FOR REVIEW PURPOSES ONLY!

THIS ISA99 COMMITTEE WORK PRODUCT HAS BEEN APPROVED AND THE FINAL VERSION IS AVAILABLE FOR PURCHASE ON THE ISA WEB SITE.

THIS EXCERPT IS PROVIDED SOLELY FOR THE PURPOSE OF REVIEW IN SUPPORT OF THE FURTHER DEVELOPMENT OF OTHER COMMITTEE WORK PRODUCTS.

THIS DOCUMENT MAY NOT BE COPIED, DISTRIBUTED TO OTHERS OR OFFERED FOR FURTHER REPRODUCTION OR SALE.

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

This page intentionally left blank

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 standard 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

Table of Contents

Foreword **11**

Introduction **13**

1 Scope **15**

2 Normative References **18**

3 Definitions **19**

3.1 Introduction 19
3.2 Terms 19
3.3 Abbreviations 31

4 The Situation **32**

4.1 General 32
4.2 Current Systems 32
4.3 Current Trends 33
4.4 Potential Impact 33

5 Concepts **35**

5.1 General 35
5.2 Security Objectives 35
5.3 Defense in Depth 36
5.4 Security Context 36
5.5 Threat-Risk Assessment 37
5.6 Security Program Maturity 44
5.7 Policies 49
5.8 Security Zones 54
5.9 Conduits 55
5.10 Security Levels 57
5.11 Security Level Lifecycle 61

6 Models **66**

6.1 General 66
6.2 Reference Models 66
6.3 Asset Models 70
6.4 Reference Architecture 74
6.5 Zone and Conduit Model 75

6.6 Model Relationships 84

Figures

Figure 1 – Comparison of Objectives 35

Figure 2 – Context Element Relationships 37

Figure 3 – Context Model 37

Figure 4 – Integration of Business and IACS Cyber Security 45

Figure 5 – Cyber Security Level over Time 45

Figure 6 – Integration of Resources to Develop the CSMS 46

Figure 7 – Conduit Example 56

Figure 8 – Security Level Lifecycle 62

Figure 9 – Security Level Lifecycle – Assess Phase 63

Figure 10 – Security Level Lifecycle – Implement Phase 64

Figure 11 – Security Level Lifecycle – Maintain Phase 65

Figure 12 – Reference Model for ISA99 Standards 67

Figure 13 – SCADA Reference Model 67

Figure 14 – Process Manufacturing Asset Model Example 71

Figure 15 – SCADA System Asset Model Example 72

Figure 16 – Reference Architecture Example 74

Figure 17 – Multiplant Zone Example 76

Figure 18 – Separate Zones Example 77

Figure 19 – SCADA Zone Example 78

Figure 20 – SCADA Separate Zones Example 79

Figure 21 – Enterprise Conduit 82

Figure 22 – SCADA Conduit Example 83

Figure 23 – Model Relationships 85

Tables

Table 1 – Types of Loss by Asset Type 39
Table 2 – Security Maturity Phases 47
Table 3 – Concept Phase 47
Table 4 – Functional Analysis Phase 48
Table 5 – Implementation Phase 48
Table 6 – Operations Phase 49
Table 7 – Recycle and Disposal Phase 49
Table 8 – Security Levels 57

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.

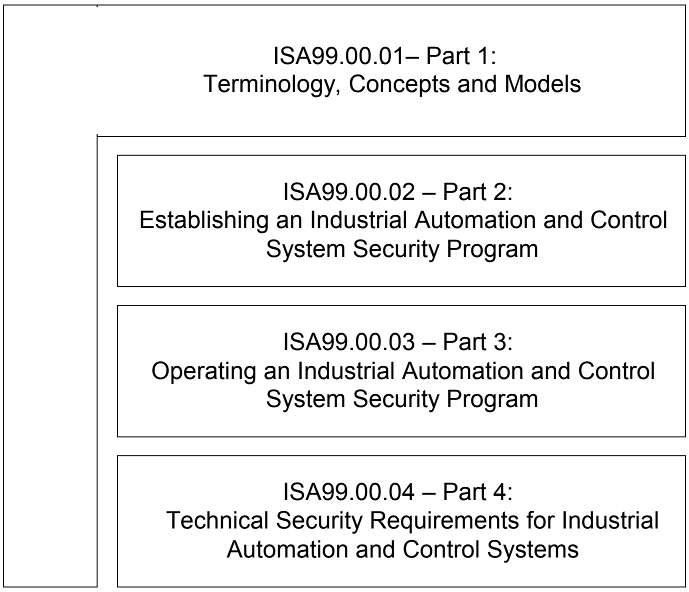
3. **ISA99.00.03 – Part 3: Operating an Industrial Automation and Control System Security Program**

   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.

This page intentionally left blank.

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.

Systems and interfaces

In encompassing all industrial automation and control systems, this standard covers systems that can affect or influence the safe, secure, and reliable operation of industrial processes. They include, but are not limited to:

a) Industrial control systems and their associated communications networks[1], including distributed control systems (DCSs), programmable logic controllers (PLCs), remote terminal units (RTUs), intelligent electronic devices, SCADA systems, networked electronic sensing and control, metering and custody transfer systems, and monitoring and diagnostic systems. (In this context, industrial control systems include basic process control system and safety-instrumented system [SIS] functions, whether they are physically separate or integrated.)

[1] The term “communications networks” includes all types of communications media, including various types of wireless communications. A detailed description of the use of wireless communications in industrial automation systems is beyond the scope of this standard. Wireless communication

b) Associated systems at level 3 or below of the reference model described in clause 6. Examples include advanced or multivariable control, online optimizers, dedicated equipment monitors, graphical interfaces, process historians, manufacturing execution systems, pipeline leak detection systems, work management, outage management, and electricity energy management systems.

c) Associated internal, human, network, software, machine or device interfaces used to provide control, safety, manufacturing, or remote operations functionality to continuous, batch, discrete, and other processes.

Activity-based criteria

ANSI/ISA-95.00.03 [5, Annex A] defines a set of criteria for defining activities associated with manufacturing operations. A similar list has been developed for determining the scope of this standard. A system should be considered to be within the range of coverage of these standards if the activity it performs is necessary for any of the following:

a) predictable operation of the process

b) process or personnel safety

c) process reliability or availability

d) process efficiency

e) process operability

f) product quality

g) environmental protection

h) regulatory compliance

i) product sales or custody transfer.

Asset-based criteria

The coverage of this standard includes those systems in assets that meet any of the following criteria, or whose security is essential to the protection of other assets that meet these criteria:

a) The asset has economic value to a manufacturing or operating process.

b) The asset performs a function necessary to operation of a manufacturing or operating process.

c) The asset represents intellectual property of a manufacturing or operating process.

d) The asset is necessary to operate and maintain security for a manufacturing or operating process.

e) The asset is necessary to protect personnel, contractors, and visitors involved in a manufacturing or operating process.

f) The asset is necessary to protect the environment.

g) The asset is necessary to protect the public from events caused by a manufacturing or operating process.

h) The asset is a legal requirement, especially for security purposes of a manufacturing or operating process.

techniques are specifically mentioned only in situations where their use or application may change the nature of the security applied or required.

i) The asset is needed for disaster recovery.

j) The asset is needed for logging security events.

This range of coverage includes 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, environmental contamination, and/or economic loss or impact on an entity or on local or national security.

2 Normative References

The following referenced documents are indispensable for the application of this standard. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ANSI/ISA-95.00.01-2000, Enterprise-Control System Integration Part 1: Models and Terminology, Clause 5 (Hierarchy Models)

ISA-88.01-1995 (R 2006), Batch Control Part 1: Models and Terminology, Clause 4.2 (Physical Model)

ISO/IEC 15408-1: Information technology — Security techniques — Evaluation criteria for IT security – Part 1: Introduction and General Model, Clause 4 (General Model)

3 Definitions

3.1 Introduction

This clause defines the terms and abbreviations used in this standard.

Wherever possible, definitions have been adapted from those used in established industry sources. Those definitions are marked to indicate the reference listed in the bibliography.

Some definitions have been adapted from more generic definitions used in the IT industry.

3.2 Terms

The following terms are referenced in this standard.

3.2.1 access

ability and means to communicate with or otherwise interact with a system in order to use system resources.

NOTE: Access may involve physical access (authorization to be allowed physically in an area, possession of a physical key lock, PIN code, or access card or biometric attributes that allow access) or logical access (authorization to log in to a system and application, through a combination of logical and physical means)

3.2.2 access control

protection of system resources against unauthorized access; a process by which use of system resources is regulated according to a security policy and is permitted by only authorized entities (users, programs, processes, or other systems) according to that policy [11].

3.2.3 accountability

property of a system (including all of its system resources) that ensures that the actions of a system entity may be traced uniquely to that entity, which can be held responsible for its actions [11].

3.2.4 application

software program that performs specific functions initiated by a user command or a process event and that can be executed without access to system control, monitoring, or administrative privileges [9].

3.2.5 area

subset of a site’s physical, geographic, or logical group of assets.

NOTE: An area may contain manufacturing lines, process cells, and production units. Areas may be connected to each other by a site local area network and may contain systems related to the operations performed in that area.

3.2.6 asset

physical or logical object owned by or under the custodial duties of an organization, having either a perceived or actual value to the organization.

NOTE: In the case of industrial automation and control systems the physical assets that have the largest directly measurable value may be the equipment under control.

3.2.7 association

cooperative relationship between system entities, usually for the purpose of transferring information between them [11].

3.2.8 assurance

attribute of a system that provides grounds for having confidence that the system operates such that the system security policy is enforced.

3.2.9 attack

assault on a system that derives from an intelligent threat — i.e., an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system [11].

NOTE: There are different commonly recognized classes of attack:

An "active attack" attempts to alter system resources or affect their operation. A "passive attack" attempts to learn or make use of information from the system but does not affect system resources.

An "inside attack" is an attack initiated by an entity inside the security perimeter (an "insider") – i.e., an entity that is authorized to access system resources but uses them in a way not approved by those who granted the authorization. An "outside attack" is initiated from outside the perimeter, by an unauthorized or illegitimate user of the system (including an insider attacking from outside the security perimeter). Potential outside attackers range from amateur pranksters to organized criminals, international terrorists, and hostile governments.

3.2.10 attack tree

formal, methodical way of finding ways to attack the security of a system.

3.2.11 audit

independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures (See *“security audit*”) [9].

NOTE: There are three forms of audit. (1) External audits are conducted by parties who are not employees or contractors of the organization. (2) Internal audit are conducted by a separate organizational unit dedicated to internal auditing. (3) Controls self assessments are conducted by peer members of the process automation function.

3.2.12 authenticate

verify the identity of a user, user device, or other entity, or the integrity of data stored, transmitted, or otherwise exposed to unauthorized modification in an information system, or to establish the validity of a transmission.

3.2.13 authentication

security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information [9].

3.2.14 authorization

right or a permission that is granted to a system entity to access a system resource [11].

3.2.15 automated vehicle

mobile device that includes a control system allowing it to operate either autonomously or under remote control.

3.2.16 availability

probability that an asset, under the combined influence of its reliability, maintainability, and security, will be able to fulfill its required function over a stated period of time, or at a given point in time.

3.2.17 border

edge or boundary of a physical or logical security zone.

3.2.18 botnet

collection of software robots, or bots, which run autonomously.

NOTE: A botnet's originator can control the group remotely, possibly for nefarious purposes.

3.2.19 boundary

software, hardware, or other physical barrier that limits access to a system or part of a system [9].

3.2.20 channel

specific communication link established within a communication conduit (See “*conduit*”).

3.2.21 ciphertext

data that has been transformed by encryption so that its semantic information content (i.e., its meaning) is no longer intelligible or directly available.

3.2.22 client

device or application receiving or requesting services or information from a server application [12].

3.2.23 communication path

logical connection between a source and one or more destinations, which could be devices, physical processes, data items, commands, or programmatic interfaces.

NOTE: The communication path is not limited to wired or wireless networks, but includes other means of communication such as memory, procedure calls, state of physical plant, portable media, and human interactions.

3.2.24 communication security

(1) measures that implement and assure security services in a communication system, particularly those that provide data confidentiality and data integrity and that authenticate communicating entities.

(2) state that is reached by applying security services, in particular, state of data confidentiality, integrity, and successfully authenticated communications entities [11].

NOTE: This phrase is usually understood to include cryptographic algorithms and key management methods and processes, devices that implement them, and the life-cycle management of keying material and devices. However, cryptographic algorithms and key management methods and processes may not be applicable to some control system applications.

3.2.25 communication system

arrangement of hardware, software, and propagation media to allow the transfer of messages (ISO/IEC 7498 application layer service data units) from one application to another.

3.2.26 compromise

unauthorized disclosure, modification, substitution, or use of information (including plaintext cryptographic keys and other critical security parameters) [13].

3.2.27 conduit

logical grouping of communication assets that protects the security of the channels it contains.

NOTE: This is analogous to the way that a physical conduit protects cables from physical damage.

3.2.28 confidentiality

assurance that information is not disclosed to unauthorized individuals, processes, or devices [9].

3.2.29 control center

central location used to operate a set of assets.

NOTE: Infrastructure industries typically use one or more control centers to supervise or coordinate their operations. If there are multiple control centers (for example, a backup center at a separate site), they are typically connected together via a wide area network. The control center contains the SCADA host computers and associated operator display devices plus ancillary information systems such as a historian.

NOTE: In some industries the term “control room” may be more commonly used.

3.2.30 control equipment

class that includes distributed control systems, programmable logic controllers, SCADA systems, associated operator interface consoles, and field sensing and control devices used to manage and control the process.

NOTE: The term also includes field bus networks where control logic and algorithms are executed on intelligent electronic devices that coordinate actions with each other, as well as systems used to monitor the process and the systems used to maintain the process.

3.2.31 control network

time-critical network that is typically connected to equipment that controls physical processes (See *“safety network”).*

NOTE: The control network can be subdivided into zones, and there can be multiple separate control networks within one company or site.

3.2.32 cost

value of impact to an organization or person that can be measured.

3.2.33 countermeasure

action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken [11].

NOTE: The term “Control” is also used to describe this concept in some contexts. The term countermeasure has been chosen for this standard to avoid confusion with the word control in the context of “process control.”

3.2.34 cryptographic algorithm

algorithm based upon the science of cryptography, including encryption algorithms, cryptographic hash algorithms, digital signature algorithms, and key agreement algorithms.

3.2.35 cryptographic key

input parameter that varies the transformation performed by a cryptographic algorithm [11].

NOTE: Usually shortened to just "key."

3.2.36 data confidentiality

property that information is not made available or disclosed to any unauthorized system entity, including unauthorized individuals, entities, or processes [7].

3.2.37 data integrity

property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner [11].

NOTE: This term deals with constancy of and confidence in data values, not with the information that the values represent or the trustworthiness of the source of the values.

3.2.38 decryption

process of changing cipher text into plaintext using a cryptographic algorithm and key (See *“encryption”)* [11].

3.2.39 defense in depth

provision of multiple security protections, especially in layers, with the intent to delay if not prevent an attack.

NOTE: Defense in depth implies layers of security and detection, even on single systems, and provides the following features:

a. attackers are faced with breaking through or bypassing each layer without being detected

b. a flaw in one layer can be mitigated by capabilities in other layers

c. system security becomes a set of layers within the overall network security.

3.2.40 demilitarized zone

perimeter network segment that is logically between internal and external networks [9].

NOTE: The purpose of a demilitarized zone is to enforce the internal network’s policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal network from outside attacks.

NOTE: In the context of industrial automation and control systems, the term “internal network” is typically applied to the network or segment that is the primary focus of protection. For example, a control network could be considered “internal” when connected to an “external” business network.

3.2.41 denial of service

prevention or interruption of authorized access to a system resource or the delaying of system operations and functions [11].

NOTE: In the context of industrial automation and control systems, denial of service can refer to loss of process function, not just loss of data communications.

3.2.42 digital signature

result of a cryptographic transformation of data which, when properly implemented, provides the services of origin authentication, data integrity, and signer non-repudiation [12].

3.2.43 distributed control system

type of control system in which the system elements are dispersed but operated in a coupled manner.

NOTE: Distributed control systems may have shorter coupling time constants than those typically found in SCADA systems.

NOTE: Distributed control systems are commonly associated with continuous processes such as electric power generation; oil and gas refining; chemical, pharmaceutical and paper manufacture, as well as discrete processes such as automobile and other goods manufacture, packaging, and warehousing.

3.2.44 domain

environment or context that is defined by a security policy, security model, or security architecture to include a set of system resources and the set of system entities that have the right to access the resources [11].

3.2.45 eavesdropping

monitoring or recording of communicated information by unauthorized parties.

3.2.46 electronic security

actions required to preclude unauthorized use of, denial of service to, modifications to, disclosure of, loss of revenue from, or destruction of critical systems or informational assets.

NOTE: The objective is to reduce the risk of causing personal injury or endangering public health, losing public or consumer confidence, disclosing sensitive assets, failing to protect business assets or failing to comply with regulations. These concepts are applied to any system in the production process and include both stand-alone 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. Electronic security includes the concepts of identification, authentication, accountability, authorization, availability, and privacy.

3.2.47 encryption

cryptographic transformation of plaintext into ciphertext that conceals the data’s original meaning to prevent it from being known or used (See *“decryption”)* [11].

NOTE: If the transformation is reversible, the corresponding reversal process is called "decryption," which is a transformation that restores encrypted data to its original state.

3.2.48 enterprise

business entity that produces or transports products or operates and maintains infrastructure services.

3.2.49 enterprise system

collection of information technology elements (i.e., hardware, software and services) installed with the intent to facilitate an organization’s business process or processes (administrative or project).

3.2.50 equipment under control

equipment, machinery, apparatus or plant used for manufacturing, process, transportation, medical or other activities [14].

3.2.51 field I/O network

communications link (wired or wireless) that connects sensors and actuators to the control equipment.

3.2.52 firewall

inter-network connection device that restricts data communication traffic between two connected networks [11].

NOTE: A firewall may be either an application installed on a general-purpose computer or a dedicated platform (appliance) that forwards or rejects/drops packets on a network. Typically firewalls are used to define zone borders. Firewalls generally have rules restricting which ports are open.

3.2.53 gateway

relay mechanism that attaches to two (or more) computer networks that have similar functions but dissimilar implementations and that enables host computers on one network to communicate with hosts on the other [11].

NOTE: Also described as an intermediate system that is the translation interface between two computer networks.

3.2.54 geographic site

subset of an enterprise’s physical, geographic, or logical group of assets.

NOTE: A geographic site may contain areas, manufacturing lines, process cells, process units, control centers, and vehicles and may be connected to other sites by a wide area network.

3.2.55 guard

gateway that is interposed between two networks (or computers or other information systems) operating at different security levels (one network is usually more secure than the other) and is trusted to mediate all information transfers between the two networks, either to ensure that no sensitive information from the more secure network is disclosed to the less secure network, or to protect the integrity of data on the more secure network [11].

3.2.56 host

computer that is attached to a communication subnetwork or inter-network and can use services provided by the network to exchange data with other attached systems [11].

3.2.57 industrial automation and control systems

collection of personnel, hardware, and software that can affect or influence the safe, secure, and reliable operation of an industrial process.

NOTE: These systems include, but are not limited to:

a. industrial control systems, including distributed control systems (DCSs), programmable logic controllers (PLCs), remote terminal units (RTUs), intelligent electronic devices, supervisory control and data acquisition (SCADA), networked electronic sensing and control, and monitoring and diagnostic systems. (In this context, process control systems include basic process control system and safety-instrumented system [SIS] functions, whether they are physically separate or integrated.)

b. associated information systems such as advanced or multivariable control, online optimizers, dedicated equipment monitors, graphical interfaces, process historians, manufacturing execution systems, and plant information management systems.

c. associated internal, human, network, or machine interfaces used to provide control, safety, and manufacturing operations functionality to continuous, batch, discrete, and other processes.

3.2.58 initial risk

risk before controls or countermeasures have been applied (See *“risk”*).

3.2.59 insider

“trusted” person, employee, contractor, or supplier who has information that is not generally known to the public (See *“outsider”*).

3.2.60 integrity

quality of a system reflecting the logical correctness and reliability of the operating system, the logical completeness of the hardware and software implementing the protection mechanisms, and the consistency of the data structures and occurrence of the stored data [9].

NOTE: In a formal security mode, integrity is often interpreted more narrowly to mean protection against unauthorized modification or destruction of information.

3.2.61 interception

capture and disclosure of message contents or use of traffic analysis to compromise the confidentiality of a communication system based on message destination or origin, frequency or length of transmission, and other communication attributes.

3.2.62 interface

logical entry or exit point that provides access to the module for logical information flows.

3.2.63 intrusion

unauthorized act of compromising a system (See *“attack”).*

3.2.64 intrusion detection

security service that monitors and analyzes system events for the purpose of finding, and providing real-time or near real-time warning of, attempts to access system resources in an unauthorized manner.

3.2.65 IP address

address of a computer or device that is assigned for identification and communication using the Internet Protocol and other protocols.

3.2.66 ISO

International Organization for Standardization[1].

3.2.67 key management

process of handling and controlling cryptographic keys and related material (such as initialization values) during their life cycle in a cryptographic system, including ordering, generating, distributing, storing, loading, escrowing, archiving, auditing, and destroying the keys and related material [11].

3.2.68 lines, units, cells

lower-level elements that perform manufacturing, field device control, or vehicle functions.

NOTE: Entities at this level may be connected together by an area control network and may contain information systems related to the operations performed in that entity.

3.2.69 local area network

communications network designed to connect computers and other intelligent devices in a limited geographic area (typically less than 10 kilometers) [10].

3.2.70 malicious code

programs or code written for the purpose of gathering information about systems or users, destroying system data, providing a foothold for further intrusion into a system, falsifying system data and reports, or providing time-consuming irritation to system operations and maintenance personnel.

NOTE: Malicious code attacks can take the form of viruses, worms, Trojan Horses, or other automated exploits.

NOTE: Malicious code is also often referred to as “malware.”

3.2.71 manufacturing operations

collection of production, maintenance, and quality assurance operations and their relationship to other activities of a production facility.

NOTE: Manufacturing operations include:

a. manufacturing or processing facility activities that coordinate the personnel, equipment, and material involved in the conversion of raw materials or parts into products.

b. functions that may be performed by physical equipment, human effort, and information systems.

c. managing information about the schedules, use, capability, definition, history, and status of all resources (personnel, equipment, and material) within the manufacturing facility.

3.2.72 nonrepudiation

security service that provides protection against false denial of involvement in a communication [11].

3.2.73 OPC

set of specifications for the exchange of information in a process control environment.

NOTE: The abbreviation “OPC” originally came from “OLE for Process Control”, where “OLE” was short for “Object Linking and Embedding.”

[1] ISO is not an acronym. The name derives from the Greek word iso, which means equal.

3.2.74 outsider

person or group not “trusted” with inside access, who may or may not be known to the targeted organization (See “*insider*”).

NOTE: Outsiders may or may not have been insiders at one time.

3.2.75 penetration

successful unauthorized access to a protected system resource [11].

3.2.76 phishing

type of security attack that lures victims to reveal information, by presenting a forged email to lure the recipient to a web site that looks like it is associated with a legitimate source.

3.2.77 plaintext

unencoded data that is input to and transformed by an encryption process, or that is output by a decryption process [11].

3.2.78 privilege

authorization or set of authorizations to perform specific functions, especially in the context of a computer operating system [11].

NOTE: Examples of functions that are controlled through the use of privilege include acknowledging alarms, changing setpoints, modifying control algorithms.

3.2.79 process

series of operations performed in the making, treatment or transportation of a product or material.

NOTE: This standard makes extensive use of the term “process” to describe the equipment under control of the industrial automation and control system.

3.2.80 protocol

set of rules (i.e., formats and procedures) to implement and control some type of association (e.g., communication) between systems [11].

3.2.81 reference model

structure that allows the modules and interfaces of a system to be described in a consistent manner.

3.2.82 reliability

ability of a system to perform a required function under stated conditions for a specified period of time.

3.2.83 remote access

use of systems that are inside the perimeter of the security zone being addressed from a different geographical location with the same rights as when physically present at the location.

NOTE: The exact definition of “remote” can vary according to situation. For example, access may come from a location that is remote to the specific zone, but still within the boundaries of a company or organization. This might represent a lower risk than access that originates from a location that is remote and outside of a company’s boundaries.

3.2.84 remote client

asset outside the control network that is temporarily or permanently connected to a host inside the control network via a communication link in order to directly or indirectly access parts of the control equipment on the control network.

3.2.85 repudiation

denial by one of the entities involved in a communication of having participated in all or part of the communication.

3.2.86 residual risk

the remaining risk after the security controls or countermeasures have been applied.

3.2.87 risk

expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular consequence [11].

3.2.88 risk assessment

process that systematically identifies potential vulnerabilities to valuable system resources and threats to those resources, quantifies loss exposures and consequences based on probability of occurrence, and (optionally) recommends how to allocate resources to countermeasures to minimize total exposure.

NOTE: Types of resources include physical, logical and human.

NOTE: Risk assessments are often combined with vulnerability assessments to identify vulnerabilities and quantify the associated risk. They are carried out initially and periodically to reflect changes in the organization's risk tolerance, vulnerabilities, procedures, personnel and technological changes.

3.2.89 risk management

process of identifying and applying countermeasures commensurate with the value of the assets protected based on a risk assessment [9].

3.2.90 risk mitigation controls

combination of countermeasures and business continuity plans.

3.2.91 role-based access control

form of identity-based access control where the system entities that are identified and controlled are functional positions in an organization or process [11].

3.2.92 router

gateway between two networks at OSI layer 3 and that relays and directs data packets through that inter-network. The most common form of router passes Internet Protocol (IP) packets [11].

3.2.93 safety

freedom from unacceptable risk [2].

3.2.94 safety-instrumented system

system used to implement one or more safety-instrumented functions [2].

Note: A safety-instrumented system is composed of any combination of sensor(s), logic solver(s), and actuator(s).

3.2.95 safety integrity level

discrete level (one out of four) for specifying the safety integrity requirements of the safety-instrumented functions to be allocated to the safety-instrumented systems [2].

NOTE: Safety integrity level 4 has the highest level of safety integrity; safety integrity level 1 has the lowest.

3.2.96 safety network

network that connects safety-instrumented systems for the communication of safety-related information.

3.2.97 secret

condition of information being protected from being known by any system entities except those intended to know it [11].

3.2.98 security

1. measures taken to protect a system.
2. condition of a system that results from the establishment and maintenance of measures to protect the system.
3. condition of system resources being free from unauthorized access and from unauthorized or accidental change, destruction, or loss [11].
4. capability of a computer-based system to provide adequate confidence that unauthorized persons and systems can neither modify the software and its data nor gain access to the system functions, and yet to ensure that this is not denied to authorized persons and systems [14].

5. prevention of illegal or unwanted penetration of or interference with the proper and intended operation of an industrial automation and control system.

NOTE: Measures can be controls related to physical security (controlling physical access to computing assets) or logical security (capability to login to a given system and application.)

3.2.99 security architecture

plan and set of principles that describe the security services that a system is required to provide to meet the needs of its users, the system elements required to implement the services, and the performance levels required in the elements to deal with the threat environment [11].

NOTE: In this context, security architecture would be an architecture to protect the control network from intentional or unintentional security events.

3.2.100 security audit

independent review and examination of a system's records and activities to determine the adequacy of system controls, ensure compliance with established security policy and procedures, detect breaches in security services, and recommend any changes that are indicated for countermeasures [7].

3.2.101 security components

assets such as firewalls, authentication modules, or encryption software used to improve the security performance of an industrial automation and control system (See *“countermeasure”*).

3.2.102 security control

See “*countermeasure.*”

3.2.103 security event

occurrence in a system that is relevant to the security of the system [11].

3.2.104 security function

function of a zone or conduit to prevent unauthorized electronic intervention that can impact or influence the normal functioning of devices and systems within the zone or conduit.

3.2.105 security incident

adverse event in a system or network or the threat of the occurrence of such an event [10].

NOTE: The term “near miss” is sometimes used to describe an event that could have been an incident under slightly different circumstances.

3.2.106 security intrusion

security event, or a combination of multiple security events, that constitutes a security incident in which an intruder gains, or attempts to gain, access to a system (or system resource) without having authorization to do so [11].

3.2.107 security level

level corresponding to the required effectiveness of countermeasures and inherent security properties of devices and systems for a zone or conduit based on assessment of risk for the zone or conduit [13].

3.2.108 security objective

aspect of security which to achieve is the purpose and objective of using certain mitigation measures, such as confidentiality, integrity, availability, user authenticity, access authorization, accountability.

3.2.109 security perimeter

boundary (logical or physical) of the domain in which a security policy or security architecture applies, i.e., the boundary of the space in which security services protect system resources [11].

3.2.110 security performance

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 security measures remain effective and appropriate.

NOTE: Tests, audits, tools, measures, or other methods are required to evaluate security practice performance.

3.2.111 security policy
set of rules that specify or regulate how a system or organization provides security services to protect its assets [11].

3.2.112 security procedures
definitions of exactly how practices are implemented and executed.

NOTE: Security procedures are implemented through personnel training and actions using currently available and installed technology.

3.2.113 security program
a combination of all aspects of managing security, ranging from the definition and communication of policies through implementation of best industry practices and ongoing operation and auditing.

3.2.114 security services
mechanisms used to provide confidentiality, data integrity, authentication, or no repudiation of information [11].

3.2.115 security violation
act or event that disobeys or otherwise breaches security policy through an intrusion or the actions of a well-meaning insider.

3.2.116 security zone
grouping of logical or physical assets that share common security requirements.

NOTE: All unqualified uses of the word “zone” in this standard should be assumed to refer to a security zone.

NOTE: A zone has a clear border with other zones. The security policy of a zone is typically enforced by a combination of mechanisms both at the zone edge and within the zone. Zones can be hierarchical in the sense that they can be comprised of a collection of subzones.

3.2.117 sensors and actuators
measuring or actuating elements connected to process equipment and to the control system.

3.2.118 server
device or application that provides information or services to client applications and devices [11].

3.2.119 sniffing
See “*interception.*”

3.2.120 spoof
pretending to be an authorized user and performing an unauthorized action [11].

3.2.121 supervisory control and data acquisition (SCADA) system
type of loosely coupled distributed monitoring and control system commonly associated with electric power transmission and distribution systems, oil and gas pipelines, and water and sewage systems.

NOTE: Supervisory control systems are also used within batch, continuous, and discrete manufacturing plants to centralize monitoring and control activities for these sites.

3.2.122 system
interacting, interrelated, or interdependent elements forming a complex whole.

3.2.123 system software
special software designed for a specific computer system or family of computer systems to facilitate the operation and maintenance of the computer system and associated programs and data [12].

3.2.124 threat
potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm [11].

3.2.125 threat action

assault on system security [11].

3.2.126 traffic analysis

inference of information from observable characteristics of data flow(s), even when the data are encrypted or otherwise not directly available, including the identities and locations of source(s) and destination(s) and the presence, amount, frequency, and duration of occurrence.

3.2.127 trojan horse

computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program [11].

3.2.128 use case

technique for capturing potential functional requirements that employs the use of one or more scenarios that convey how the system should interact with the end user or another system to achieve a specific goal.

NOTE: Typically use cases treat the system as a black box, and the interactions with the system, including system responses, are as perceived from outside of the system. Use cases are popular because they simplify the description of requirements, and avoid the problem of making assumptions about how this functionality will be accomplished.

3.2.129 user

person, organization entity, or automated process that accesses a system, whether authorized to do so or not [11].

3.2.130 virus

self-replicating or self-reproducing program that spreads by inserting copies of itself into other executable code or documents.

3.2.131 vulnerability

flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's integrity or security policy [11].

3.2.132 wide area network

communications network designed to connect computers, networks and other devices over a large distance, such as across the country or world [12].

3.2.133 wiretapping

attack that intercepts and accesses data and other information contained in a flow in a communication system [11].

NOTE: Although the term originally referred to making a mechanical connection to an electrical conductor that links two nodes, it is now used to refer to reading information from any sort of medium used for a link or even directly from a node, such as a gateway or subnetwork switch.

NOTE: "Active wiretapping" attempts to alter the data or otherwise affect the flow; "passive wiretapping" only attempts to observe the flow and gain knowledge of information it contains.

3.2.134 worm

computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and may consume computer resources destructively [11].

3.2.135 zone

See *“security zone.”*

3.3 Abbreviations

This subclause defines the abbreviations used in this standard.

ANSI	American National Standards Institute
CIA	Confidentiality, Integrity, and Availability
CN	Control Network
COTS	Commercial off the Shelf
CSMS	Cyber Security Management System
DCS	Distributed Control System
DDoS	Distributed Denial of Service
DoS	Denial of Service
DMZ	Demilitarized Zone
FIPS	U. S. Federal Information Processing Standards
IACS	Industrial Automation and Control Systems
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
I/O	Input/Output
IP	Internet Protocol
ISA	The Instrumentation, Systems, and Automation Society
IT	Information Technology
LAN	Local Area Network
NASA	U. S. National Aeronautics and Space Administration
NOST	NASA Office of Standards and Technology
OSI	Open Systems Interconnect
PLC	Programmable Logic Controller
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SIL	Safety Integrity Level
SIS	Safety-Instrumented System
WAN	Wide Area Network

Annex A - Bibliography

The following documents contain material referenced in this standard.

[1] ISA-d99.00.02, Security for Industrial Automation and Control Systems, Part 2: Establishing an Industrial Automation and Control Systems Security Program. In development when this Part 1 standard was published. Visit www.isa.org/standards.

[2] ANSI/ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod), Functional Safety: Safety Instrumented Systems for the Process Industry Sector — Part 1: Framework, Definitions, System, Hardware and Software Requirements

[3] ANSI/ISA-84.00.01-2004 Part 3 (IEC 61511-3 Mod), Functional Safety: Safety Instrumented Systems for the Process Industry Sector – Part 3: Guidance for the Determination of the Required Safety Integrity Levels

[4] ANSI/ISA-95.00.01-2000, Enterprise-Control System Integration Part 1: Models and Terminology

[5] ANSI/ISA-95.00.03-2005, Enterprise-Control System Integration Part 3: Activity Models of Manufacturing Operations Management

[6] ISO/IEC 7498: Information processing systems – Open System Interconnection – Basic reference Model, Part 2: Security Architecture

[7] NASA/Science Office of Standards and Technology (NOST), http://ssdoo.gsfc.nasa.gov/nost/isoas/us04/defn.html

[8] CNSS Instruction No. 4009, National Information Assurance Glossary, May 2003, http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf

[9] SANS Glossary of Terms used in Security and Intrusion Detection, May 2003, http://www.sans.org/resources/glossary.php

[10] RFC 2828, Internet Security Glossary, May 2000, http://www.faqs.org/rfcs/rfc2828.html

[11] Federal Information Processing Standards (FIPS) PUB 140-2, (2001) “Security Requirements for Cryptographic Modules,” Section 2, Glossary of Terms and Acronyms, U.S. National Institute of Standards and Technology.

[12] Federal Information Processing Standards Publication, FIPS PUB 140-2, Security Requirements for Cryptographic Modules, December 2002

[13] International Electrotechnical Commission (IEC) Glossary, http://std.iec.ch/glossary

[14] IEC 61508-4: Functional safety of electrical/electronic/programmable electronic safety-related systems, Part 4: Definitions and abbreviations

Developing and promulgating technically sound consensus standards and recommended practices is one of ISA's primary goals. To achieve this goal the Standards and Practices Department relies on the technical expertise and efforts of volunteer committee members, chairmen, and reviewers.

ISA is an American National Standards Institute (ANSI) accredited organization. ISA administers United States Technical Advisory Groups (USTAGs) and provides secretariat support for International Electrotechnical Commission (IEC) and International Organization for Standardization (ISO) committees that develop process measurement and control standards. To obtain additional information on the Society's standards program, please write:

ISA
Attn: Standards Department
67 Alexander Drive
P.O. Box 12277
Research Triangle Park, NC 27709

ISBN: 978-1-934394-37-3