AMERICAN NATIONAL STANDARD

ANSI/ISA–99.00.01–2007

Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models

Approved 29 October 2007

ANSI/ISA–99.00.01–2007
Security for Industrial Automation and Control Systems
Part 1: Terminology, Concepts, and Models

ISBN: 978-1-934394-37-3

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

Preface

This preface, as well as all footnotes and annexes, is included for information purposes and is not part of ANSI/ISA–99.00.01–2007.

This document has been prepared as part of the service of ISA, 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.

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 standard, 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 standard or a license on reasonable terms and conditions that are free from unfair discrimination.

Even if ISA is unaware of any patent covering this standard, the user is cautioned that implementation of the standard 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 standard. ISA is not responsible for identifying all patents that may require a license before implementation of the standard or for investigating the validity or scope of any patents brought to its attention. The user should carefully investigate relevant patents before using the standard for the user's intended application.

However, ISA asks that anyone reviewing this standard who is aware of any patents that may impact implementation of the standard notify the ISA Standards and Practices Department of the patent and its owner.

Additionally, the use of this standard may involve hazardous materials, operations or equipment. The standard cannot anticipate all possible applications or address all possible safety issues associated with use in hazardous conditions.

The user of this standard 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 standard.

The following participated as voting members of ISA99 in the development of this standard:

NAME	**COMPANY**
B. Singer, Chair	Fluid IQs
R. Webb, Managing Director	Consultant
E. Cosman, Lead Editor	The Dow Chemical Co.
R. Bhojani	Bayer Technology Services
M. Braendle	ABB
D. Brandl	BR&L Consulting, Inc.
E. Byres	Byres Security, Inc.
R. Clark	Invensys Systems, Inc. / Wonderware
A. Cobbett	BP Process Control Digital Protection
J. Dalzon	ISA France
T. Davis	Citect
R. Derynck	Verano, Inc.
R. Evans	Idaho National Laboratory
R. Forrest	The Ohio State University
J. Gilsinn	NIST/MEL
T. Glenn	Yokogawa
T. Good	E I DuPont De Nemours & Co.
E. Hand	Sara Lee Food & Beverage
M. Heard	Eastman Chemical Co.
D. Holstein	OPUS Publishing
C. Hoover	Rockwell Automation
B. Huba	Emerson Processing Management
M. Lees	Schering-Plough Corp.
C. Mastromonico	Westinghouse Savannah River Co.
D. Mills	Procter & Gamble Co.
G. Morningstar	Cedar Rapids Water Dept.
A. Nangia	3M
J. Nye	ExxonMobil Research and Engineering
T. Phinney	Honeywell ACS Adv Tech Lab
E. Rakaczky	Invensys Systems Canada Inc.
C. Sossman	WGI-W Safety Management Solutions LLC
L. Steinocher	Fluor Enterprises, Inc.
I. Susanto	Chevron Information Technology Co.
B. Taylor	The George Washington University
D. Teumim	Teumim Technical LLC
D. Tindill	Matrikon Inc.
L. Uden	Lyondell Chemical Co.
J. Weiss	Applied Control Solutions, LLC
M. Widmeyer	Consultant
L. Winkel	Siemens SG

The following served as active members of ISA99 Working Group 3 in the preparation of this standard:

Name	**Company**	**Contributor**	**Reviewer**
E. Cosman, Lead Editor	The Dow Chemical Co.	√	
J. Bauhs	Cargill	√	
R. Bhojani	Bayer	√	
M. Braendle	ABB		√
D. Brandl	BR&L Consulting, Inc.		√

M. Bush	Rockwell Automation	√	
E. Byres	Byres Security, Inc.		√
A. Capel	Comgate Engineering Ltd.		√
L. Capuder	Aramco		√
R. Clark	Invensys Wonderware		√
A. Cobbett	BP		√
J. Dalzon	ISA France		√
H. Daniel	Consultant	√	
A. Daraiseh	Saudi Aramco		√
R. Derynck	Verano, Inc.	√	
G. Dimowo	Shell		√
D. Elley	Aspen Technology, Inc.	√	
R. Evans	Idaho National Laboratories		√
J. Gilsinn	NIST/MEL		√
T. Glenn	Yokogawa		√
T. Good	DuPont	√	
R. Greenthaler	TXU Energy		√
E. Hand	Sara Lee Food & Beverage	√	
D. Holstein	OPUS Publishing	√	
C. Hoover	Rockwell Automation	√	
M. Jansons	Siemens	√	
R. Lara	Invensys		√
J. Lellis	Aspen Technology, Inc.		√
D. Mills	Procter & Gamble Co.		√
C. Muehrcke	Cyber Defense Agency		√
M. Naedele	ABB		√
J. Nye	ExxonMobil	√	
R. Oyen	Consultant	√	√
D. Peterson	Digital Bond		√
T. Phinney	Honeywell		√
J. Potter	Emerson		√
E. Rakaczky	Invensys		√
J. Seest	Novo Nordisk A/S	√	
B. Singer, ISA99 Chair	Fluid IQs	√	
L. Steinocher	Fluor Enterprises, Inc.		√
I. Susanto	Chevron		√
E. Tieghi	ServiTecno SRL		√
R. Webb	Consultant		√

J. Weiss	Applied Control Solutions LLC		√
L. Winkel	Siemens SG		√

The ISA Standards and Practices Board approved the first edition of this technical report for publication on 27 September 2007:

NAME	**COMPANY**
T. McAvinew, Chair	Jacobs Engineering Group
M. Coppler	Ametek, Inc.
E. Cosman	The Dow Chemical Co.
B. Dumortier	Schneider Electric
D. Dunn	Aramco Services Co.
J. Gilsinn	NIST/MEL
W. Holland	Consultant
E. Icayan	ACES, Inc.
J. Jamison	Consultant
K. Lindner	Endress & Hauser Process Solutions AG
V. Maggioli	Feltronics Corp.
A. McCauley, Jr.	Chagrin Valley Controls, Inc.
G. McFarland	Emerson Process Management
R. Reimer	Rockwell Automation
N. Sands	E I du Pont
H. Sasajima	Yamatake Corp.
T. Schnaare	Rosemount, Inc.
J. Tatera	Consultant
I. Verhappen	MTL Instrument Group
R. Webb	Consultant
W. Weidman	Parsons Energy & Chemicals Group
J. Weiss	Applied Control Solutions LLC
M. Widmeyer	Consultant
M. Zielinski	Emerson Process Management

This page intentionally left blank

Table of Contents

Figures

Tables

Foreword

This is the first in a series of ISA standards that addresses the subject of security for industrial automation and control systems. The focus is on the electronic security of these systems, commonly referred to as cyber security. This Part 1 standard describes the basic concepts and models related to cyber security.

This standard is structured to follow ISO/IEC directives part 2 for standards development as closely as possible. An introduction before the first numbered clause describes the range of coverage of the entire series of standards. It defines industrial automation and control systems and provides various criteria to determine whether a particular item is included within the scope of the standards.

Clause 1 defines the scope of this standard.

Clause 2 lists normative references that are indispensable for the application of this document.

Clause 3 is a list of terms and definitions used in this standard. Most are drawn from established references, but some are derived for the purpose of this standard.

Clause 4 provides an overview of the current situation with respect to the security of industrial automation and control systems, including trends and their potential impact.

Clause 5 contains a broad description of the subject and the basic concepts that establish the scope of industrial automation and control systems security. Many of these concepts are well established within the security discipline, but their applicability to industrial control systems may not have been clearly described. In some cases the nature of industrial control systems leads to an interpretation that may be different from that used for more general information technology applications.

Clause 6 describes a series of models that are used to apply the basic concepts of security for industrial automation and control systems. As with the concepts, several models are based on more generic views, with some aspects adjusted to address specific aspects of industrial control system applications.

The ISA99 Series

Standards in the ISA99 series address the application of these concepts and models in areas such as security program definition and minimum security requirements. The series includes the following standards.

1. **ISA99.00.01 – Part 1: Terminology, Concepts and Models**

   Part 1 (this standard) establishes the context for all of the remaining standards in the series by defining a common set of terminology, concepts and models for electronic security in the industrial automation and control systems environment.

2. **ISA99.00.02 – Part 2: Establishing an Industrial Automation and Control System Security Program**

   Part 2 will describe the elements of a cyber security management system and provide guidance for their application to industrial automation and control systems.

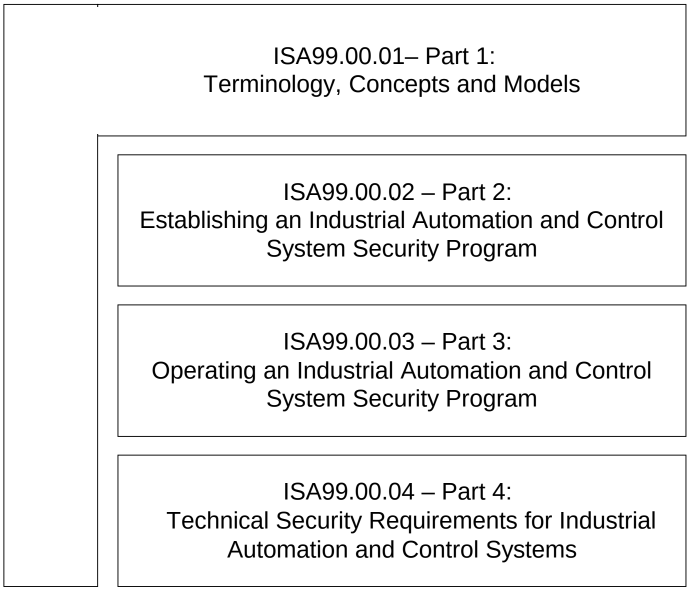
3. **ISA99.00.03 – Part 3: Operating an Industrial Automation and Control System Security Program**

   Part 3 will address how to operate a security program after it is designed and implemented. This includes definition and application of metrics to measure program effectiveness.

4. **ISA99.00.04 – Part 4: Technical Security Requirements for Industrial Automation and Control Systems**

   Part 4 will define the characteristics of industrial automation and control systems that differentiate them from other information technology systems from a security point of view. Based on these characteristics, the standard will establish the security requirements that are unique to this class of systems.

The relationship between the standards in this series is shown in the following diagram:


ISA99.00.01– Part 1:
Terminology, Concepts and Models
ISA99.00.02 – Part 2:
Establishing an Industrial Automation and Control System Security Program
ISA99.00.03 – Part 3:
Operating an Industrial Automation and Control System Security Program
ISA99.00.04 – Part 4:
Technical Security Requirements for Industrial Automation and Control Systems

Relationships of the ISA99 Standards

In addition, the ISA99 committee has produced two technical reports on the subject of electronic security within the industrial automation and control systems environment.

1. **ANSI/ISA-TR99.00.01-2007 – Technologies for Protecting Manufacturing and Control Systems**

   Technical Report 1, updated from the original 2004 version, describes various security technologies in terms of their applicability for use with industrial automation and control systems. This technical report will be updated periodically to reflect changes in technology.

2. **ANSI/ISA-TR99.00.02-2004 – Integrating Electronic Security into the Manufacturing and Control Systems Environment**

   Technical Report 2 describes how electronic security can be integrated into industrial automation and control systems. The contents of this technical report will be superseded with the completion of the Part 2 standard.

Introduction

The subject of this standard is *security for industrial automation and control systems*. In order to address a range of applications (i.e., industry types), each of the terms in this description have been interpreted very broadly.

The term *industrial automation and control systems (IACS)* includes control systems used in manufacturing and processing plants and facilities, building environmental control systems, geographically dispersed operations such as utilities (i.e., electricity, gas, and water), pipelines and petroleum production and distribution facilities, and other industries and applications such as transportation networks, that use automated or remotely controlled or monitored assets.

The term s*ecurity* is considered here to mean the prevention of illegal or unwanted penetration, intentional or unintentional interference with the proper and intended operation, or inappropriate access to confidential information in industrial automation and control systems. *Electronic security,* the particular focus of this standard, includes computers, networks, operating systems, applications and other programmable configurable components of the system.

The audience for this standard includes all users of industrial automation and control systems (including facility operations, maintenance, engineering, and corporate components of user organizations), manufacturers, suppliers, government organizations involved with, or affected by, control system cyber security, control system practitioners, and security practitioners. Because mutual understanding and cooperation between information technology (IT) and operations, engineering, and manufacturing organizations is important for the overall success of any security initiative, this standard is also a reference for those responsible for the integration of industrial automation and control systems and enterprise networks.

Typical questions addressed by this Part 1 standard include:

a) What is the general scope of application for “industrial automation and control systems security”?

b) How can the needs and requirements of a security system be defined using consistent terminology?

c) What are the basic concepts that form the foundation for further analysis of the activities, system attributes, and actions that are important to provide electronically secure control systems?

d) How can the components of an industrial automation and control system be grouped or classified for the purpose of defining and managing security?

e) What are the different electronic security objectives for control system applications?

f) How can these objectives be established and codified?

Each of these questions is addressed in detail in subsequent clauses of this standard.

1 Scope

This standard defines the terminology, concepts and models for industrial automation and control systems (IACS) security. It establishes the basis for the remaining standards in the ISA99 series.

To fully articulate the systems and components the ISA99 standards address, the range of coverage may be defined and understood from several perspectives, including:

a) range of functionality included

b) specific systems and interfaces

c) criteria for selecting included activities

d) criteria for selecting included assets

Each of these is described in the following paragraphs.

Functionality Included

The scope of this standard can be described in terms of the range of functionality within an organization's information and automation systems. This functionality is typically described in terms of one or more models.

This standard is focused primarily on industrial automation and control, as described in a reference model (see clause 6). Business planning and logistics systems are not explicitly addressed within the scope of this standard, although the integrity of data exchanged between business and industrial systems is considered.

Industrial automation and control includes the supervisory control components typically found in process industries. It also includes SCADA (supervisory control and data acquisition) systems that are commonly used by organizations that operate in critical infrastructure industries. These include:

a) electricity transmission and distribution

b) gas and water distribution networks

c) oil and gas production operations

d) gas and liquid transmission pipelines

This is not an exclusive list. SCADA systems may also be found in other critical and non-critical infrastructure industries.