

# Guide to the ISA-99 Standards

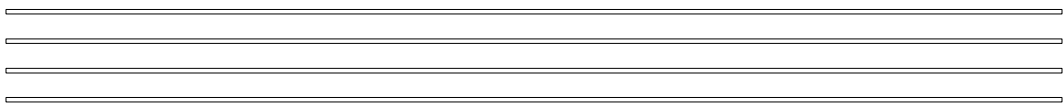
## Manufacturing and Control Systems Security

Revision 4  
November 2005

This document is a work product of the ISA SP-99 committee. It IS NOT part of any draft standard or technical report. Copies may be shared for purposes related to the operation of the SP-99 committee, but all copies must reproduce a copyright notice as follows:

*Copyright 2005 © ISA. All rights reserved. Reproduced and distributed with permission of ISA.*

The reader is cautioned that this document has not been approved and cannot be presumed to reflect the position of ISA or any other committee, society, or group. Although every effort has been made to ensure accuracy, neither ISA, members of the S&P Department, nor their employers shall be held liable for errors or limitations.



## Contents

1	Introduction .....	1
1.1	Structure of the Standard .....	1
1.2	Standard Descriptions .....	1
2	ISA 99.00.01 – Scope, Concepts, Models and Terminology .....	2
2.1	Theme .....	2
2.2	Audience .....	2
2.3	Purpose .....	2
2.4	Organization .....	2
2.5	Typical Questions Addressed .....	2
2.6	Additional Comments .....	2
3	ISA 99.00.02 – Establishing a Manufacturing and Control Systems Security Program .....	3
3.1	Theme .....	3
3.2	Audience .....	3
3.3	Purpose .....	3
3.4	Organization .....	3
3.5	Typical Questions Addressed .....	3
3.6	Additional Comments .....	3
4	ISA 99.00.3 – Operating a Manufacturing and Control Systems Security Program .....	4
4.1	Theme .....	4
4.2	Audience .....	4
4.3	Purpose .....	4
4.4	Organization .....	4
4.5	Typical Questions Addressed .....	4
4.6	Additional Comments .....	4
5	ISA 99.00.04 – Specific Security Requirements for Manufacturing and Control Systems .....	5
5.1	Theme .....	5
5.2	Audience .....	5
5.3	Purpose .....	5
5.4	Organization .....	5
5.5	Typical Questions Addressed .....	5
5.6	Additional Comments .....	5
6	ISA TR 99.00.01 – Technologies for Protecting Manufacturing and Control Systems .....	6
6.1	Theme .....	6

6.2	Audience.....	6
6.3	Purpose .....	6
6.4	Organization .....	6
6.5	Typical Questions Addressed.....	6
6.6	Additional Comments .....	6
7	Revision History.....	8



## 1 Introduction

The purpose of this document is to provide a general overview of the standards in the series “ISA-99: Manufacturing and Control Systems Security”. Content is described only for the purpose of explaining the general organization and coverage of topics.

### 1.1 Structure of the Standard

There are several standards in the ISA-99 series, each covering a specific aspect or subset of the subject of Manufacturing and Control Systems Security. They are:

- ISA 99.00.01 – Scope, Concepts, Models and Terminology
- ISA 99.00.02 – Establishing a Manufacturing and Control Systems Security Program
- ISA 99.00.03 – Operating a Manufacturing and Control Systems Security Program
- ISA 99.00.04 – Specific Security Requirements for Manufacturing and Control Systems

In addition to the standards, the committee has developed and released two technical reports. They are:

- ISA TR 99.00.01 – Technologies for Protecting Manufacturing and Control Systems
- ISA TR 99.00.02 – Integrating Electronic Security into the Manufacturing and Control Systems Environment

### 1.2 Standard Descriptions

Each standard in the series is described in more detail in subsequent sections of this document. For consistency, each description follows a common format, consisting of the following headings:

**Theme** – describes the general theme or subject of the standard. Each standard addresses a specific aspect of security for automation systems.

**Audience** – addresses the type of reader who might find the material in this standard useful.

**Purpose** – a specific purpose or set of objectives, in terms of the information conveyed and the level of understanding or awareness to be achieved.

**Organization** – a general description of how the material in this standard is organized, listing the major topics covered and describing how they are related.

**Questions Addressed** – a list of typical questions that could be addressed by the material in this standard.

**Additional Comments** – any additional information that supports the above descriptions.

Presenting the information in this form helps the reader determine where within the series of standards specific topics of interest are addressed, and how the various standards are related to one another.

## 2 ISA 99.00.01 – Scope, Concepts, Models and Terminology

### 2.1 Theme

Establish the scope and context of the ISA 99 series of standards by describing it from several different perspectives. Define the terminology used and provide framework within which to position the basic concepts related to Manufacturing and Control Systems security.

### 2.2 Audience

Anyone wishing to understand the basic scope of the subject.

### 2.3 Purpose

This standard presents the basic concepts and terminology that form the basis for the remaining standards in the series.

### 2.4 Organization

Content is organized into three major subject areas. The first is a glossary of terms and definitions. This is followed by a description of basic concepts. The final section describes several models that form the basis for the standard.

### 2.5 Typical Questions Addressed

- What is the scope of the ISA-99 series of standards?
- How does it relate to other standards addressing cyber security of industrial control systems?
- How is a control system different from a typical business system in the context of security?
- How are the various components of a control system treated in terms of security?
- What are the key security terms and concepts and how are they defined in this context?

### 2.6 Additional Comments

None

### 3 ISA 99.00.02 – Establishing a Manufacturing and Control Systems Security Program

#### 3.1 Theme

Give practical guidance and direction on how to establish the business case for a security program and how to design the program to meet your business needs.

#### 3.2 Audience

- Persons who have taken or been assigned the task of establishing such a program.
- Management who will be asked to provide support and resources

#### 3.3 Purpose

Provide the reader with a basic guidebook that can be used to assemble their program, without prescribing details for every industry type.

#### 3.4 Organization

The first topic addressed is how to establish the business case for a security system. This is followed by a description of the steps required. The key elements of a cyber security management system are described.

#### 3.5 Typical Questions Addressed

- What constitutes a minimum level to establishing a security program?
- How do I make a business case for security in Manufacturing and controls environment?
- What is the step-by-step process of building such a program?
- What skills and organizations need to be involved?
- What program features must be included in order to maximize my chances for success?
- What are some typical pitfalls to avoid?

#### 3.6 Additional Comments

The material in this standard is partially based on the previously released Technical Report 2.

## 4 ISA 99.00.3 – Operating a Manufacturing and Control Systems Security Program

### 4.1 Theme

Programs must be effectively transferred from "build mode" to "operate mode" and be regularly renewed in order to be successful in the long term. This standard provides more normative material related to measuring or assessing program effectiveness.

### 4.2 Audience

- Persons who have taken or been assigned the task of implementing and maintaining such a program.
- Operational and other personnel who will have to run such a program long-term.
- Management who will be asked to provide support and resources

### 4.3 Purpose

Describe how a security program is run after it is designed and implemented.

### 4.4 Organization

To be defined

### 4.5 Typical Questions Addressed

- What should the short-term and long-term responsible organization(s) look like?
- Who should be the responsible executive(s)?
- What do I do when the project team goes away?
- How do I keep a program relevant and effective in the face of changing technology and business needs?
- What kind and number of resources are required to run such a program?
- How do I work effectively with my IT and audit organizations?
- What metrics are used or required to assess the effectiveness of the program?

### 4.6 Additional Comments

The ISA 99.00.3 standard provides a logical step from planning to execution. There are many aspects of running a security program that are different between these two steps, and this breakdown helps address this need. This would include more details on the periodic audit, metrics, performance evaluation, and policy implementation and management.

## 5 ISA 99.00.04 – Specific Security Requirements for Manufacturing and Control Systems

### 5.1 Theme

Focus on those operational and design requirements that "set apart" manufacturing and control systems from "traditional" IT systems.

### 5.2 Audience

- Anyone providing products or services related to manufacturing and Control Systems
- Security professionals from outside of Manufacturing or Operations who wish to understand these special needs.

### 5.3 Purpose

Define the requirements for the security of Manufacturing and Control Systems. Particular emphasis is placed on characteristics that differentiate M&CS systems from other Information Technology systems from a security point of view.

### 5.4 Organization

To be defined

### 5.5 Typical Questions Addressed

- What is "special" about the Manufacturing and Controls Environment that it requires different policies, procedures, and technologies?
- What are the metrics that should be used in selecting, designing, building, and maintaining secure automation systems?

### 5.6 Additional Comments

The intent is to provide a reference as to what are the measures necessary for end users to ensure that they are selecting controls and components that are appropriate to their environment, and to give them the measures as a standard reference that all vendors would start to use to describe their products.

## 6 ISA TR 99.00.01 – Technologies for Protecting Manufacturing and Control Systems

### 6.1 Theme

This technical report provides a reference for the selection of security technologies for protecting Manufacturing and Controls assets. This will always remain a technical report to facilitate the committee being able to quickly revise and publish this as the technology changes over time

### 6.2 Audience

IT professionals, engineers, and other individuals that are involved in the process of selecting and implement security technologies,

### 6.3 Purpose

Communicate to the reader the current state of control systems security, technologies for protecting them, and to provide a common reference by which persons implementing ISA 99 can look back upon to select security technologies.

### 6.4 Organization

The first topic addressed is common terms and definitions. This is followed by a general overview of the content of the document. The remaining sections describe various classes of security technologies in more detail, including:

- authentication and authorization
- filtering, blocking and access control
- audit, measurement, monitoring and detection
- computer software
- physical security controls

### 6.5 Typical Questions Addressed

- What are the appropriate tools to protect manufacturing and control system environment?
- What are the typical weaknesses and strengths of these tools?
- What are the current technical issues with control systems that affect cyber security technology?

### 6.6 Additional Comments

The current edition of this report covers only security technologies and their strengths/weaknesses in the manufacturing environment. Eventually this should be expanded to include traditional strengths and weaknesses of the different types of control systems (DCS, PLC, SCADA, HMI, etc)

## 7 ISA TR 99.00.02 – Integrating Electronic Security into the Manufacturing and Control Systems Environment

### 7.1 Theme

This technical report provides a framework for developing an electronic security program and provides a recommended organization and structure for the security plan.

### 7.2 Audience

IT professionals, engineers, and other individuals that are involved in the process of selecting and implement security technologies.

### 7.3 Purpose

The purpose of this technical report was to establish the basic scope and foundation of what was to become part 2 of the formal standard. For that reason, when work on ISA 99.00.02 is complete and the standard is published, this report will most likely be withdrawn.

### 7.4 Organization

The content of this document is organized to reflect the major steps required in establishing an electronic security program. These steps range from defining the risk goals, through conducting risk assessments to conducting periodic audits.

Appendices are included that show examples of the supporting documents and procedures.

### 7.5 Typical Questions Addressed

The questions addressed are essentially the same as those for ISA 99.00.02. They include:

- What constitutes a minimum level to establishing a security program?
- How do I make a business case for security in Manufacturing and controls environment?
- What is the step-by-step process of building such a program?
- What skills and organizations need to be involved?
- What program features must be included in order to maximize my chances for success?
- What are some typical pitfalls to avoid?

### 7.6 Additional Comments

None

## 8 Revision History

<b>Revision</b>	<b>Date</b>	<b>Revised By</b>	<b>Comments</b>
1	September 2005	Eric Cosman	Initial Draft
2	October 2005	Eric Cosman	Updated based on comments from SP99 leaders group
3	November 2005	Eric Cosman	Minor edits
4	November 2005	Eric Cosman	Added references to technical reports 1 and 2, and a description of the content of technical report 2.