ANSI/ISA–99.02.01–2009

Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program

Approved 13 January 2009

ANSI/ISA–99.02.01–2009
Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program

ISBN: 978-1-934394-93-9

ISA
67 Alexander Drive
P.O. Box 12277
Research Triangle Park, NC 27709
www.isa.org

Preface

This preface, as well as all footnotes and annexes, is included for information purposes and is not part of ANSI/ISA–99.02.01–2009.

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

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

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

CAUTION — ISA does not take any position with respect to the existence or validity of any patent rights asserted in connection with this document, and ISA disclaims liability for the infringement of any patent resulting from the use of this document. Users are advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility.

Pursuant to ISA's Patent Policy, one or more patent holders or patent applicants may have disclosed patents that could be infringed by use of this document and executed a Letter of Assurance committing to the granting of a license on a worldwide, non-discriminatory basis, with a fair and reasonable royalty rate and fair and reasonable terms and conditions. For more information on such disclosures and Letters of Assurance, contact ISA or visit www.isa.org/StandardsPatents.

Other patents or patent claims may exist for which a disclosure or Letter of Assurance has not been received. ISA is not responsible for identifying patents or patent applications for which a license may be required, for conducting inquiries into the legal validity or scope of patents, or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory.

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

Additionally, the use of this 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 people served as active members of ISA99 Working Group 2 in the preparation of this standard:

Name	Company	Contributor	Reviewer
Thomas Good, WG Leader	DuPont	X	
James Gilsinn, Lead Editor	NIST	X	
Soloman Almadi	Saudi Aramco		X
Ken Anderson	MTS Allstream Inc.	X	
Rahul Bhojani	Bayer Technology Services	X	
Dennis Brandl	BR&L Consulting	X	
Eric Byres	Byres Security Inc.		X
Antony Capel	Comgate Engineering Ltd.		X
Richard Clark	Invensys/Wonderware		X
Eric Cosman, ISA99 Co-Chair	The Dow Chemical Company	X	
Jean-Pierre Dalzon	ISA France		X
Ronald Derynck	Verano		X
Gabriel Dimowo	Shell International	X	
Robert Evans	Idaho National Laboratory	X	
Donna Guillen	Idaho National Laboratory		X
Evan Hand	ConAgra Foods	X	
Mark Heard	Eastman Chemical Co.		X
Marnix Haije	Shell Information Technology	X	
Dave Mills	Proctor and Gamble Co.	X	
Carol Muehrcke	Cyber Defense Agency LLC	X	
Tom Phinney	Consultant	X	X
Jeff Potter	Emerson		X
Matt Rollinson	Monsanto Co.	X	
Bryan Singer, ISA99 Co-Chair	Kenexis Consulting Group	X	
Martin Solum	Cyber Defense Agency LLC	X	
Leon Steinocher	Fluor Enterprises		X
Ivan Susanto	Chevron Information Technology Co.		X
Brad Taylor	The George Washington University		X
Loren Uden	Lyondell Chemical Co.	X	
Bob Webb	ICS Secure LLC		X
Joe Weiss	Applied Control Solutions, LLC	X	
Ludwig Winkel	Siemens	X	

Contents

Foreword

This standard is part of a multipart series that addresses the issue of security for industrial automation and control systems. It has been developed by Working Group 2 of the ISA99 committee.

This standard describes the elements contained in a cyber security management system for use in the industrial automation and control systems environment and provides guidance on how to meet the requirements described for each element.

This standard has been developed in large part from a previous Technical Report produced by the ISA99 committee, ANSI/ISA–TR99.00.02–2004, Integrating Electronic Security into the Manufacturing and Control Systems Environment. The majority of the contents of this Technical Report have been included in this standard and as such this standard supersedes the Technical Report.

The ISA99 Series[1] and the IEC

The ISA99 series addresses electronic security within the industrial automation and control systems environment. The series will serve as the foundation for the IEC 62443 series of the same titles, as being developed by IEC TC65 WG10, “Security for industrial process measurement and control - Network and system security.” For information, visit www.iec.ch, Technical Committee 65.

The ISA99 series includes the following:

- **ANSI/ISA–99.01.01–2007 – Terminology, concepts and models**

  ANSI/ISA–99.01.01 establishes the context for all of the remaining standards in the series by defining the terminology, concepts and models to understand electronic security for the industrial automation and control systems environment.

- **ANSI/ISA–TR99.01.02–2007 – Security Technologies for Industrial Automation and Control Systems**

  ANSI/ISA–TR99.01.02 describes various security technologies in terms of their applicability for use with industrial automation and control systems. This report will be updated periodically to reflect changes in technology.

- **ANSI/ISA–99.02.01–2009 – Establishing an industrial automation and control system security program**

  ANSI/ISA–99.02.01 describes the elements to establish a cyber security management system and provides guidance on how to meet the requirements for each element.

- **ISA–99.02.02 (in development at the time of publication of this standard) – Operating an industrial automation and control system security program**

  ISA–99.02.02 will address how to operate a security program after it is designed and implemented. This includes the definition and application of metrics to measure program effectiveness.

- **ISA–99.03.xx – Technical security requirements for industrial automation and control systems (in development at the time of publication of this standard)**

  The ISA–99.03.xx standards will define the characteristics of industrial automation and control systems that differentiate them from other information technology systems from a

[1] For information about the status of the ISA99 series, visit http://www.isa.org/standards.

security point of view. Based on these characteristics, the standards will establish the security requirements that are unique to this class of systems.

ISA values your input

Users of this standard and all ISA standards are asked to submit comments and suggestions for consideration in future revisions. Please send your input to standards@isa.org.

Introduction

NOTE The format of this document follows the ISO/IEC requirements discussed in ISO/IEC Directives, Part 2. [9] This document specifies the format of the document as well as the use of terms like “shall”, “should”, and “may”. The directives requirements specified in Clause 4 use the conventions discussed in Appendix H of the Directives document.

Overview

Cyber security is an increasingly important topic in modern organizations. Many organizations involved in information technology (IT) and business have been concerned with cyber security for many years and have well-established Cyber Security Management Systems (CSMS) in place as defined by International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) 17799 [14] and ISO/IEC 27001 [15]. These management systems give an organization a well-established method for protecting its assets from cyber attacks.

Industrial Automation and Control System (IACS) organizations have begun using commercial-off-the-shelf (COTS) technology developed for business systems in their everyday processes, which has provided an increased opportunity for cyber attack against the IACS equipment. For many reasons these systems are not usually as robust, in the IACS environment, as are systems designed specifically as IACS at dealing with cyber attack for many reasons. This weakness may lead to health, safety and environmental (HSE) consequences.

Organizations may try to use the pre-existing IT and business cyber security solutions to address security for IACS without understanding the consequences. While many of these solutions can be applied to IACS, they need to be applied in the correct way to eliminate inadvertent consequences.

A cyber security management system for IACS

Management systems typically provide guidance on what should be included in a management system, but do not provide guidance on how to go about developing the management system. ANSI/ISA–99.02.01–2009 addresses the “what” aspect of a CSMS for IACS and also provides guidance on how to go about developing the CSMS for IACS.

A common engineering approach when faced with a challenging problem is to break the problem into smaller pieces and address each piece in a disciplined manner. This approach is a sound one for addressing cyber security risks with IACS. However, a frequent mistake made in addressing cyber security is to deal with cyber security one system at a time. Cyber security is a much larger challenge that must address the entire set of IACS as well as the policies, procedures, practices and personnel that surround and utilize those IACS. Implementing such a wide-ranging management system may require a cultural change within an organization.

Addressing cyber security on an organization-wide basis can seem like a daunting task. Unfortunately, there is no simple cookbook for security. There is good reason for this. There is not a one-size-fits-all set of security practices. Absolute security may be achievable, but is probably undesirable because of the loss of functionality that would be necessary to achieve this near perfect state. Security is really a balance of risk versus cost. All situations will be different. In some situations the risk may be related to HSE factors rather than purely economic impact. The risk may have an unrecoverable consequence rather than a temporary financial setback. Therefore, a cookbook set of mandatory security practices will either be overly restrictive and likely quite costly to follow, or be insufficient to address the risk.

Relationship with ISO/IEC 17799 and ISO/IEC 27001

ISO/IEC 17799 [14] and ISO/IEC 27001 [15] are excellent standards that describe a cyber security management system for business/information technology systems. Much of the content in these standards is applicable to IACS as well. ANSI/ISA–99.02.01–2009 emphasizes the need

for consistency between the practices to manage IACS cyber security with the practices to manage business/information technology systems cyber security. Economies will be realized by making these programs consistent. Users of this ISA document are encouraged to read ISO/IEC 17799 and 27001 for additional supporting information. ANSI/ISA–99.02.01–2009 builds on the guidance in these standards. It addresses some of the important differences between IACS and general business/information technology systems. It introduces the important concept that cyber security risks with IACS may have HSE implications and must be integrated with other existing risk management practices addressing these risks.

Document outline

This standard is structured to follow the ISO/IEC and ISA guidelines for standards development as closely as possible, per the following:.

- Clause 1 describes the scope of this standard.
- Clause 2 lists a number of normative references for this standard.
- Clause 3 defines a list of terms and abbreviations needed for this standard. This list is in addition to the list of terms defined in ANSI/ISA–99.01.01–2007. [1]
- Clause 4 defines the elements of a cyber security management system for industrial automation and control systems. Clause 4 is normative.
- Annex A provides guidance on how to develop the elements of the cyber security management system for IACS.
- Annex B describes an example process that an organization could use to develop the elements of the cyber security management system for IACS.
- The bibliography lists references to other sources used in the development of this standard or with some relevance to the material presented here.

1 Scope

This standard defines the elements necessary to establish a cyber security management system (CSMS) for industrial automation and control systems (IACS) and provides guidance on how to develop those elements. This document uses the broad definition and scope of what constitutes an IACS described in ANSI/ISA–99.01.01–2007. [1]

The elements of a CSMS described in this standard are mostly policy, procedure, practice and personnel related, describing what shall or should be included in the final CSMS for the organization.

NOTE Other documents in the ISA-99 series and in the Bibliography discuss specific technologies and/or solutions for cyber security in more detail.

The guidance provided on how to develop a CSMS is an example. It represents the authors' opinion on how an organization could go about developing the elements and may not work in all situations. The user of this standard will have to read the requirements carefully and apply the guidance appropriately in order to develop a fully functioning CSMS for their organization. The policies and procedures discussed in this standard should be tailored to fit within the organization.

NOTE There may be cases where a pre-existing CSMS is in place and the IACS portion is being added or there may be some organizations that have never formally created a CSMS at all. The authors of this standard cannot anticipate all cases where an organization will be establishing a CSMS for the IACS environment, so this standard does not attempt to create a solution for all cases.