

ANSI/ISA-62443-3-3 (99.03.03)-2013

**Security for industrial automation
and control systems**

**Part 3-3: System security requirements
and security levels**

Approved 12 August 2013

ANSI/ISA-62443-3-3 (99.03.03)-2013

Security for industrial automation and control systems

Part 3-3: System security requirements and security levels

ISBN: 978-0-876640-39-5

Copyright © 2013 by ISA. All rights reserved. Not for resale. Printed in the United States of America.

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-62443-3-3 (99.03.03)-2013.

This document has been prepared as part of the service of ISA, the International Society of Automation, 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 endeavor 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 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 served as active members of ISA99 Working Group 4, Task Group 2 in developing this standard:

Name	Company	Contributor	Reviewer
Jeff Potter, TG Chair	Emerson	X	
Adedotun Adeyemi	Quaddynamics Nigeria Ltd		X
Leandro Pflieger de Aguiar	Chemtech - Siemens	X	
Raghu Avali	Westinghouse Electric Corp		X
Satishkumar Balasubramanian	Yokogawa IA Technologies		X
Rahul Bhojani	Bayer	X	
Wayne Boyer	US Idaho National Laboratory		X
Antony Capel	Comgate Engineering Ltd.		X
Penny Chen	Yokogawa Corp. of America		X
Eric Cosman	The Dow Chemical Co.		X
John Cusimano	Exida	X	
Kelli Dean	Okonite		X
Aris Espejo	Syncrude Canada Ltd.		X
Dean Ford	Glenmount Global Solutions	X	
Donald Fraser	Jacobs		X
James Gilsinn	Kenexis	X	
Thomas Good	DuPont		X
Vic Hammond	US Argonne National Laboratory		X
Jean-Pierre Hauet	KB Intelligence		X
Dennis Holstein	Opus Consulting Group	X	
Charles Hoover	Rockwell Automation	X	
Bob Huba	Emerson	X	
Freemon Johnson	US State Department	X	
Pierre Kobes	Siemens	X	
Sinclair Koelemij	Honeywell Industrial IT Solutions		X
Erwin Kruschitz	Anapur AG		X
Tyson Macaulay	Bell Business Markets (Bell Canada)		X
Pete MacLeod	Engenuity Consulting	X	
Wayne Manges	US Oak Ridge National Laboratory		X
William Miller	MaCT USA		X
Kevin Minnick	GE Energy		X
Ajay Mishra	Invensys - Triconex		X
Olav Mo	ABB AS		X
John Munro	US Oak Ridge National Laboratory	X	
Johan Nye	ExxonMobil	X	
Nor'Azuwa Binti Pahri	CyberSecurity Malaysia		X
Tom Phinney	Consultant		X
Ragnar Schierholz	ABB AG	X	

Graham Speake	Yokogawa		X
Kevin Staggs	Honeywell	X	
Herman Storey	Herman Storey Consulting		X
Tatsuaki Takabe	Yokogawa	X	
Steven Tom	US Idaho National Laboratory	X	
Gerd Wartmann	Endress + Hauser		X
Vernon Williams	Patria Group		X

This page intentionally left blank.

CONTENTS

PREFACE	3
FOREWORD	10
0 Introduction	11
0.1 Overview.....	11
0.2 Purpose and intended audience	12
0.3 Usage within other parts of the ISA - 62443 series	12
1 Scope	15
2 Normative references	15
3 Terms, definitions, abbreviated terms, acronyms, and conventions	15
3.1 Terms and definitions.....	15
3.2 Abbreviated terms and acronyms	21
3.3 Conventions.....	23
4 Common control system security constraints	24
4.1 Overview.....	24
4.2 Support of essential functions	24
4.3 Compensating countermeasures	24
4.4 Least privilege	25
5 FR 1 – Identification and authentication control	25
5.1 Purpose and SL-C(IAC) descriptions	25
5.2 Rationale	25
5.3 SR 1.1 – Human user identification and authentication.....	25
5.4 SR 1.2 – Software process and device identification and authentication	27
5.5 SR 1.3 – Account management	28
5.6 SR 1.4 – Identifier management.....	28
5.7 SR 1.5 – Authenticator management	29
5.8 SR 1.6 – Wireless access management	30
5.9 SR 1.7 – Strength of password-based authentication	31
5.10 SR 1.8 – Public key infrastructure (PKI) certificates	32
5.11 SR 1.9 – Strength of public key authentication	33
5.12 SR 1.10 – Authenticator feedback	34
5.13 SR 1.11 – Unsuccessful login attempts	34
5.14 SR 1.12 – System use notification.....	35
5.15 SR 1.13 – Access via untrusted networks.....	35
6 FR 2 – Use control	36
6.1 Purpose and SL-C(UC) descriptions.....	36
6.2 Rationale	36
6.3 SR 2.1 – Authorization enforcement	37
6.4 SR 2.2 – Wireless use control	38
6.5 SR 2.3 – Use control for portable and mobile devices	39
6.6 SR 2.4 – Mobile code	39

6.7	SR 2.5 – Session lock	40
6.8	SR 2.6 – Remote session termination	40
6.9	SR 2.7 – Concurrent session control	41
6.10	SR 2.8 – Auditable events	41
6.11	SR 2.9 – Audit storage capacity	42
6.12	SR 2.10 – Response to audit processing failures	43
6.13	SR 2.11 – Timestamps	43
6.14	SR 2.12 – Non-repudiation	44
7	FR 3 – System integrity	45
7.1	Purpose and SL-C(SI) descriptions	45
7.2	Rationale	45
7.3	SR 3.1 – Communication integrity	45
7.4	SR 3.2 – Malicious code protection	46
7.5	SR 3.3 – Security functionality verification	47
7.6	SR 3.4 – Software and information integrity	48
7.7	SR 3.5 – Input validation	49
7.8	SR 3.6 – Deterministic output.....	49
7.9	SR 3.7 – Error handling.....	50
7.10	SR 3.8 – Session integrity.....	50
7.11	SR 3.9 – Protection of audit information	51
8	FR 4 – Data confidentiality	52
8.1	Purpose and SL-C(DC) descriptions.....	52
8.2	Rationale	52
8.3	SR 4.1 – Information confidentiality.....	52
8.4	SR 4.2 – Information persistence	53
8.5	SR 4.3 – Use of cryptography	54
9	FR 5 – Restricted data flow	55
9.1	Purpose and SL-C(RDF) descriptions.....	55
9.2	Rationale	55
9.3	SR 5.1 – Network segmentation	55
9.4	SR 5.2 – Zone boundary protection	56
9.5	SR 5.3 – General purpose person-to-person communication restrictions	57
9.6	SR 5.4 – Application partitioning	58
10	FR 6 – Timely response to events	58
10.1	Purpose and SL-C(TRE) descriptions.....	58
10.2	Rationale	59
10.3	SR 6.1 – Audit log accessibility	59
10.4	SR 6.2 – Continuous monitoring.....	59
11	FR 7 – Resource availability.....	60
11.1	Purpose and SL-C(RA) descriptions	60
11.2	Rationale	61
11.3	SR 7.1 – Denial of service protection	61
11.4	SR 7.2 – Resource management.....	61
11.5	SR 7.3 – Control system backup	62

11.6	SR 7.4 – Control system recovery and reconstitution	62
11.7	SR 7.5 – Emergency power	63
11.8	SR 7.6 – Network and security configuration settings	63
11.9	SR 7.7 – Least functionality	64
11.10	SR 7.8 – Control system component inventory	64
Annex A (informative) Discussion of the SL vector		67
A.1	Introduction	67
A.2	Security levels	67
A.3	SL vector	72
Annex B (informative) Mapping of SRs and REs to FR SL levels 1-4		75
B.1	Overview	75
B.2	SL mapping table	75
BIBLIOGRAPHY		80
Figure 1 – ISA-62443 Work Products		13
Figure A.1 – High-level process-industry example showing zones and conduits		69
Figure A.2 – High-level manufacturing example showing zones and conduits		70
Figure A.3 – Schematic of correlation of the use of different SL types		71
Table B.1 – Mapping of SRs and REs to FR SL levels 1-4		75

FOREWORD

This standard is part of a multipart series of standards that address the issue of security for industrial automation and control systems (IACS). It has been developed by Working Group 4, Task Group 2 of the ISA99 committee in cooperation with IEC TC65 Working Group 10.

This standard prescribes the security requirements for control systems related to the seven foundational requirements defined in ISA-62443-1-1 (99.01.01) [1]¹ and assigns system security levels (SLs) to the system under consideration (SuC).

¹ Numbers in brackets indicate references in the Bibliography on page 73.

0 Introduction

NOTE The format of this document follows the ISO/IEC requirements discussed in ISO/IEC Directives, Part 2 [13]. These directives specify the format of the document as well as the use of terms like “shall”, “should”, and “may”. The requirements specified in normative clauses use the conventions discussed in Appendix H of the Directives document.

0.1 Overview

Industrial automation and control system (IACS) organizations increasingly use commercial-off-the-shelf (COTS) networked devices that are inexpensive, efficient and highly automated. Control systems are also increasingly interconnected with non-IACS networks for valid business reasons. These devices, open networking technologies and increased connectivity provide an increased opportunity for cyber attack against control system hardware and software. That weakness may lead to health, safety and environmental (HSE), financial and/or reputational consequences in deployed control systems.

Organizations deploying business information technology (IT) cyber security solutions to address IACS security may not fully comprehend the results of this decision. While many business IT applications and security solutions can be applied to IACS, they need to be applied in an appropriate way to eliminate inadvertent consequences. For this reason, the approach used to define system requirements needs to be based on a combination of functional requirements and risk assessment, often including an awareness of operational issues as well.

IACS security measures should not have the potential to cause loss of essential services and functions, including emergency procedures. (IT security measures, as often deployed, do have this potential.) IACS security goals focus on control system availability, plant protection, plant operations (even in a degraded mode) and time-critical system response. IT security goals often do not place the same emphasis on these factors; they may be more concerned with protecting information rather than physical assets. These different goals need to be clearly stated as security objectives regardless of the degree of plant integration achieved. A key step in risk assessment, as required by ISA-62443-2-1 (99.02.01)² [5], should be the identification of which services and functions are truly essential for operations. (For example, in some facilities engineering support may be determined to be a non-essential service or function.) In some cases, it may be acceptable for a security action to cause temporary loss of a non-essential service or function, unlike an essential service or function that should not be adversely affected.

This document assumes that a security program has been established and is being operated in accordance with ISA-62443-2-1 (99.02.01). Furthermore, it is assumed that patch management is implemented consistent with the recommendations detailed in ISA-TR62443-2-3 (TR99.02.03) [7] utilizing the appropriate control system requirements and requirement enhancements as described in this document. In addition, ISA-62443-3-2 (99.03.02) [10] describes how a project defines risk-based security levels (SLs) which then are used to select products with the appropriate technical security capabilities as detailed in this document. Key input to this document included ISO/IEC 27002 [14] and NIST SP800-53, rev 3 [26] (see Clause 2 and the Bibliography for a more complete listing of source material).

The primary goal of the ISA-62443 series is to provide a flexible framework that facilitates addressing current and future vulnerabilities in IACS and applying necessary mitigations in a systematic, defensible manner. It is important to understand that the intention of the ISA-62443 series is to build extensions to enterprise security that adapt the requirements for business IT systems and combines them with the unique requirements for strong availability needed by IACS.

² Many documents in the ISA-62443 series were under review or in development at the time of publication of this standard.

0.2 Purpose and intended audience

The IACS community audience for this specification is intended to be asset owners, system integrators, product suppliers, service providers and, where appropriate, compliance authorities. Compliance authorities include government agencies and regulators with the legal authority to perform audits to verify compliance with governing laws and regulations.

System integrators, product suppliers and service providers will use this document to evaluate whether their products and services can provide the functional security capability to meet the asset owner's target security level (SL-T) requirements. As with the assignment of SL-Ts, the applicability of individual control system requirements (SRs) and requirement enhancements (REs) needs to be based on an asset owner's security policies, procedures and risk assessment in the context of their specific site. Note that some SRs contain specific conditions for permissible exceptions, such as where meeting the SR will violate fundamental operational requirements of a control system (which may trigger the need for compensating countermeasures).

When designing a control system to meet the set of SRs associated with specific SL-Ts, it is not necessary that every component of the proposed control system support every system requirement to the level mandated in this standard. Compensating countermeasures can be employed to provide the needed functionality to other subsystems, such that the overall SL-T requirements are met at the control system level. Inclusion of compensating countermeasures during the design phase should be accompanied by comprehensive documentation so that the resulting achieved control system SL, SL-A(control system), fully reflects the intended security capabilities inherent in the design. Similarly, during certification testing and/or post-installation audits, compensating countermeasures can be utilized and documented in order to meet the overall control system SL.

There is insufficient detail in this document to design and build an integrated security architecture. That requires additional system-level analysis and development of derived requirements that are the subject of other documents in the ISA-62443 series (see 0.3). Note that providing specifications detailed enough to build a security architecture is not the goal of this document. The goal is to define a common, minimum set of requirements to reach progressively more stringent security levels. The actual design of an architecture that meets these requirements is the job of system integrators and product suppliers. In this task, they retain the freedom to make individual choices, thus supporting competition and innovation. Thus this standard strictly adheres to specifying functional requirements, and does not address how these functional requirements should be met.

0.3 Usage within other parts of the ISA-62443 series

Figure 1 shows a graphical depiction of the ISA-62443 series when this standard was written.

ISA-62443-3-2 (99.03.02) uses the SRs and REs as a checklist. After the system under consideration (SuC) has been described in terms of zones and conduits, and individual target SLs have been assigned to these zones and conduits, the SRs and REs in this document, as well as their mapping to capability SLs (SL-Cs), are used to compile a list of requirements which the control system design needs to meet. A given control system design can then be checked for completeness, thereby providing the SL-As.

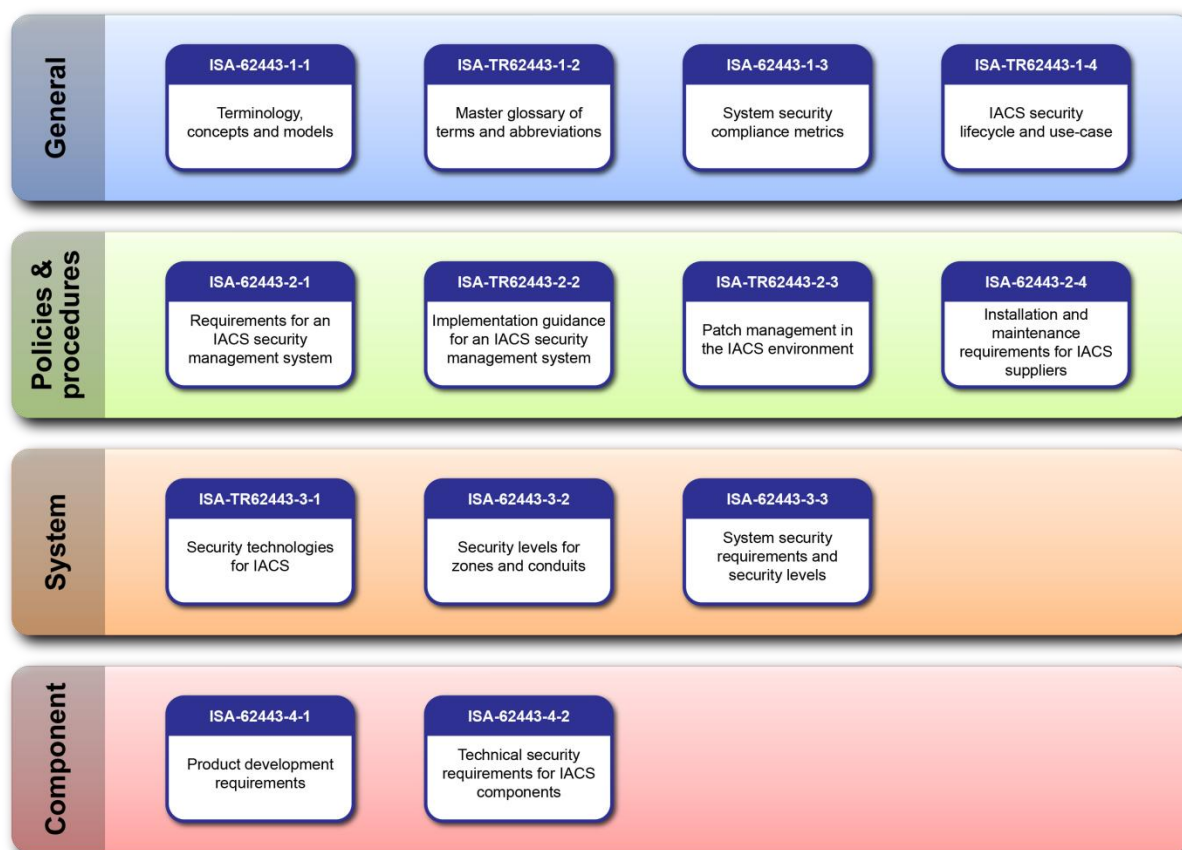


Figure 1 – ISA-62443 Work Products

ISA-62443-1-3 (99.01.03) [3] uses the foundational requirements (FRs), SRs, REs and the mapping to SL-Cs as a checklist to test for completeness of the specification of quantitative metrics. The quantitative security compliance metrics are context specific. Together with ISA-62443-3-2 (99.03.02), the asset owner's SL-T assignments are translated into quantitative metrics that can be used to support system analysis and design trade-off studies, to develop a security architecture.

ISA-62443-4-1 (99.04.01) [11] addresses the overall requirements during the development of products. As such, ISA-62443-4-1 (99.04.01) is product supplier centric. Product security requirements are derived from the list of baseline requirements and REs specified in this document. Normative quality specifications in ISA-62443-4-1 (99.04.01) will be used when developing these product capabilities.

ISA-62443-4-2 (99.04.02) [12] contains sets of derived requirements that provide a detailed mapping of the SRs specified in this document to subsystems and components of the SuC. At the time this document was written, the component categories addressed in ISA-62443-4-2 (99.04.02) were: embedded devices, host devices, network devices and applications. As such, the ISA-62443-4-2 (99.04.02) document is vendor (product supplier and service provider) centric. Product security requirements are first derived from the list of baseline requirements and REs specified in this document. Security requirements and metrics from ISA-62443-3-2 (99.03.02) and ISA-62443-1-3 (99.01.03) are used to refine these normative derived requirements.

This page intentionally left blank.

1 Scope

This part of the ISA-62443 series provides detailed technical control system requirements (SRs) associated with the seven foundational requirements (FRs) described in ISA-62443-1-1 (99.01.01) [1] including defining the requirements for control system capability security levels, SL-C (control system). These requirements would be used by various members of the industrial automation and control system (IACS) community along with the defined zones and conduits for the system under consideration (SuC) while developing the appropriate control system target SL, SL-T(control system), for a specific asset.

As defined in ISA-62443-1-1 (99.01.01) there are a total of seven FRs:

- 1) Identification and authentication control (IAC),
- 2) Use control (UC),
- 3) System integrity (SI),
- 4) Data confidentiality (DC),
- 5) Restricted data flow (RDF),
- 6) Timely response to events (TRE), and
- 7) Resource availability (RA).

These seven requirements are the foundation for control system capability SLs, SL-C(control system). Defining security capability at the control system level is the goal and objective of this document as opposed to target SLs, SL-T, or achieved SLs, SL-A, which are out of scope.

NOTE Refer to ISA-62443-2-1 (99.02.01) for an equivalent set of non-technical, program-related, capability SRs necessary for fully achieving a control system target SL.

2 Normative references

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

ISA-62443-1-1 (99.01.01) – *Security for industrial automation and control systems Part 1-1: Terminology, concepts and models* [1]

ISA-62443-2-1 (99.02.01) – *Security for industrial automation and control systems Part 2-1: Requirements for an IACS security management system* [5]

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 the normative references specified in clause 2 apply, in addition to the following.

NOTE Many of the following terms and definitions are originally based on relevant International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) or U.S. National Institute of Standards and Technology (NIST) sources, sometimes with minor modifications to enhance suitability when defining control system security requirements.

3.1.1

asset

physical or logical object having either a perceived or actual value to the IACS

Note to entry: In this specific case, an asset is any item that should be protected as part of the IACS security management system.

3.1.2**asset owner**

individual or company responsible for one or more IACS

Note 1 to entry: Used in place of the generic term end user to provide differentiation.

Note 2 to entry: This includes the components that are part of the IACS.

Note 3 to entry: In the context of this standard, an asset owner also includes the operator of the IACS.

3.1.3**attack**

assault on a system that derives from an intelligent threat

Note 1 to entry: For example, 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

Note 2 to entry: 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"), for example, 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.

3.1.4**authentication**

provision of assurance that a claimed characteristic of an identity is correct

Note to entry: Authentication is usually a prerequisite to allowing access to resources in a control system.

3.1.5**authenticator**

means used to confirm the identity of a user (human, software process or device)

Note to entry: For example, a password or token may be used as an authenticator.

3.1.6**authenticity**

property that an entity is what it claims to be

Note to entry: Authenticity is typically used in the context of confidence in the identity of an entity, or the validity of a transmission, a message or message originator.

3.1.7**automatic**

process or equipment that, under specified conditions, functions without human intervention

3.1.8**availability**

property of ensuring timely and reliable access to and use of control system information and functionality

3.1.9**communication channel**

specific logical or physical communication link between assets

Note to entry: A channel facilitates the establishment of a connection.

3.1.10**compensating countermeasure**

countermeasure employed in lieu of or in addition to inherent security capabilities to satisfy one or more security requirements

Note to entry: Examples include:

- (component-level): locked cabinet around a controller that doesn't have sufficient cyber access control countermeasures;
- (control system/zone-level): physical access control (guards, gates and guns) to protect a control room to restrict access to a group of known personnel to compensate for the technical requirement for personnel to be uniquely identified by the IACS; and
- (component-level): a vendor's programmable logic controller (PLC) can't meet the access control capabilities from an end-user, so the vendor puts a firewall in front of the PLC and sells it as a system.

3.1.11**compliance authority**

entity with legal jurisdiction to determine the adequacy of a security assessment, implementation or effectiveness as specified in a governing document

3.1.12**conduit**

logical grouping of communication channels, connecting two or more zones, that share common security requirements

Note to entry: A conduit is allowed to traverse a zone as long as the security of the channels contained within the conduit is not impacted by the zone.

3.1.13**confidentiality**

preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information

Note to entry: When used in the context of an IACS, refers to protecting IACS data and information from unauthorized access.

3.1.14**connection**

association established between two or more endpoints which supports the establishment of a session

3.1.15**consequence**

condition or state that logically or naturally follows from an event

3.1.16**control system**

hardware and software components of an IACS

3.1.17**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

Note to entry: The term "control" is also used to describe this concept in some contexts. The term countermeasure has been chosen for this document to avoid confusion with the term "control" in the context of "process control".

3.1.18**degraded mode**

mode of operation in the presence of faults which have been anticipated in the design of the control system

Note to entry: Degraded modes allow the control system to continue to provide essential functions despite the deficiency of one or several system elements, for example malfunction or outage of control equipment, disruption of communication due to failure or intentional system isolation in response to identified or suspected compromise of subsystems.

3.1.19

demilitarized zone

common, limited network of servers joining two or more zones for the purpose of controlling data flow between zones

Note to entry: Demilitarized zones (DMZs) are typically used to avoid direct connections between different zones.

3.1.20

device

asset incorporating one or more processors with the capability of sending or receiving data/control to or from another asset

Note to entry: Examples include controllers, human-machine interfaces (HMIs), PLCs, remote terminal units (RTUs), transmitters, actuators, valves, network switches, etc.

3.1.21

environment

surrounding objects, region or circumstances which may influence the behavior of the IACS and/or may be influenced by the IACS

3.1.22

essential function

function or capability that is required to maintain health, safety, the environment and availability for the equipment under control

Note to entry: Essential functions include, but are not limited to, the safety instrumented function (SIF), the control function and the ability of the operator to view and manipulate the equipment under control. The loss of essential functions is commonly termed loss of protection, loss of control and loss of view respectively. In some industries additional functions such as history may be considered essential.

3.1.23

event

occurrence of or change to a particular set of circumstances

Note to entry: In an IACS this may be an action taken by an individual (authorized or unauthorized), a change detected within the control system (normal or abnormal) or an automated response from the control system itself (normal or abnormal).

3.1.24

firecall

method established to provide emergency access to a secure control system

Note to entry: In an emergency situation, unprivileged users can gain access to key systems to correct the problem. When a firecall is used, there is usually a review process to ensure that the access was used properly to correct a problem. These methods generally either provide a one-time use user identifier (ID) or one-time password.

3.1.25

identifier

symbol, unique within its security domain, that identifies, indicates or names an entity which makes an assertion or claim of identity

3.1.26

identify

assertion of an identity

3.1.27

impact

evaluated consequence of a particular event

**3.1.28
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 control system

**3.1.29
industrial automation and control system**

collection of personnel, hardware, software and policies involved in the operation of the industrial process and that can affect or influence its safe, secure and reliable operation

**3.1.30
integrity**

property of protecting the accuracy and completeness of assets

**3.1.31
least privilege**

basic principle that holds that users (humans, software processes or devices) should be assigned the fewest privileges consistent with their assigned duties and functions

Note to entry: Least privilege is commonly implemented as a set of roles in an IACS.

**3.1.32
mobile code**

program transferred between a remote, possibly “untrusted” system, across a network or via removable media that can be executed unchanged on a local system without explicit installation or execution by the recipient

Note to entry: Examples of mobile code include JavaScript, VBScript, Java applets, ActiveX controls, Flash animations, Shockwave movies, and Microsoft Office macros.

**3.1.33
mobile device**

intelligent electronic device intended for use while mobile

Note to entry: Examples of mobile devices include laptop computers (depending on their usage, laptops can also be considered “portable devices”), mobile robots, smart phones, hand-held programmers, tablet computers and personal digital assistants.

**3.1.34
non-repudiation**

ability to prove the occurrence of a claimed event or action and its originating entities

Note to entry: The purpose of non-repudiation is to resolve disputes about the occurrence or non-occurrence of the event or action and involvement of entities in the event.

**3.1.35
portable device**

intelligent electronic device intended to be used in more than one physical location, but not intended for use while in transport between locations

Note to entry: Examples of portable devices include laptop computers (depending on their usage, laptops can also be considered “mobile devices”), maintenance workstations and analyzers.

**3.1.36
product supplier**

manufacturer of hardware and/or software product

Note to entry: Used in place of the generic word “vendor” to provide differentiation.

**3.1.37
remote access**

access to a control system by any user (human, software process or device) communicating from outside the perimeter of the zone being addressed

3.1.38**role**

set of connected behaviors, privileges and obligations associated with all users (humans, software processes or devices) of an IACS

Note to entry: The privileges to perform certain operations are assigned to specific roles.

3.1.39**safety instrumented system**

system used to implement one or more safety-related functions

3.1.40**security level**

measure of confidence that the IACS is free from vulnerabilities and functions in the intended manner

Note to entry: Vulnerabilities can either be designed into the IACS, inserted at any time during its lifecycle or result from changing threats. Designed-in vulnerabilities may be discovered long after the initial deployment of the IACS, for example an encryption technique has been broken or an improper policy for account management such as not removing old user accounts. Inserted vulnerabilities may be the result of a patch or a change in policy that opens up a new vulnerability.

3.1.41**service provider**

organization (internal or external organization, manufacturer, etc.) that has agreed to undertake responsibility for providing a given support service and obtaining, when specified, supplies in accordance with an agreement

Note to entry: This term is used in place of the generic word “vendor” to provide differentiation.

3.1.42**session**

semi-permanent, stateful and interactive information interchange between two or more communicating devices

Note to entry: Typically a session has clearly defined start and end processes.

3.1.43**session ID**

identifier used to indicate a specific session entry

3.1.44**set point**

target value identified within a control system that controls one or more actions within the control system

3.1.45**system integrator**

person or company that specializes in bringing together component subsystems into a whole and ensuring that those subsystems perform in accordance with project specifications

3.1.46**threat**

circumstance or event with the potential to adversely affect operations (including mission, functions, image or reputation), assets, control systems or individuals via unauthorized access, destruction, disclosure, modification of data and/or denial of service

3.1.47**trust**

confidence that an operation, data transaction source, network or software process can be relied upon to behave as expected

Note 1 to entry: Generally, an entity can be said to 'trust' a second entity when it (the first entity) makes the assumption that the second entity will behave as the first entity expects.

Note 2 to entry: This trust may apply only for some specific function.

3.1.48**untrusted**

not meeting predefined requirements to be trusted

Note to entry: An entity may simply be declared as untrusted.

3.1.49**zone**

grouping of logical or physical assets that share common security requirements

Note to entry: A zone has a clear border. The security policy of a zone is typically enforced by a combination of mechanisms both at the zone edge and within the zone.

3.2 Abbreviated terms and acronyms

AES	Advanced encryption standard
API	Application programming interface
ASLR	Address space layout randomization
BPCS	Basic process control system
CA	Certification authority
CIP	Critical infrastructure protection
COTS	Commercial off the shelf
CRL	Certificate revocation list
DC	Data confidentiality
DEP	Data execution prevention
DHCP	Dynamic host configuration protocol
DMZ	Demilitarized zone
DNS	Domain name service
DoS	Denial of service
EICAR	European Institute for Computer Antivirus Research
EMI	Electromagnetic interference
FAT	Factory acceptance testing
FIPS	[US NIST] Federal Information Processing Standard
FR	Foundational requirement
FS-PLC	Functional safety PLC
FTP	File transfer protocol
GLONASS	Global Navigation Satellite System
GPS	Global Positioning System
HMI	Human-machine interface
HSE	Health, safety and environmental
HTTP	Hypertext transfer protocol
HTTPS	HTTP secure
IAC	Identification and authentication control

IACS	Industrial automation and control system(s)
IAMS	Instrument asset management system
ID	Identifier
IDS	Intrusion detection system
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IM	Instant messaging
IP	Internet Protocol
IPS	Intrusion prevention system
ISA	International Society of Automation
ISO	International Organization for Standardization
IT	Information technology
MES	Manufacturing execution system
NERC	North American Electric Reliability Corporation
NIST	U.S. National Institute of Standards and Technology
NX	No Execute
OCSP	Online certificate status protocol
OWASP	Open Web Application Security Project
PDF	Portable document format
PKI	Public key infrastructure
PLC	Programmable logic controller
RA	Resource availability
RAM	Random access memory
RDF	Restricted data flow
RE	Requirement enhancement
RFC	[IETF] Request for Comment
RJ	Registered jack
RTU	Remote terminal unit
SAT	Site acceptance testing
SHA	Secure hash algorithm
SI	System integrity
SIEM	Security Information and Event Management
SIF	Safety instrumented function
SIL	Safety integrity level
SIS	Safety instrumented system
SL	Security level
SL-A	Achieved security level
SL-C	Capability security level

SL-T	Target security level
SP	[US NIST] Special Publication
SR	System requirement
SSH	Secure socket shell
SuC	System under consideration
TCP	Transmission Control Protocol
TPM	Trusted platform module
TRE	Timely response to events
UC	Use control
USB	Universal serial bus
VoIP	Voice over internet protocol
WEP	Wired equivalent privacy
WLAN	Wireless local area network

3.3 Conventions

This document expands the seven FRs defined in ISA-62443-1-1 (99.01.01) into a series of SRs. Each SR has a baseline requirement and zero or more requirement enhancements (REs) to strengthen security. To provide clarity to the reader, rationale and supplemental guidance is provided for each baseline requirement and notes for any associated REs as is deemed necessary. The baseline requirement and REs, if present, are then mapped to the control system capability security level, SL-C(FR, control system) 1 to 4.

All seven FRs have a defined set of four SLs. The control system capability level 0 for a particular FR is implicitly defined as no requirements. For example, the purpose statement for clause 8, FR 4 – Data confidentiality, is:

Ensure the confidentiality of information on communication channels and in data repositories to prevent unauthorized disclosure.

The associated four SLs are defined as:

- SL 1 – Prevent the unauthorized disclosure of information via eavesdropping or casual exposure.
- SL 2 – Prevent the unauthorized disclosure of information to an entity actively searching for it using simple means with low resources, generic skills and low motivation.
- SL 3 – Prevent the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with moderate resources, IACS specific skills and moderate motivation.
- SL 4 – Prevent the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with extended resources, IACS specific skills and high motivation.

The individual SR and RE assignments are thus based on an incremental increase in overall control system security for that particular FR.

The SL-C(control system), used throughout this document, signifies a capability required to meet a given SL rating for a given FR. A complete description of the SL vector concept can be found in Annex A.

4 Common control system security constraints

NOTE The contents of this clause will eventually be incorporated into ISA-62443-1-1 (99.01.01).

4.1 Overview

When reading, specifying and implementing the control system SRs detailed in clauses 5 through 11 of this standard, there are a number of common constraints that shall be adhered to. Clause 0 of this document provided some contextual, informative discussion of what this standard is designed to accomplish. This clause and the subsequent FR-specific clauses furnish the normative material necessary to build extensions to existing enterprise security to support the rigorous integrity and availability requirements needed by IACS.

4.2 Support of essential functions

As documented in clause 3.1.22, an essential function is a “function or capability that is required to maintain health, safety, the environment and availability for the equipment under control.”

- Security measures shall not adversely affect essential functions of a high availability IACS unless supported by a risk assessment.

NOTE Refer to ISA-62443-2-1 (99.02.01) regarding the documentation requirements associated with the risk assessment required to support instances where security measures may affect essential functions.

When reading, specifying and implementing the SRs described in this standard, implementation of security measures should not cause loss of protection, loss of control, loss of view or loss of other essential functions. After a risk analysis, some facilities may determine certain types of security measures may halt continuous operations, but security measures shall not result in loss of protection that could result in health, safety and environmental (HSE) consequences. Some specific constraints include:

- Access Controls (IAC and UC) shall not prevent the operation of essential functions, specifically:
 - Accounts used for essential functions shall not be locked out, even temporarily (see 5.5, SR 1.3 – Account management, 5.6, SR 1.4 – Identifier management, 5.13, SR 1.11 – Unsuccessful login attempts and 6.7, SR 2.5 – Session lock).
 - Verifying and recording operator actions to enforce non-repudiation shall not add significant delay to system response time (see 6.14, SR 2.12 – Non-repudiation).
 - For high availability control systems, the failure of the certificate authority shall not interrupt essential functions (see 5.10, SR 1.8 – Public key infrastructure (PKI) certificates).
 - Identification and authentication shall not prevent the initiation of the SIF (see 5.3, SR 1.1 – Human user identification and authentication and 5.4, SR 1.2 – Software process and device identification and authentication). Similarly for authorization enforcement (see 6.3, SR 2.1 – Authorization enforcement).
 - Incorrectly timestamped audit records (see 6.10, SR 2.8 – Auditable events and 6.13 SR 2.11 – Timestamps) shall not adversely affect essential functions.
- Essential functions of an IACS shall be maintained if zone boundary protection goes into fail-close and/or island mode (see 9.4, SR 5.2 – Zone boundary protection).
- A denial of service (DoS) event on the control system or safety instrumented system (SIS) network shall not prevent the SIF from acting (see 11.3, SR 7.1 – Denial of service protection).

4.3 Compensating countermeasures

Compensating countermeasures, as used in this document, shall adhere to the guidelines described in ISA-62443-3-2 (99.03.02).

Throughout this standard, the SR normative language states that “the control system shall provide the capability to...” support some specific security requirement. The control system shall provide the capability, but it might be performed by an external component. In such a case, the control system shall provide an ‘interface’ to that external component. Some examples of compensating countermeasures include user identification (including centralized versus distributed), password strength enforcement, signature validity checking, security event correlation and device decommissioning (information persistence).

NOTE 1 The control system security requirements detailed in this document pertain to all technical functions relevant to a control system including tools and applications. However, as noted here, some of these functions can be handled by an external resource.

NOTE 2 In some high resource availability applications (high SL-T(RA,control system)), compensating countermeasures external to the control system (such as additional physical security measures and/or enhanced personnel background checks) will be needed. In these cases, it may be possible to see a normally high resource availability SL control system at a lower IAC SL 1 or 2 rating, depending upon the compensating countermeasures. Lockout or loss of control due to security measures is increased, not decreased for very high availability SL control system. Thus higher SLs are not always “better”, even where cost is not a significant factor.

4.4 Least privilege

The capability to enforce the concept of least privilege shall be provided, with granularity of permissions and flexibility of mapping those permissions to roles sufficient to support it. Individual accountability should be available when required.

5 FR 1 – Identification and authentication control

5.1 Purpose and SL-C(IAC) descriptions

Identify and authenticate all users (humans, software processes and devices) before allowing them to access to the control system.

- SL 1 – Identify and authenticate all users (humans, software processes and devices) by mechanisms which protect against casual or coincidental access by unauthenticated entities.
- SL 2 – Identify and authenticate all users (humans, software processes and devices) by mechanisms which protect against intentional unauthenticated access by entities using simple means with low resources, generic skills and low motivation.
- SL 3 – Identify and authenticate all users (humans, software processes and devices) by mechanisms which protect against intentional unauthenticated access by entities using sophisticated means with moderate resources, IACS specific skills and moderate motivation.
- SL 4 – Identify and authenticate all users (humans, software processes and devices) by mechanisms which protect against intentional unauthenticated access by entities using sophisticated means with extended resources, IACS specific skills and high motivation.

5.2 Rationale

Asset owners will have to develop a list of all users (humans, software processes and devices) and to determine for each control system component the required level of IAC protection. The goal of IAC is to protect the control system by verifying the identity of any user requesting access to the control system before activating the communication. Recommendations and guidelines should include mechanisms that will operate in mixed modes. For example, some control system components require strong IAC, such as strong authentication mechanisms, and others do not.

5.3 SR 1.1 – Human user identification and authentication

5.3.1 Requirement

The control system shall provide the capability to identify and authenticate all human users. This capability shall enforce such identification and authentication on all interfaces which provide

human user access to the control system to support segregation of duties and least privilege in accordance with applicable security policies and procedures.

5.3.2 Rationale and supplemental guidance

All human users need to be identified and authenticated for all access to the control system. Authentication of the identity of these users should be accomplished by using methods such as passwords, tokens, biometrics or, in the case of multifactor authentication, some combination thereof. The geographic location of human users can also be used as part of the authentication process. This requirement should be applied to both local and remote access to the control system. In addition to identifying and authenticating all human users at the control system level (for example, at system login), identification and authentication mechanisms are often employed at the application level.

Where human users function as a single group (such as control room operators), user identification and authentication may be role-based or group-based. For some control systems, the capability for immediate operator interaction is critical. It is essential that local emergency actions as well as control system essential functions not be hampered by identification or authentication requirements (see clause 4 for a more complete discussion). Access to these systems may be restricted by appropriate physical security mechanisms (see ISA-62443-2-1 (99.02.01)). An example of such a situation is a critical operations room where strict physical access control and monitoring is in place and where shift plans allocate responsibility to a group of users. These users may then be using the same user identity. In addition, the designated operator workstation clients should be authenticated (see 5.4, SR 1.2 – Software process and device identification and authentication) or the use of this shared account should be limited to the constrained environment of the control room.

In order to support IAC policies, as defined according to ISA-62443-2-1 (99.02.01), the control system verifies the identity of all human users as a first step. In a second step, the permissions assigned to the identified human user are enforced (see 6.3, SR 2.1 – Authorization enforcement).

5.3.3 Requirement enhancements

(1) Unique identification and authentication

The control system shall provide the capability to uniquely identify and authenticate all human users.

(2) Multifactor authentication for untrusted networks

The control system shall provide the capability to employ multifactor authentication for human user access to the control system via an untrusted network (see 5.15, SR 1.13 – Access via untrusted networks).

NOTE See 5.7.3 (1), SR 1.5 – Authenticator management, RE (1) for enhanced authenticator management for software processes.

(3) Multifactor authentication for all networks

The control system shall provide the capability to employ multifactor authentication for all human user access to the control system.

5.3.4 Security levels

The requirements for the four SL levels that relate to SR 1.1 – Human user identification and authentication are:

- SL-C(IAC, control system) 1: SR 1.1
- SL-C(IAC, control system) 2: SR 1.1 (1)
- SL-C(IAC, control system) 3: SR 1.1 (1) (2)