FOR USE AND REVIEW ONLY BY MEMBERS OF ISA99 AND APPROVED PARTIES:

This abridged copy of a published 62443 document is to be used solely for the purpose of supporting the further development of ISA-62443 standards. This is an excerpt from a published ISA standard. It is to be used solely for the purpose of supporting the further development of ISA-62443 standards. It is subject to change without notice. It may not be reproduced or distributed to others, offered for sale, or used for commercial purposes.

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

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

ISA99 Work Product

This page intentionally left blank

ISA99 Work Product

ABRIDGED

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

This abridged copy of a published 62443 document is to be used solely for the purpose of supporting the further development of ISA-62443 standards. It is subject to change without notice. It may not be reproduced or distributed to others, offered for sale, or used for commercial purposes.

ABRIDGED

This abridged copy of a published 62443 document is to be used solely for the purpose of supporting the further development of ISA-62443 standards.
It is subject to change without notice. It may not be reproduced or distributed to others, offered for sale, or used for commercial purposes.

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

Copyright © 2009 by ISA. All rights reserved. Printed in the United States of America. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), without the prior written permission of the publisher.

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

Copyright 2009 ISA. All rights reserved.

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

Copyright 2009 ISA. All rights reserved.

This abridged copy of a published 62443 document is to be used solely for the purpose of supporting the further development of ISA-62443 standards. It is subject to change without notice. It may not be reproduced or distributed to others, offered for sale, or used for commercial purposes.

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.

This abridged copy of a published 62443 document is to be used solely for the purpose of supporting the further development of ISA-62443 standards. It is subject to change without notice. It may not be reproduced or distributed to others, offered for sale, or used for commercial purposes.

Copyright 2009 ISA. All rights reserved.

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	

This abridged copy of a published 62443 document is to be used solely for the purpose of supporting the further development of ISA-62443 standards. It is subject to change without notice. It may not be reproduced or distributed to others, offered for sale, or used for commercial purposes.

Copyright 2009 ISA. All rights reserved.

Contents

This abridged copy of a published 62443 document is to be used solely for the purpose of supporting the further development of ISA-62443 standards. It is subject to change without notice. It may not be reproduced or distributed to others, offered for sale, or used for commercial purposes.

Copyright 2009 ISA. All rights reserved.

Copyright 2009 ISA. All rights reserved.

This abridged copy of a published 62443 document is to be used solely for the purpose of supporting the further development of ISA-62443 standards. It is subject to change without notice. It may not be reproduced or distributed to others, offered for sale, or used for commercial purposes.

This abridged copy of a published 62443 document is to be used solely for the purpose of supporting the further development of ISA-62443 standards.
It is subject to change without notice. It may not be reproduced or distributed to others, offered for sale, or used for commercial purposes.

Copyright 2009 ISA. All rights reserved.

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.

Copyright 2009 ISA. All rights reserved.

This abridged copy of a published 62443 document is to be used solely for the purpose of supporting the further development of ISA-62443 standards. It is subject to change without notice. It may not be reproduced or distributed to others, offered for sale, or used for commercial purposes.

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.

This abridged copy of a published 62443 document is to be used solely for the purpose of supporting the further development of ISA-62443 standards. It is subject to change without notice. It may not be reproduced or distributed to others, offered for sale, or used for commercial purposes.

Copyright 2009 ISA. All rights reserved.

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

This abridged copy of a published 62443 document is to be used solely for the purpose of supporting the further development of ISA-62443 standards. It is subject to change without notice. It may not be reproduced or distributed to others, offered for sale, or used for commercial purposes.

Copyright 2009 ISA. All rights reserved.

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.

This abridged copy of a published 62443 document is to be used solely for the purpose of supporting the further development of ISA-62443 standards. It is subject to change without notice. It may not be reproduced or distributed to others, offered for sale, or used for commercial purposes.

Copyright 2009 ISA. All rights reserved.

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.

This abridged copy of a published 62443 document is to be used solely for the purpose of supporting the further development of ISA-62443 standards.
It is subject to change without notice. It may not be reproduced or distributed to others, offered for sale, or used for commercial purposes.

Copyright 2009 ISA. All rights reserved.

2 Normative references

The following normative document contains provisions, which through reference in this text constitute provisions of standard. At the time of publication, the edition indicated was valid. All normative documents are subject to revision and parties to agreements based on standard are encouraged to investigate the possibility of applying the most recent edition of the normative document indicated below.

ANSI/ISA–99.01.01–2007 – *Security for industrial automation and control systems: Terminology, concepts and models* [1]

As noted in the foreword to this standard, the ISA99 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.

This abridged copy of a published 62443 document is to be used solely for the purpose of supporting the further development of ISA-62443 standards.
It is subject to change without notice. It may not be reproduced or distributed to others, offered for sale, or used for commercial purposes.

Copyright 2009 ISA. All rights reserved.

3 Terms, definitions, abbreviated terms, acronyms, and conventions

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in ANSI/ISA–99.01.01–2007 and the following apply. Wherever possible, the definitions presented in this sub-clause have been taken from established industry sources. Others have been adapted from more generic definitions used in the information technology industry. Definitions that do not list a specific reference have been derived from sources in the public domain. All sources cited are listed in the bibliography.

3.1.1
access account
access control function that allows the user access to a particular set of data or functions for certain equipment

NOTE Many times accounts are linked to user identifications (IDs) and passwords. These user IDs and passwords may be linked to an individual or group of individuals such as a control room work team performing the same set of operating tasks.

3.1.2
administrative practices
defined and documented practices/procedures that individuals are personally accountable to follow at all times

NOTE These are usually in the conditions of employment for the organization. In the IACS environment, these often have HSE implications.

3.1.3
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 [1]

NOTE In this specific case, an asset is any item that should be protected as part of the cyber security management system.

3.1.4
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 [1]

3.1.5
burner management system
system for the safe start-up, monitoring and shutdown of burner systems associated with boilers, flares, incinerators, gas turbines, thermal oxidizers, and other fired equipment

3.1.6
business continuity plan
document with identified procedures for recovering from a significant disruption and restoring business operations [43]

NOTE 1 This umbrella term also refers to other aspects of disaster recovery, such as emergency management, human resources and media or press relations.

NOTE 2 A business continuity plan also identifies procedures for sustaining essential business operations while recovering from a significant disruption.

3.1.7
business continuity planning
process to develop a business continuity plan

This abridged copy of a published 62443 document is to be used solely for the purpose of supporting the further development of ISA-62443 standards. It is subject to change without notice. It may not be reproduced or distributed to others, offered for sale, or used for commercial purposes.

Copyright 2009 ISA. All rights reserved.

3.1.8
change management
process of controlling and documenting any change in a system to maintain the proper operation of the equipment under control

3.1.9
compliance
relation between two specifications, A and B, that holds when specification A makes requirements which are all fulfilled by specification B (when B complies with A) [10]

3.1.10
conformance
relation between a specification and a real implementation, such as an example of a product [10]

NOTE It holds when specific requirements in the specification (the conformance requirements) are met by the implementation. Conformance assessment is the process through which this relation is determined.

3.1.11
consequence
result that occurs from a particular incident

3.1.12
critical
very important device, computer system, process, and the like, that if compromised by an incident could have high financial, health, safety or environmental impact to an organization

3.1.13
cyber security management system
program designed by an organization to maintain the cyber security of the entire organization's assets to an established level of confidentiality, integrity and availability, whether they are on the business side or the industrial automation and control systems side of the organization

3.1.14
gatekeeper
trusted individual that senior managers use to prioritize issues they need to address over the remaining issues that others are more suited to address

3.1.15
health, safety, and environment
responsibility for protecting the health and safety of workers and the surrounding community and maintaining high environmental stewardship

3.1.16
human-machine interface
aggregate of means by which people (the users) interact with a particular machine, device, computer program or other complex tool (the system)

NOTE In many cases, these involve video screens or computer terminals, push buttons, auditory feedback, flashing lights, and the like. The human-machine interface provides means of:

- Input, allowing the users to control the machine
- Output, allowing the machine to inform the users. [44]

3.1.17
incident
event that is not part of the expected operation of a system or service that causes or may cause, an interruption to, or a reduction in, the quality of the service provided by the system

This abridged copy of a published 62443 document is to be used solely for the purpose of supporting the further development of ISA-62443 standards. It is subject to change without notice. It may not be reproduced or distributed to others, offered for sale, or used for commercial purposes.

Copyright 2009 ISA. All rights reserved.

3.1.18
independent audit
review of an organization (policies, procedures, processes, equipment, personnel, and the like) by an external group not affiliated with the organization

NOTE These may be required for public companies.

3.1.19
information technology
computer-related assets of an organization that represent nonphysical assets, such as software applications, process programs and personnel files

NOTE 1 Throughout this document, this use of the term information technology is not abbreviated.

NOTE 2 Another use of information technology (IT) refers to the company's internal organization (for example, the IT department) or the items traditionally maintained by this department (that is, the administrative computers, servers, and network infrastructure). Throughout this document, this use of the term information technology is abbreviated as IT.

3.1.20
legacy system
existing industrial automation and control system in a facility that may not be available as a commercial off the shelf (COTS) item

NOTE A legacy system may have been COTS at one time, but it may be no longer available and/or supported.

3.1.21
likelihood
quantitative chance that an action, event or incident may occur

3.1.22
local user
user who is inside the perimeter of the security zone being addressed

NOTE A person in the immediate manufacturing area or control room is an example of a local user.

3.1.23
manufacturing execution system
production scheduling and tracking system used to analyze and report resource availability and status, schedule and update orders, collect detailed execution data such as material usage, labor usage, operating parameters, order and equipment status and other critical information

NOTE 1 It accesses bills of material, routing and other data from the base enterprise resource planning system and is typically the system used for real-time shop floor reporting and monitoring that feeds activity data back to the base system. [45]

NOTE 2 Refer to ANSI/ISA-95.00.01-2000, Enterprise-Control System Integration Part 1: Models and Terminology, [7] for additional information.

3.1.24
MAC address
hardware address that differentiates one device on a network from another

NOTE For some networks, such as Ethernet, this address is typically encoded on a chip in the device, while in some industrial networks, such as DeviceNet, these can be controlled in software or with a hardware switch.

3.1.25
operator
particular type of user that is usually responsible for the correct operation of the equipment under control

This abridged copy of a published 62443 document is to be used solely for the purpose of supporting the further development of ISA-62443 standards.
It is subject to change without notice. It may not be reproduced or distributed to others, offered for sale, or used for commercial purposes.

Copyright 2009 ISA. All rights reserved.

3.1.26
patch management
area of systems management that involves acquiring, testing and installing multiple patches (code changes) to an administered computer system

NOTE Patch management tasks include: maintaining current knowledge of available patches, deciding what patches are appropriate for particular systems, ensuring that patches are installed properly, testing systems after installation and documenting all associated procedures, such as specific configurations required remotely across heterogeneous environments according to recognized best practices. [52]

3.1.27
process engineer
person typically responsible for the technical operation of the industrial operation and who uses the IACS and other tools to oversee and manage the industrial automation in the facility

3.1.28
process information management system
set of systems that provides supporting information to assist with the operation of the facility

3.1.29
programmable logic controller
programmable microprocessor-based device that is used in industry to control assembly lines and machinery on the shop floor as well as many other types of mechanical, electrical and electronic equipment in a plant. [54]

NOTE Typically programmed in an IEC 61131 programming language, a PLC is designed for real time use in rugged, industrial environments. Connected to sensors and actuators, PLCs are categorized by the number and type of I/O ports they provide and by their I/O scan rate.

3.1.30
process safety management
United States regulation intended to prevent a disaster in chemical and biotechnology systems by addressing sound management and engineering design. [16]

3.1.31
remote access
communication with or use of assets or systems within a defined perimeter from any location outside that perimeter

3.1.32
remote user
user who is outside the perimeter of the security zone being addressed

NOTE A person in an office in the same building, a person connecting over the corporate wide area network (WAN) and a person connecting over public infrastructure networks are all examples of remote users.

3.1.33
risk assessment
process of identifying and evaluating risks to the organization’s operations (including mission, functions, image, or reputation), the organization’s assets or individuals by determining the likelihood of occurrence, the resulting impact, and additional countermeasures that would mitigate this impact

NOTE Synonymous with risk analysis and incorporates threat and vulnerability analyses. [25]

3.1.34
risk mitigation
actions to reduce the likelihood and/or severity of an event

This abridged copy of a published 62443 document is to be used solely for the purpose of supporting the further development of ISA-62443 standards. It is subject to change without notice. It may not be reproduced or distributed to others, offered for sale, or used for commercial purposes.

Copyright 2009 ISA. All rights reserved.

3.1.35
risk tolerance
risk the organization is willing to accept

3.1.36
self assessment
review of an organization (that is, policies, procedures, operations, equipment, and personnel) by a group inside the organization

NOTE This group may be either directly associated with the organization's business process or may be in another part of the organization, but should be intimately familiar with the risks associated with that business process.

3.1.37
Six Sigma®
process-focused methodology designed to improve business performance through improving specific areas of strategic business processes [46]

3.1.38
social engineering
practice of obtaining confidential information by manipulation of legitimate users [44]

3.1.39
system administrator
person(s) responsible for managing the security of the computer system

NOTE This may include operating system maintenance, network management, account administration and patch management, in accordance with the change management process

3.1.40
stakeholder
individual or group with an interest in the success of an organization in delivering intended results and maintaining the viability of the organization's products and services [50]

NOTE Stakeholders influence programs, products and services. In this particular case, stakeholders are personnel in an organization responsible for promoting and overseeing the cyber security process. These personnel include the manager of the cyber security program as well as the cross-functional team of individuals from all of the departments affected by the cyber security program.

3.1.41
ushered access
procedure for monitoring the actions of a remotely connected user

NOTE This is also called shadowing.

3.1.42
vulnerability assessment
formal description and evaluation of the vulnerabilities in a system [25]

3.2 Abbreviated terms and acronyms

This sub-clause defines the abbreviated terms and acronyms used in this document.

ANSI	American National Standards Institute
CFR	U.S. Code of Federal Regulations
ChemITC	Chemical Information Technology Center of the American Chemistry Council
COTS	Commercial off the shelf
CPU	Central processing unit

This abridged copy of a published 62443 document is to be used solely for the purpose of supporting the further development of ISA-62443 standards.
It is subject to change without notice. It may not be reproduced or distributed to others, offered for sale, or used for commercial purposes.

Copyright 2009 ISA. All rights reserved.

CSCSP	Chemical Sector Cyber Security Program
CSMS	Cyber security management system
CSVA	Cyber security vulnerability assessment
DCS	Distributed control system
DoS, DDoS	Denial of service, Distributed denial of service
FDN	Field device network
FTP	File transfer protocol
HMI	Human machine interface
HSE	Health, safety, and environmental
HVAC	Heating, ventilation, and air-conditioning
IACS	Industrial automation and control system(s)
ID	Identification
IEC	International Electrotechnical Commission
IEEE	The Institute of Electrical and Electronics Engineers
IP	Internet protocol
ISA	International Society of Automation
ISO	International Organization for Standardization
IT	Information technology
KPI	Key performance indicator(s)
LAN	Local area network
MAC	Media access control
MES	Manufacturing execution system
NERC	North American Electric Reliability Council
NIST	U.S. National Institute of Standards and Technology
OS	Operating system
PC	Personal computer
PCN	Process control network
PCSRF	Process Control Security Requirements Forum
PIM	Process information management
PIN	Personal identification number
PLC	Programmable logic controller
PSM	Process safety management
RAID	Redundant array of independent disks
RCN	Regulatory control network
SANS	SysAdmin, Audit, Networking, and Security Institute

This abridged copy of a published 62443 document is to be used solely for the purpose of supporting the further development of ISA-62443 standards.
It is subject to change without notice. It may not be reproduced or distributed to others, offered for sale, or used for commercial purposes.

Copyright 2009 ISA. All rights reserved.

SCADA	Supervisory control and data acquisition
SI	International System of Units
SIS	Safety instrumented system(s)
SoA	Statement of applicability
SOC	Standard operating condition
SOP	Standard operating procedure
SP	Special Publication (by NIST)
SSL	Secure socket layer
TCP	Transmission control protocol
TR	Technical report
VLAN	Virtual local area network
VPN	Virtual private network
WAN	Wide area network

3.3 Conventions

The elements of a cyber security management system lists:

- the objective of the element
- a basic description of the element
- a rationale to explain why the element is included
- the requirements for that element

The requirements are presented as a table but not treated as tables in the sense of ISO/IEC directives. The tables list the description and the requirements for these elements. These are numbered similar to a sub-clause, so that they could be referenced, but the tables are not numbered with table numbers. The reference is given by the heading number in the description cell of the table.

This abridged copy of a published 62443 document is to be used solely for the purpose of supporting the further development of ISA-62443 standards.
It is subject to change without notice. It may not be reproduced or distributed to others, offered for sale, or used for commercial purposes.

Copyright 2009 ISA. All rights reserved.

4 Elements of a cyber security management system

4.1 Overview

This clause presents the elements that constitute a CSMS for IACS. These elements represent what shall and should be included in the CSMS in order to protect IACS against cyber attacks.

The elements are presented in three main categories:

- Risk analysis
- Addressing risk with the CSMS
- Monitoring and improving the CSMS

This abridged copy of a published 62443 document is to be used solely for the purpose of supporting the further development of ISA-62443 standards. It is subject to change without notice. It may not be reproduced or distributed to others, offered for sale, or used for commercial purposes.

Copyright 2009 ISA. All rights reserved.

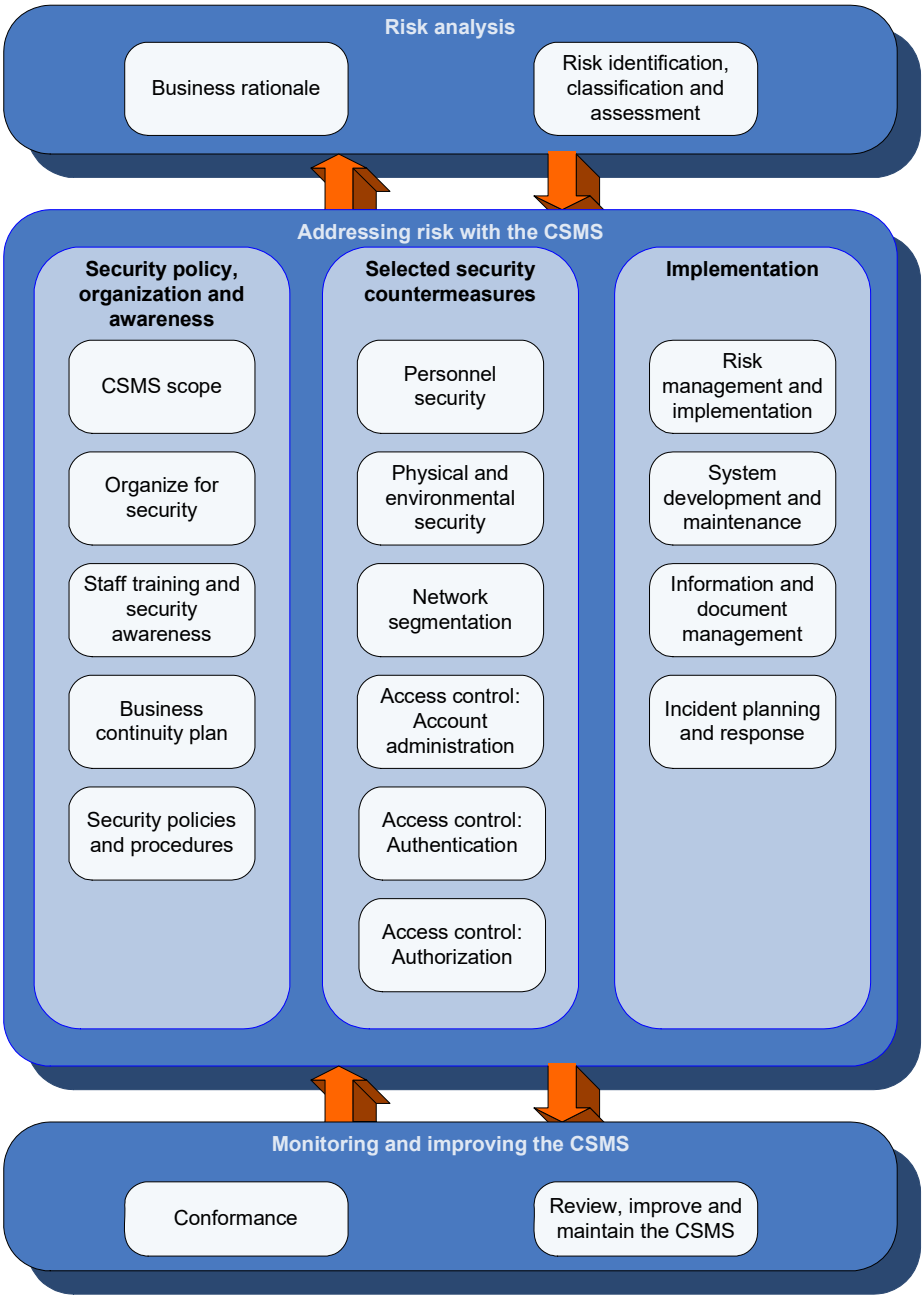

Figure 1 – Graphical view of elements of a cyber security management system

Each of these categories is further divided into element groups and/or elements. Figure 1 depicts the relationship between the categories, element groups and elements.

Each element in this clause lists the objective of the element, a basic description of the element, a rationale to explain why the element is included, and the requirements for that element.

Annex A follows the same basic structure of this clause with categories, element groups, and elements. However, Annex A provides guidance on how to develop the elements of the CSMS. The reader should read Annex A in order to understand the special needs and issues involved

Copyright 2009 ISA. All rights reserved.

This abridged copy of a published 62443 document is to be used solely for the purpose of supporting the further development of ISA-62443 standards.
It is subject to change without notice. It may not be reproduced or distributed to others, offered for sale, or used for commercial purposes.

with developing a CSMS for IACS. The guidance discussed in Annex A should be tailored to the special requirements of each organization.

This standard specifies the elements required for a CSMS. It is not the intent of the standard to specify a particular sequential process for identifying and addressing risk that incorporates these elements. Thus, an organization will create such a process in accordance with its culture, organization, and the current status of its cyber security activities. To assist organizations with this aspect of applying the standard, Annex A.3.4.2 provides an example of a process for identifying and addressing risk. In addition, Annex B offers insights on effective ordering for activities related to all of the elements discussed in this standard.

While a CSMS is an excellent tool for managing risk within a large company, it is equally applicable to small companies. The CSMS may be more formalized in a large company so it can be used in many different situations and geographies. In a small company, similar CSMS activities need to be conducted, but they may not be as formal. Clause 4 and Annex A provide guidance to help the user better understand the elements and activities of a CSMS.

4.2 Category: Risk analysis

4.2.1 Description of category

The first main category of the CSMS is risk analysis. This category discusses much of the background information that feeds into many of the other elements in the CSMS. Figure 2 shows the two elements in this category:

- Business rationale
- Risk identification, classification, and assessment

Figure 2 – Graphical view of category: Risk analysis

4.2.2 Element: Business rationale

Objective:

Identify and document the unique needs of an organization to address cyber risk for IACS.

Description:

A business rationale is based on the nature and magnitude of financial, health, safety, environmental, and other potential consequences should IACS cyber incidents occur.

Rationale:

Establishing a business rationale is essential for an organization to maintain management buy-in to an appropriate level of investment for the IACS cyber security program.

This abridged copy of a published 62443 document is to be used solely for the purpose of supporting the further development of ISA-62443 standards. It is subject to change without notice. It may not be reproduced or distributed to others, offered for sale, or used for commercial purposes.

Copyright 2009 ISA. All rights reserved.

ABRIDGED

Several pages have been removed from this excerpt of a published document in the 62443 series

This abridged copy of a published 62443 document is to be used solely for the purpose of supporting the further development of ISA-62443 standards.
It is subject to change without notice. It may not be reproduced or distributed to others, offered for sale, or used for commercial purposes.

Bibliography

NOTE This bibliography includes references to sources used in the creation of this standard as well as references to sources that may aid the reader in developing a greater understanding of cyber security as a whole and developing a management system. Not all references in this bibliography are referred to throughout the text of this standard. The references have been broken down into different categories depending on the type of source they are.

Standards references:

[1] ANSI/ISA–99.01.01–2007, Security for industrial automation and control systems: Terminology, concepts and models*"*

[2] ANSI/ISA–TR99.01.02–2007, Security for Industrial Automation and Control Systems, Technical Report 1: Security Technologies for Industrial Automation and Control Systems – *Referred to throughout this document as "ISA–TR99.01.02."*

[3] ANSI/ISA–99.02.02, Security for industrial automation and control systems: Operating an industrial automation and control system security program – *Referred to throughout this document as "ISA–99.02.02."*

[4] ISA–d99.03.01, Security for industrial automation and control systems: Technical security requirements for industrial automation and control systems: Target security levels – *Referred to throughout this document as "ISA–d99.03.01."*

[5] ISA–d99.03.02, Security for industrial automation and control systems: Technical security requirements for industrial automation and control systems: System security compliance metrics – *Referred to throughout this document as "ISA–d99.03.02."*

[6] ISA–d99.03.03, Security for industrial automation and control systems: Technical security requirements for industrial automation and control systems: Allocation to subsystems and components – *Referred to throughout this document as "ISA–d99.03.03."*

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

[8] ISA–88.01–1995, Batch Control, Part 1: Models and Terminology

[9] ISO/IEC Directives, Part 2: 2004, Rules for the structure and drafting of International Standards

[10] ISO/IEC 10746-1:1998, Information technology – Open Distributed Processing – Reference model: Overview

[11] ISO/IEC 15408-1:2005, Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model

[12] ISO/IEC 15408-2:2005, Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements

[13] ISO/IEC 15408-3:2005, Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements

[14] ISO/IEC 17799:2005, Information technology – Security techniques – Code of practice for information security management – *Referred to throughout this document as "ISO/IEC 17799."*

This abridged copy of a published 62443 document is to be used solely for the purpose of supporting the further development of ISA-62443 standards. It is subject to change without notice. It may not be reproduced or distributed to others, offered for sale, or used for commercial purposes.

Copyright 2009 ISA. All rights reserved.

[15] ISO/IEC 27001:2005, Information technology – Security techniques – Information security management systems – Requirements – *Referred to throughout this document as "ISO/IEC 27001."*

[16] 29 CFR 1910.119 – U.S. Occupational Safety and Health Standards – Hazardous Materials – Process safety management of highly hazardous chemicals

Industry-specific and sector-specific references:

[17] Guidance for Addressing Cyber Security in the Chemical Sector, Version 3.0, May 2006, American Chemistry Council's Chemical Information Technology Center (ChemITC), http://chemicalcybersecurity.com/cybersecurity_tools/guidance_docs.cfm – *Referred throughout this document as "ChemITC Guidance for Cyber Security."*

[18] Report on Cyber Security Vulnerability Assessments Methodologies, Version 2.0, November 2004, ChemITC, http://chemicalcybersecurity.com/cybersecurity_tools/guidance_docs.cfm – *Referred to throughout this document as "ChemITC Report on CSVA."*

[19] Cyber Security Architecture Reference Model, Version 1.0, August 2004, ChemITC, http://chemicalcybersecurity.com/cybersecurity_tools/guidance_docs.cfm – *Referred to throughout this document as "ChemITC Reference Model."*

[20] Report on the Evaluation of Cybersecurity Self-assessment Tools and Methods, November 2004, ChemITC, http://chemicalcybersecurity.com/cybersecurity_tools/guidance_docs.cfm – *Referred to throughout this document as "ChemITC Report on Self-assessment."*

[21] U.S. Chemicals Sector Cyber Security Strategy, September 2006, http://chemicalcybersecurity.com/strategy/strategy.cfm

Other documents and published resources:

[22] Carlson, Tom, *Information Security Management: Understanding ISO 17799*, 2001, http://www.responsiblecaretoolkit.com/pdfs/Cybersecurity_att3.pdf – *Referred to throughout this document as "Understanding ISO 17799."*

[23] Purdue Research Foundation, A Reference Model for Computer Integrated Manufacturing, 1989, ISBN 1-55617-225-7

[24] NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, July 2002 – *Referred to throughout this document as "NIST SP 800-30."*

[25] NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004

[26] NIST Special Publication 800-55, *Security Metrics Guide for Information Technology Systems*, July 2003 – *Referred to throughout this document as "NIST SP 800-55."*

[27] NIST Special Publication 800-61, *Computer Security Incident Handling Guide*, January 2004 – *Referred to throughout this document as "NIST SP 800-61."*

[28] NIST Special Publication 800-82, *Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control System Security*, March 2006, Draft – *Referred to throughout this document as "NIST SP 800-82."*

This abridged copy of a published 62443 document is to be used solely for the purpose of supporting the further development of ISA-62443 standards. It is subject to change without notice. It may not be reproduced or distributed to others, offered for sale, or used for commercial purposes.

Copyright 2009 ISA. All rights reserved

[29] NIST Process Control Security Requirements Forum (PCSRF), Industrial Control System – System Protection Profile (ICS-SPP) – *Referred to throughout this document as "PCSRF ICS-SPP."*

[30] Carnegie Mellon Software Engineering Institute, *Capability Maturity Model Integration (CMMI) for Software Engineering*, v1.1, August 2002 – *Referred to throughout this document as "CMMI-SW v1.1."*

Websites:

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

[32] Zachmann Enterprise Reference Model, http://www.zifa.com/

[33] Sarbanes – Oxley Web site, http://www.sarbanes-oxley.com/

[34] Sans Web site, http://www.sans.org/

[35] MIS Training Institute, http://www.misti.com/

[36] U.S. National Institute of Standards & Technology, http://www.nist.gov/

[37] Information Systems Technology Audit Programs, http://www.auditnet.org/asapind.htm

[38] NIST eScan Security Assessment, http://www.escan.nist.gov/sat/index.htm

[39] American National Standards Institute, http://www.ansi.org/

[40] IDEAL Model, http://www.sei.cmu.edu/ideal/ideal.html

[41] Control Objectives for Information and Related Technology (COBIT), http://www.isaca.org/

[42] Corporate Governance Task Force "Information Security Governance- A call to action" http://www.cyberpartnership.org/InfoSecGov4_04.pdf

[43] Michigan State Cybersecurity Definitions, http://www.michigan.gov/cybersecurity/0,1607,7-217-34415---,00.html

[44] The Free Internet Encyclopedia – Wikipedia, http://www.wikipedia.org/

[45] Bridgefield Group Glossary, http://www.bridgefieldgroup.com/

[46] Six Sigma Information, http://www.onesixsigma.com/

[47] Carnegie Mellon Software Engineering Institute, http://www.sei.cmu.edu/

[48] Carnegie Mellon Software Engineering Institute, Computer Emergency Response Team (CERT), http://www.cert.org/

[49] SCADA and Control Systems Procurement Project, http://www.msisac.org/scada/

[50] Interoperability Clearinghouse, http://www.ichnet.org/

[51] New York State Financial Terminology, http://www.budget.state.ny.us/citizen/financial/audit.html

This abridged copy of a published 62443 document is to be used solely for the purpose of supporting the further development of ISA-62443 standards. It is subject to change without notice. It may not be reproduced or distributed to others, offered for sale, or used for commercial purposes.

Copyright 2009 ISA. All rights reserved.

ABRIDGED

[52] Search Windows Security, http://www.searchwindowssecurity.com/

[53] Chemical Sector Cyber Security Program, http://chemicalcybersecurity.com/

[54] TechEncyclopedia, http://www.techweb.com/encyclopedia/

This abridged copy of a published 62443 document is to be used solely for the purpose of supporting the further development of ISA-62443 standards.
It is subject to change without notice. It may not be reproduced or distributed to others, offered for sale, or used for commercial purposes.

Copyright 2009 ISA. All rights reserved

This page intentionally left blank.

This abridged copy of a published 62443 document is to be used solely for the purpose of supporting the further development of ISA-62443 standards.
It is subject to change without notice. It may not be reproduced or distributed to others, offered for sale, or used for commercial purposes.

ABRIDGED

This abridged copy of a published 62443 document is to be used solely for the purpose of supporting the further development of ISA-62443 standards.
It is subject to change without notice. It may not be reproduced or distributed to others, offered for sale, or used for commercial purposes.

ABRIDGED

Developing and promulgating technically sound consensus standards and recommended practice 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 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: 978-1-934394-93-9

This abridged copy of a published 62443 document is to be used solely for the purpose of supporting the further development of ISA-62443 standards.
It is subject to change without notice. It may not be reproduced or distributed to others, offered for sale, or used for commercial purposes.