
| R. Forrest                                         | The Ohio State University                |
| T. Good                                            | DuPont                                   |
| M. Heard                                           | Eastman Chemical Co.                     |
| M. Lees                                            | Schering-Plough Corp.                    |
| C. Mastromonico                                    | Westinghouse Savannah River Co.          |
| W. Matz                                            | Invensys-Foxboro                         |
| G. Morningstar                                     | Cedar Rapids Water Dept.                 |
| A. Nangia                                          | 3M                                       |
| S. Oda                                             | Yokogawa Corp. of America                |
| R. Oyen                                            | ABB Inc.                                 |
| M. Schilt                                          | Rockwell Automation                      |
| C. Sossman                                         | WGI-W Safety Management Solutions LLC    |
| L. Steinocher                                      | Fluor Enterprises Inc.                   |
| B. Taylor                                          | The George Washington University         |
| D. Tindill                                         | Matrikon Inc.                            |
| L. Uden                                            | Lyondell/Equistar Chemicals              |
| J. Weiss                                           | KEMA Inc.                                |

This technical report was approved for publication by the ISA Standards and Practices Board on 12 April 2004:

| <b>NAME</b>               | <b>COMPANY</b>              |
|---------------------------|-----------------------------|
| V. Maggioli, <i>Chair</i> | Feltronics Corp.            |
| F. Amir                   | DuPont                      |
| D. Bishop                 | David N. Bishop, Consultant |
| K. Bond                   | Consultant                  |
| D. Bouchard               | Paprican                    |

M. Coppler  
B. Dumortier  
W. Holland  
E. Içayan  
A. Iverson  
T. McAviney  
A. McCauley, Jr.  
G. McFarland  
R. Reimer  
J. Rennie  
N. Sands  
H. Sasajima  
T. Schnaare  
A. Summers  
I. Verhappen  
R. Webb  
W. Weidman  
J. Weiss  
M. Widmeyer  
R. Wiegler  
C. Williams  
M. Zielinski

Ametek, Inc.  
Schneider Electric  
Consultant  
ACES, Inc.  
Ivy Optiks  
Jacobs Engineering Group  
Chagrin Valley Controls, Inc.  
Emerson Process Management  
Rockwell Automation  
Consultant  
DuPont  
Yamatake Corp.  
Rosemount Inc.  
SIS-TECH Solutions LLC  
Syncrude Canada Ltd.  
Consultant  
Parsons Energy & Chemicals Group  
KEMA Inc.  
Stanford Linear Accelerator Center  
CANUS Corp.  
Eastman Kodak Co.  
Emerson Process Management

This page intentionally left blank.

## Table of Contents

|      |                                                                                        |    |
|------|----------------------------------------------------------------------------------------|----|
| 1    | Scope .....                                                                            | 15 |
| 2    | Purpose.....                                                                           | 15 |
| 3    | Intended Audience .....                                                                | 15 |
| 4    | General Terms and Definitions .....                                                    | 15 |
| 5    | Background.....                                                                        | 17 |
| 6    | Developing a Security Program.....                                                     | 18 |
| 6.1  | Leadership Commitment .....                                                            | 18 |
| 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.....                      | 21 |
| 6.6  | Program Elements.....                                                                  | 22 |
| 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 .....                                                   | 42 |
| 8.4  | Make Preliminary Assessment of Overall Vulnerability .....                             | 42 |
| 9    | Conduct Risk Assessment and Gap Analysis .....                                         | 42 |
| 9.1  | Conduct Detailed Risk Analysis Vulnerability Assessment of the Prioritized Assets..... | 42 |
| 9.2  | Prioritize Systems for Implementation Phase of Risk Mitigation Plan.....               | 54 |
| 10   | Design or Select Countermeasures.....                                                  | 55 |
| 10.1 | Implement Risk Mitigation Strategies Based upon Detected Vulnerabilities .....         | 55 |

|       |                                                                                          |    |
|-------|------------------------------------------------------------------------------------------|----|
| 10.2  | Address Vulnerabilities .....                                                            | 59 |
| 10.3  | Formalize Change Management Plan for the System .....                                    | 60 |
| 11    | Procure or Build Countermeasures .....                                                   | 60 |
| 11.1  | Translate Requirements from Design Phase to Specification or Complete Construction ..... | 60 |
| 12    | Define Component Test Plans .....                                                        | 60 |
| 12.1  | Decisions to Make When Planning a Test Program .....                                     | 60 |
| 12.2  | Sufficient Testing .....                                                                 | 62 |
| 12.3  | Component Test Plans .....                                                               | 63 |
| 13    | Test Countermeasures .....                                                               | 63 |
| 14    | Define Integration Test Plan .....                                                       | 64 |
| 15    | Perform Pre-Installation Integration Test .....                                          | 64 |
| 16    | Define System Validation Test Plan .....                                                 | 64 |
| 17    | Perform Validation Test on Installed System .....                                        | 65 |
| 18    | Finalize Operational Security Measures .....                                             | 65 |
| 18.1  | Establish Operational Security Baseline .....                                            | 65 |
| 18.2  | Finalize Operational Security Policy .....                                               | 66 |
| 18.3  | Establish Management of Change (MOC) Program .....                                       | 66 |
| 18.4  | Establish Periodic Audit Plan .....                                                      | 66 |
| 18.5  | Establish Audit Metrics .....                                                            | 66 |
| 18.6  | Establish Audit Metrics Reporting Procedure .....                                        | 66 |
| 18.7  | Establish Compliance Requirements .....                                                  | 67 |
| 18.8  | Establish Corrective Action Procedures .....                                             | 67 |
| 18.9  | Disaster Recovery .....                                                                  | 67 |
| 18.10 | Monitoring and Logging .....                                                             | 67 |
| 18.11 | Intrusion Detection .....                                                                | 67 |
| 18.12 | Incident Response .....                                                                  | 67 |
| 18.13 | Contingency Plans .....                                                                  | 68 |
| 18.14 | Normal Support .....                                                                     | 68 |

|         |                                                                  |    |
|---------|------------------------------------------------------------------|----|
| 18.15   | Formalize Audit Plan for the System .....                        | 68 |
| 18.16   | Implement .....                                                  | 69 |
| 19      | Routine Security Reporting and Analysis .....                    | 69 |
| 20      | Periodic Audit and Compliance Measures .....                     | 69 |
| 21      | Reevaluate Security Countermeasures.....                         | 69 |
| 22      | Work with Suppliers and Consultants.....                         | 69 |
| 22.1    | System Suppliers .....                                           | 70 |
| 22.2    | Consultants .....                                                | 70 |
| 22.3    | Integrators.....                                                 | 70 |
| 22.4    | User Groups.....                                                 | 70 |
| 23      | Participate in Industry Forums and Development Programs.....     | 71 |
| 23.1    | ISA—The Instrumentation, Systems, and Automation Society .....   | 71 |
| 23.2    | U.S. National Institute of Standards and Technology (NIST) ..... | 71 |
| 23.3    | North American Electric Reliability Council (NERC).....          | 71 |
| 23.4    | Chemical Industry Data Exchange (CIDX) .....                     | 71 |
| 23.5    | Institute of Electrical and Electronics Engineers (IEEE).....    | 71 |
| 23.6    | International Electrotechnical Commission (IEC) .....            | 71 |
| 23.7    | International Council on Large Electric Systems (CIGRE) .....    | 72 |
| 23.8    | U.S. Department of Energy National SCADA Test Bed Program .....  | 72 |
| 23.9    | Process Control System Cyber Security Forum (PCSRF) .....        | 72 |
| 24      | Bibliography and References .....                                | 72 |
| Annex A | — Sample Policies and Procedures Document .....                  | 75 |
| Annex B | — A Sample Vulnerability Assessment Procedure .....              | 87 |
| Annex C | —Integrating Security into Supplier Practices .....              | 87 |

This page intentionally left blank.

## Foreword

In order to protect Manufacturing and Control Systems environments from potential threats and probability of attacks, each site or corporate entity should be responsible for developing an electronic security program and creating a security plan to protect manufacturing control networks.

This ISA Technical Report provides a framework for developing an electronic security program and provides a recommended organization and structure for the security plan. The information provides detailed information about the minimum elements to include. Site or entity-specific information should be included at the appropriate places in the program.

This technical report addresses Manufacturing and Control Systems whose compromise could result in any or all of the following situations:

- endangerment of public or employee health and safety
- loss of public confidence
- violation of regulatory requirements
- loss of proprietary or confidential information
- economic loss
- impact on entity, local, state or national security

The concept of Manufacturing and Control Systems electronic security is applied in the broadest practical sense, encompassing all types of plants, facilities, and systems in all industries. Manufacturing and Control Systems include, but are not limited to:

- Hardware and software systems such as Distributed Control Systems (DCSs), Programmable Logic Controllers (PLCs), Supervisory Control and Data Acquisition (SCADA) systems, networked electronic sensing, and monitoring and diagnostic systems
- Associated internal, human, network, or machine interfaces used to provide control, safety, and manufacturing operations functionality to continuous, batch, discrete, and other processes.
- Basic Process Control System (BPCS), Safety Instrumented System (SIS), and associated systems such as advanced or multivariable control, online optimizers, dedicated equipment monitors, and graphical interfaces.

This page intentionally left blank.

## Introduction

This document, the second in a series of ISA Technical Reports, provides guidance to Manufacturing and Control Systems users (including operations, maintenance, engineering, and other user services), manufacturers, suppliers, and security practitioners, on how to provide adequate electronic (cyber) security for these systems. It focuses on the planning, developing, and implementing activities involved with a comprehensive program for integrating security into the Manufacturing and Control Systems environment. The program includes requirements, policies, procedures, and practices in areas ranging from risk analysis to management of change and compliance auditing.

Implementing this type of program often involves additional or changed hardware and software and may require training personnel on new technologies (such as network firewalls). Guidance on procedures in this area will involve some technology-related discussion and examples. This information is provided in the companion Technical Report in this series:

- **ISA-TR99.00.01-2004, Security Technologies for Manufacturing and Control Systems—** Provides an overview of the types of electronic security technologies currently available to the Manufacturing and Control Systems environment; the pros, cons, and specific details of how each technology fits the environment; a list of types of products currently evaluated by the ISA-SP99 committee; and an idea of where security technology is headed in the future. A significant part of ISA-TR99.00.02-2004, *Integrating Electronic Security into the Manufacturing and Control Systems Environment*, is technology-independent, but there are parts that rely on technology. Refer to ISA-TR99.00.01-2004 for more comprehensive information on the alternatives available to implement security technologies.

Please refer to both technical reports in this series for a more comprehensive presentation and understanding of the technology, programs, and audits and testing necessary to provide electronic security to the Manufacturing and Control Systems environment.

This ISA technical report provides guidance for attaining adequate electronic security. It should be used to help identify and address vulnerabilities and reduce the risk of undesired intrusions that could compromise confidential information or cause disruption or failure of manufacturing or control systems.

The guidance presented in this document is general in nature, and must be applied to each system or network by personnel knowledgeable in the manufacturing or control systems to which it is being applied. The guidance identifies those activities, system attributes, and actions that are typically important to provide electronically secure control systems, but whose application is not always compatible with maintenance of a system's functions. Guidance includes suggestions on appropriate application to specific control systems; however, selection of activities and practices for a given system is the responsibility of the system's owner.

It is expected that this guidance will grow and change over time, as experience is obtained with system vulnerability and security and new technologies become available. While the general format of this guidance is expected to remain relatively stable, the specifics of its application and specific solutions are expected to evolve with developments in technology, industry requirements, and regulatory requirements.

This page intentionally left blank.

## 1 Scope

The scope of this ISA technical report includes Manufacturing and Control Systems whose compromise could result in the endangerment of public or employee health or safety, loss of public confidence, violation of regulatory requirements, loss or invalidation of proprietary or confidential information, or economic loss. The concept of Manufacturing and Control Systems electronic security is applied in the broadest practical sense, encompassing all types of manufacturing and process facilities and systems in all industries. Manufacturing and Control Systems include, but are not limited to:

- Hardware and software systems such as Distributed Control Systems (DCSs), Programmable Logic Controllers (PLCs), Supervisory Control and Data Acquisition (SCADA) systems, networked electronic sensing systems, and monitoring and diagnostic systems;
- Associated internal, human, network, or machine interfaces used to provide control, safety, and manufacturing operations functionality to continuous, batch, discrete, and other processes.

Enterprise Resource Management and Enterprise Resource Planning Systems are not within the scope of this document, although the integrity of data communications from the Manufacturing and Control Systems domains into the Enterprise Resource Business Systems should be included.

## 2 Purpose

The purpose of this ISA technical report is to present a consistent approach for developing, implementing, and operating a program that addresses security for Manufacturing and Control Systems.

## 3 Intended Audience

The audience for this ISA technical report includes all users of Manufacturing and Control Systems (including facility operations, maintenance, engineering, and corporate components of user organizations), manufacturers, suppliers, and security practitioners.

## 4 General Terms and Definitions

While the following terms can take on various interpretations, the definitions in this section are used to show how they apply to this technical report.

**Component Testing**—Testing performed by a vendor, a user's plant, or an outside lab to assure all parties that the purchased security components will meet the purchase specifications and will demonstrate the required security performance.

**Compromise**—Any action from authorized or unauthorized sources that results in the undesirable release of confidential information, modification of critical information, loss of control over system or component assets, physical endangerment, loss of system availability, degraded monitoring capability, or decreased reliability of Manufacturing and Control Systems, or their informational dependencies.

**Control System Operations**—Control system operations encompass the collection of production, maintenance, and quality assurance operations with other activities of a manufacturing facility. They include:

- facility activities that coordinate the personnel, equipment, and material involved in the conversion of raw materials into end products

- functions that may be performed by physical equipment, human effort, and information systems
- managing information about the schedules, use, capability, definition, history, and status of all of the resources (personnel, equipment, and material) within a facility.

**Integration Testing**—The examination and testing of several security components, perhaps from different vendors, temporarily connected together in a test environment to see if the security components will work together correctly before being placed in an actual Manufacturing and Control System.

**Manufacturing and Control Systems**—Systems (personnel, hardware, and software) comprised in either standalone or networked configurations, designed to control or monitor specific aspects of a production process, including safety. Production includes conveyance, treatment, processing, manufacturing, distribution, or engineering of the production process for any product including, but not limited to, utilities production and distribution, consumer goods, raw materials, component parts, and the like. Manufacturing and Control Systems can include DCS, HMI, PLC, SCADA, hybrid, or any other type of control system serving any part of a manufacturing process and utility industries including continuous, discrete, batch, or other processes.

**Manufacturing and Control Systems Electronic Security**—Manufacturing and Control Systems Electronic Security includes the concepts of identification, authentication, accountability, authorization, and privacy. The objective is to preclude unauthorized use, modification, disclosure, or destruction of critical systems or informational assets in an effort to reduce the risk of personal injury or possibility of endangering public health, loss of public or consumer confidence, disclosure of sensitive assets, and protection of business assets. These concepts are applied to any system in the production process and include both standalone and networked components. Communications between systems may be either through internal messaging or by any human or machine interfaces that authenticate, operate, control, or exchange data with any of these control systems.

**Manufacturing Operations**—Manufacturing operations encompass the collection of production, maintenance, and quality assurance operations with other activities of a production facility. Operations include:

- manufacturing or processing facility activities that coordinate the personnel, equipment, and material involved in the conversion of raw materials and/or parts into products
- functions that may be performed by physical equipment, human effort, and information systems
- managing information about the schedules, use, capability, definition, history, and status of all resources (personnel, equipment, and material) within the manufacturing facility.

**Security Components (also called Security Countermeasures)**—Techniques such as firewalls, authentication modules, or encryption software purchased from outside security vendors for insertion into the existing Manufacturing and Control System to improve the security performance of that system.

**Security Guidelines**—Security guidelines define the objectives and constraints for a security program. Guidelines are created at several levels, ranging from company or corporate policy to specific operational constraints (e.g., remote access). In general, guidelines provide answers to the questions “what” and “why” without dealing with “how.” Guidelines are normally stated in terms that are technology-independent.

**Security Performance**—Security performance may be evaluated in terms of a program’s compliance, completeness of measures to provide specific threat protection, post-compromise analysis, review of changing business requirements, new threat and vulnerability information, and periodic audit of control systems to ensure that security measures remain effective and appropriate. Tests, audits, tools, measures, or other methods are required to evaluate security practice performance.

**Security Practices**—Security practices provide a means of capturing experiences and activities that help ensure system protection and reduce potential Manufacturing and Control Systems compromise. Subject areas include physical security, procedures, organization, design, and programming. Security practices include the actual steps to be taken to ensure system protection.

**Security Procedures**—Security procedures define exactly how practices are implemented and executed. They are implemented through personnel training and actions using currently available and installed technology (such as disconnecting modems). Procedures and contained criteria also include more technology-dependent system requirements that need careful analysis, design, planning, and coordinated installation and implementation.

**Security Program**—A security program brings together all aspects of managing security, ranging from the definition and communication of guidelines through implementation of best industry practices and ongoing operation and auditing.

**System Validation Testing**—Testing done on the entire Manufacturing and Control System after all security components are inserted, configured, and made operational. The Manufacturing and Control System may have to be in a non-production mode, such as turnaround mode, to conduct this testing. The purpose of system validation testing and assurance is to see whether the entire Manufacturing and Control System, with new security components retrofitted, will meet the desired security performance while still meeting the non-security functional performance requirements and specifications.

**Teleworking**—Teleworking is an arrangement through which employees work from a location away from their employer's main office. Electronic connections (e.g., telephone lines, cellular/wireless circuits, Internet access) are relied upon for the bulk of interactions and information transfer.

## 5 Background

During the past several years, process automation systems that support the process and manufacturing enterprise have evolved from individual, isolated computers with proprietary operating systems and networks to interconnected systems and applications employing widely used and well understood “open systems” technology (i.e., operating systems and protocols). These automation systems are now being integrated with enterprise systems and other business applications through site and corporate communication networks. This integrated architecture provides significant business benefits including the following:

- Increased visibility of shop floor activities (work in process, equipment status, production schedules), enabling improved business analysis and decision making.
- Integrated manufacturing systems that have more direct access to and from enterprise information, enabling a more responsive manufacturing enterprise.
- Common interfaces that reduce overall support costs and permit remote support of production processes.
- Improved data accessibility that provides the ability to conduct analyses to drive out production costs and improve productivity.
- Remote monitoring of the process control systems that allows problems to be solved more quickly and reduces support costs.

ANSI/ISA standards, such as the ANSI/ISA-50 (Fieldbus) series, ANSI/ISA-84 (Application of Safety Instrumented Systems for the Process Industries) series, ANSI/ISA-88 (Batch Control) series, ANSI/ISA-91.00.01-2001 (Identification of Emergency Shutdown Systems and Controls that Are Critical to

Maintaining Safety in Process Industries), and ANSI/ISA-95 (Enterprise-Control System Integration) series, have added considerable value to the Manufacturing and Control Systems community by establishing models, terms, and information exchanges that provide the ability to share information in an open and standardized way (visit [www.isa.org/standards/](http://www.isa.org/standards/) for additional information on these standards). However, this ability to exchange information increases vulnerability to misuse and attack by individuals with malicious intent and introduces potential risks to the enterprise that uses Manufacturing and Control Systems.

In recent years, electronic security has become a more significant and widely acknowledged concern. People with knowledge of features provided by open operating systems and networks could potentially intrude into console devices, remote devices, databases and, in some cases, control platforms. The impact of intruders on Manufacturing and Control Systems may include:

- unauthorized access, theft, or misuse of confidential information
- loss of integrity or reliability of process data and production information
- loss of system availability
- process upsets leading to inferior product quality, lost production capacity, compromised process safety, or environmental releases
- equipment damage
- personal injury
- violation of legal and regulatory requirements
- public health and confidence
- impact on a nation's security.

The focus on unauthorized access has broadened from “hackers” or disgruntled employees to include deliberate terrorist activities aimed at harming large groups and facilities. This shift requires a more structured set of guidelines and procedures to define electronic security applicable to Manufacturing and Control Systems, as well as the respective connectivity to other systems.

## 6 Developing a Security Program

Effectively integrating security into a Manufacturing and Control System environment requires defining and executing a comprehensive program that addresses all aspects of security, ranging from identifying objectives to day-to-day operation and ongoing auditing for compliance and improvement. This section describes the basic process for developing a security program. More detailed information on the various steps is provided in subsequent sections.

### 6.1 Leadership Commitment

The commitment to a security program begins at the top. Senior management must demonstrate a clear commitment to cybersecurity. Cybersecurity is a business responsibility shared by all members of the enterprise and especially by leading members of the business, process, and manufacturing management teams. Cybersecurity programs with visible, top-level support and “buy-in” from organization leaders are more likely to gain compliance, function more smoothly, and have earlier success.

## 6.2 Develop a Business Case

Even with a general commitment, upper management does not always recognize or understand the practical benefits of cybersecurity for Manufacturing and Control Systems. In order to obtain funding, it may be necessary to build a business case. *The ISA-SP99 committee recognizes this topic as important and will address it further in a future revision of this Technical Report.*

## 6.3 Develop a Charter or Scope

With the imperative understood and the business case established, the next step is to develop a formal charter or scope for the effort. This charter should explain clearly what is to be accomplished (in business terms) and when. The scope of the program defines the specific entity (business, site, or corporation) of focus.

The charter should be owned by a senior executive program champion who will be responsible for guiding the team during program development. The champion will ultimately be responsible for making sure that the program is executed, including communications, enforcement, and auditing.

### 6.3.1 Assemble Stakeholders and Establish a Program Team

The next step is to assemble the team of people responsible for developing the various program elements, including guidelines, processes, and procedures. The team should consist of, but not be limited to, personnel from the following areas:

- Information Technology (IT)
- Telecommunications
- Process Control
- Operations and Production
- Maintenance
- Security
- Management
- Training
- Human Resources
- Finance

Programs should be developed so that they can be implemented throughout a specific entity (business, site, or corporation). The initial program scope is defined when the program team is formed, but may have to be adjusted as the team's knowledge grows.

Programs should be developed within existing business, site, or corporation program structures as appropriate to simplify and expedite the process.

A senior executive program champion should be responsible for guiding the team during program development. The champion will ultimately be responsible for making sure that the program is executed, including communications, enforcement, and auditing.

## 6.4 Program Tasks

Once the team has been assembled, its first activity is to plan the basic tasks that must be accomplished in developing an effective program. These tasks are briefly described in the following paragraphs. More detailed information is provided in sections 7 through 21.

### 1. Define Risks

The first task for the program team is to define the potential risks for the Manufacturing and Control System. Risks may be identified through a variety of means, ranging from corporate governance or external regulatory compliance to the application of a formal risk assessment methodology. Regardless of how they are identified, risks must be categorized and prioritized.

### 2. Establish Program Goals

Establish specific goals to address the risks identified. These goals form the foundation of the security program and must be clearly supported by senior management, as well as the technical experts responsible for Manufacturing and Control Systems.

Goals should include developing an implementation plan and schedule including all aspects of the program, along with recommendations for developing awareness and training all personnel. The implementation plan includes a transition phase that provides the methodology and architecture to get from the “as-is” security conditions to the “to-be” security conditions. It also provides the details of actually performing the work required to make the security changes and additions to the Manufacturing and Control Systems. The schedule may depend on funding the program, but should consider the priorities defined in the plan.

### 3. Identify Program Elements and Develop a Plan

Security programs consist of various combinations of written guidelines, standards, processes, and procedures that address the issues and requirements within the stated scope of the program. Written documentation must clearly state whether actions and procedures are mandatory or recommended practices.

Each program requires a specific list of elements to be included. These elements build on existing Information Technology (IT) security experience, programs, and practices, but are tailored to the specific security requirements of the Manufacturing and Control System environment. A list of possible elements can be found in section 6.6.

### 4. Address Configuration Management

Vital information and assets must be assessed and classified based on the consequences of loss, damage, or failure. Assign the appropriate levels of security protection and assess the vulnerability of Manufacturing and Control System information loss or compromise.

### 5. Establish Performance Considerations

When developing an electronic security program, it is important to consider various aspects of Manufacturing and Control System performance to ensure that each element is applied without adversely impacting the systems to which it is applied. However, it is also essential to review and consider the required performance at an overall systems level to ensure that when all security

features are taken together, they do not adversely affect required time-critical or other performance characteristics of these systems.

Successful completion of this task requires a detailed understanding of the factors that make Manufacturing and Control Systems different from typical business information technology systems. Special considerations for Manufacturing and Control Systems are examined in more detail in section 6.5.

## 6. Execute the Program

A complete program includes plans that define the approach to and criteria for Manufacturing and Control Systems electronic security. Plans define how necessary security is provided, and usually include functional requirements, as well as certain specific technical requirements. They provide for the system's electronic security, while ensuring that the basic manufacturing and control functionality is fully met. Plans encompass all aspects of the program; they define the program in its entirety, even though the plans may be performed or implemented throughout the organization, (e.g., design, engineering, IT services, operations, maintenance, procurement).

### 6.5 Special Considerations for Manufacturing and Control Systems

Manufacturing and Control System electronic security plans and programs are consistent with, and build on, existing IT (information technology) security experience, programs, and practices. However, there are critical operational differences between IT and Manufacturing and Control Systems that influence how specific measures should be applied. Key differences include:

- **Differing risk management goals**—Human safety and fault tolerance to prevent loss of life or endangerment of public health or confidence, loss of equipment, loss of intellectual property, or lost or damaged product.
- **Differing architecture security focus**—In a typical IT system, the primary focus of security is protecting the information stored on the central server. In manufacturing systems, the situation is reversed. Edge clients (e.g., PLC, operator station, or DCS controller) are typically more important than the central server.
- **Differing availability requirements**—Many manufacturing processes are continuous in nature. Unexpected outages of systems that control manufacturing processes are not acceptable. Exhaustive pre-deployment testing is essential to ensure high availability for the Manufacturing and Control System. In addition to unexpected outages, many control systems cannot be easily stopped and started without affecting production. In some cases, the products produced or equipment being used is more important than the information being relayed. The requirement for high availability, reliability, and maintainability reduces the effectiveness of IT strategies like rebooting.
- **Unintended consequences**—Manufacturing and Control Systems can be very complex in the way that they interact with physical processes. All security functions integrated into the process control system must be tested to prove that they do not introduce unacceptable vulnerabilities. Adding any physical or logical component to the system may reduce reliability of the control system, but the resulting reliability should be kept to acceptable levels.
- **Time critical responses**—For some systems, automated response time or system response to human interaction is critical. For example, emergency actions on regulatory process control systems should not be hampered by requiring password authentication and authorization. Information flow must not be interrupted or compromised.

- **Differing response time requirements**—Manufacturing and Control Systems are generally time critical; delay is not acceptable for the delivery of information, and high throughput is typically not essential.
- **System software**—Differing and “custom” operating systems and applications may not tolerate typical IT practices. Networks are often more complex and require a different level of expertise (e.g., control networks are typically managed by control engineers, not IT personnel). Software and hardware applications are more difficult to upgrade in a control system network. Many systems may not have desired features including encryption capabilities, error logging, and password protection.
- **Resource constraints**—Control systems and their real time operating systems are resource-constrained systems that do not include typical IT security technologies. There may not be available computing resources to retrofit these security technologies.
- **Information integrity**—In-bound information is highly essential to the control system operation. It is important to take practical precautions to eliminate malicious in-bound information in an effort to maintain control operation.
- **Communications**—Communication protocols and media used by control systems environments are typically different from the generic IT environment, and may be proprietary. Examples include radio telemetry using asynchronous serial protocols and proprietary communication networks.
- **Software Updates**—Security patches cannot always be implemented on a timely basis because software changes need to be thoroughly tested by the vendor of the manufacturing control application and the end user of the application before being implemented. Change management control is necessary to maintain integrity of the control systems.

These differences require careful assessment by Manufacturing and Control System experts working in conjunction with security and IT personnel. This team of people should carefully evaluate the applicability of IT and specific Manufacturing and Control Systems electronic security features, including thorough testing before application, where necessary.

## 6.6 Program Elements

There are several specific elements that are delivered as part of a comprehensive security program. These elements should be carefully documented. Written records should be kept of all policies and procedures, as well as all results of their application. Backups or archives should be maintained so that failures or compromise of the systems will not destroy records.

The following paragraphs describe several elements that are commonly included in such a program.

### 6.6.1 Definitions

Provide a set of definitions for all key words and phrases, especially as they apply to Manufacturing and Control Systems.

### 6.6.2 Scope and Purpose

A description of the program's scope and purpose is typically taken from the initial charter. The security perimeter of the hardware and software to which the program is to be applied should also be defined. Defining the security perimeter supports a clear understanding of all connections and interfaces that must be secure.

### 6.6.3 Organization Responsibilities

Define the roles and responsibilities for the entire organization, along with interfaces between each part of the organization. This structure allows all participants to clearly understand their role and the role of others with whom they must interface at all levels.

The organization responsible for Manufacturing and Control Systems may be different from that responsible for IT systems. The organization may have different priorities with established training procedures focused on legal compliance, preventing accidents, controlling incidents, maintaining product quality, and preventing loss of revenue.

### 6.6.4 Principles

The security program should develop or identify principles for process control security that balance the needs of both production and corporate security. Examples of where principles may be required include:

- Ownership and accountability—how are these assigned within the organization?
- Operation and production requirements.
- Support needs and strategies.
- Access control.
- Physical security.
- Monitoring and controlling physical features.
- Physical access control, locking, and protection.
- Maintenance management.

### 6.6.5 Vulnerability Assessment

Every business organization should identify its vital information and assets, classify them based on the consequences of loss or failure, assign appropriate levels of security protection, and assess the vulnerability of its Manufacturing and Control Systems to information loss or compromise. Once system vulnerabilities are understood, the security program can be designed to take the appropriate actions to ensure that levels of security protection are achieved through both system design and administrative controls.

### 6.6.6 Policies

In response to the principles and management direction, the program team must identify or develop a series of policies that determine exactly how security is to be managed. These policies will exist at several levels, ranging from basic organizational policies that are established by management to more detailed policies that pertain to specific aspects of the program. The appropriate level of management must understand and approve all policies. Potential areas requiring policies include:

- Legal and regulatory compliance
- Training and certification

- Hiring, evaluating and terminating personnel
- Assignment of appropriate security clearance levels
- Authentication
- Authorization
- Logical rights
- Change control
- Logging
- Passwords
- Accounts
- Modem access
- Other remote access
- Unused resources

Annex A provides an example set of security policies and practices developed to support the security risk goals and overall security program for one company's Manufacturing and Control Systems environment. These examples are provided to illustrate the level of policy and practice decisions that need to be made to support meeting the risk goals.

#### 6.6.7 Standards

In addition to principles and policies, specific standards must be identified or established under the security program. Areas where standards may exist or be required include:

- Communication protocols
- Network architecture
- Operating systems
- Databases
- Safety
- Physical installations
- Maintenance
- Security clearance parameters

In some cases, the standards selected may be the same as those applied to business IT systems. However, there will be situations where different standards are selected to meet the specific needs of manufacturing systems.

### 6.6.8 Design Models

The security program may include developing design models to describe the minimum acceptable or recommended practices to be used in constructing a secure system. Topics that could be addressed through the use of models include:

- System hardware and software design and implementation requirements, such as the use of firewalls, routers, and switches
- Permissible data flows
- Management activities to ensure compliance with the requirements

While the focus of models is on meeting functional requirements, some technology is suggested in these discussions and guidance to provide examples and ensure understanding. ISA-TR99.00.01-2004, *Security Technologies for Manufacturing and Control Systems*, provides a more comprehensive listing of available technologies to meet these requirements, along with recommendations for use in the Manufacturing and Control System environment. ISA-TR99.00.01-2004 should be used in conjunction with the requirements and solutions developed in accordance with this technical report.

Several models will be required in any program.

#### 6.6.8.1 Network Segments

The network in a modern manufacturing facility is typically comprised of a series of logical and physical network segments that represent a “layers of protection” approach to design. The specific names used for these segments will vary, but the general arrangement will be similar to the following:

- **Enterprise Network Segment**—Enterprise system computers, such as Enterprise Resource Planning (ERP), Supply Chain Management (SCM), and Customer Relationship Management (CRM) computers are connected on this segment. General-purpose internal client systems (desktops and laptops) also typically connect here.
- **Process Information Network Segment**—Manufacturing Execution System (MES) computers are connected to the process information network segment. This network segment is connected to the enterprise network via routers, but sometimes shares the network with enterprise network segment.
- **Control Network Segment**—Controllers and Human Machine Interface (HMI) devices for manufacturing control are connected on this segment. Media and protocols may be proprietary or general-purpose. Primitive, but essential, information for control is exchanged, such as measured variables and manipulating variables; sometimes controller configuration information is exchanged for maintenance purposes. Communication frames designated to field network may also use this network. The control network is usually connected to the information network via a gateway or similar device and may be further isolated by means of a firewall.
- **Field Network Segment**—Field devices, such as sensors and actuators, are connected on this network segment. Usually proprietary protocols and/or media are used for communication and the connected devices usually have less computing capability. Primitive, but essential, information for control is exchanged, such as measured variables and manipulating variables; sometimes controller configuration information is exchanged for maintenance purposes. The field network is usually connected to the control network via a controller or gateway.

- **Process Segment**—The most elementary segment consists of pipe, valves, vessels, transport belts, and vehicles containing the production fluid or product devices. These segments are entirely physical and provide the means to attach the primary element sensors mentioned under field network segment. Although this segment is not directly impacted by information system vulnerabilities, it could be impacted indirectly by the control systems or by intentional human interaction, and thus must also be considered.

This technical report focuses on the process information network, control network, and field network security. The enterprise network should be protected by IT and business policies; process segments and the physical plan should be protected by a physical security plan that is beyond the scope of this document.

#### 6.6.8.2 Access Control Model

The Access Control Model describes the recommended practices for accessing Manufacturing and Control Systems. Because there are various segments in the network model, there may be varying access control practices for devices on the different network segments. When applying access control, make sure to recognize the unique aspects of Manufacturing and Control Systems. For example, operators in a control room typically need to be able to operate the plant and take control actions, often immediately, without any hindrance from passwords. Physical security and trustworthy personnel are assumed to ensure that operators can perform needed actions immediately. However, the need to modify or reconfigure the system on such an immediate basis is not likely to be required, and therefore stronger access controls could be used to ensure that the person is authorized to perform this function.

##### 6.6.8.2.1 User Access Management

Access Management addresses policies and practices for managing user accounts at the different network segment levels. Develop policies for the following aspects of managing user accounts. Follow ISO 17799:2000<sup>1</sup>, 9.2 as appropriate regarding user account management.

- User registration
- Privilege management
- User password management
- Review of user access rights

##### 6.6.8.2.2 User Responsibilities

Users on different network segments may have different responsibilities. The vulnerabilities and risks at different network segment levels require that different policies and practices be created for the following aspects of the information network. Develop policies for the following aspects of user responsibilities. Follow ISO 17799:2000, 9.3 as appropriate.

---

<sup>1</sup> ISO 17799, *Information Technology—Code of Practice for Information Security Management*, was developed for traditional IT systems. Many of the recommendations, including password policies, may not be appropriate for control system applications.

- Password use
- Unattended user equipment

#### 6.6.8.2.3 Network Access Control

The security program must include policies and practices for the following aspects of the information, control and field network segments and all devices connected to them. Develop policies for the following aspects of network access control. Follow ISO 17799:2000, 9.4 as appropriate.

- Policy on the use of network services
- Enforced path
- User authentication for external connections
- Node authentication
- Remote diagnostic port protection
- Network connection control
- Network routing control
- Security of network services

Control Networks and Field Networks should be physically secured. Refer to section 6.6.8.3, “[Physical and Environmental Security](#).”

#### 6.6.8.2.4 Operating System Access Control

Develop policies for the following aspects of the network, including gateways that connect network segments. Follow ISO 17799:2000, 9.5 as appropriate.

- Automatic terminal identification
- Terminal log-on procedures
- User identification and authentication
- Password management system
- Use of system utilities
- Duress alarm to safeguard users
- Terminal time-out
- Limitation of connection time

#### 6.6.8.2.5 Application Access Control