



Standards
Certification
Education & Training
Publishing
Conferences & Exhibits

Setting the Standard for Automation™

AMERICAN NATIONAL STANDARD

ANSI/ISA-62443-4-2-2018

Security for industrial automation and control systems, Part 4-2: Technical security requirements for IACS components

Approved 13 August 2018

NOTICE OF COPYRIGHT

This is a copyrighted document and may not be copied or distributed in any form or manner without the permission of ISA. This copy of the document was made for the sole use of the person to whom ISA provided it and is subject to the restrictions stated in ISA's license to that person. It may not be provided to any other person in print, electronic, or any other form. Violations of ISA's copyright will be prosecuted to the fullest extent of the law and may result in substantial civil and criminal penalties.



Documents
Document Sharing Hub

ANSI/ISA-62443-4-2-2018

Security for industrial automation and control systems – Part 4-2:
Technical security requirements for IACS components

ISBN: 978-1-64331-025-1

Copyright © 2018 by ISA. All rights reserved. Not for resale. Printed in the United States of America.

ISA

67 T.W. 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-62443-4-2.

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 T.W. 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.

ISA (www.isa.org) is a nonprofit professional association that sets the standard for those who apply engineering and technology to improve the management, safety, and cybersecurity of modern automation and control systems used across industry and critical infrastructure. Founded in 1945, ISA develops widely used global standards; certifies industry professionals; provides education and training; publishes books and technical articles; hosts conferences and exhibits; and provides networking and career development programs for its 40,000 members and 400,000 customers around the world.

ISA owns Automation.com, a leading online publisher of automation-related content, and is the founding sponsor of The Automation Federation (www.automationfederation.org), an association of nonprofit organizations serving as “The Voice of Automation.” Through a wholly owned subsidiary, ISA bridges the gap between standards and their implementation with the ISA Security Compliance Institute (www.isasecure.org) and the ISA Wireless Compliance Institute (www.isa100wci.org).

The following people served as active members of ISA99 Working Group 04, Task Group 4 in the preparation of this document:

Name	Company	Contributor	Reviewer
Kevin Staggs, TG Chair	Honeywell Inc.	X	
Dennis Brandl	BR&L Consulting		X
Khaled Brown	Intel Security		X
Eric Byres	Byres Security Consulting.		X
Eric Cosman	OIT Concepts, LLC		X
William Cotter	3M Company		X
Ed Crawford	ProcessControl/SCADA Security		X
John Cusimano	AE Solutions	X	
Maarten de Caluwé	Dow Benelux BV		X
Michael Dransfield	NSA	X	
Mark Fabro	Lofty Perch Inc.		X
Ronald Forrest	Forrest Automation & Technology Solutions LLC		X
Dirk Gebert	Siemens AG	X	
Jim Gilsinn	Kenexis Consulting	X	
Thomas Good	ICS Security Consultant		X
Evan Hand	Consultant		X
Vic Hammond	Argonne National Laboratory		X
Mark Heard	TMD Consulting		X
Dennis Holstein	OPUS Consulting Group		X
Bruce Honda	Weyerhaeuser		X
Charles Hoover	Emerson	X	
Eric Hopp	Rockwell Automation		X
Bob Huba	Tall Corn Security Consulting		X
Andrew Kling	Schneider Electric	X	
Pierre Kobes	Siemens AG	X	
Nate Kube	Consultant	X	
Joel Langill	AECOM		X

Suzanne Lightman	NIST		X
Charles Mastromonico	Westinghouse Savannah River Co.		X
Mike Medoff	Exida		X
Roberto Minicucci	GE Oil and Gas	X	
Ajay Mishra	Schneider Electric	X	
Jason Moore	Xilinx Inc.	X	
Alex Nicoll	Rockwell Automation	X	
Johan Nye	Consultant	X	
Bryan Owen	OSISoft Inc		X
Tom Phinney	Consultant		X
Jeff Potter	Consultant	X	
Bob Radvanovsky	Infracritical		X
Judith Rossebo	ABB AS	X	
Ragnar Schierholz	ABB AG	X	
Omar Sherin	Q-Cert		X
Leon Steinocher	Redstone Investors		X
Herman Storey	Herman Storey Consulting		X
Michele Struvay	NXP Semiconductors	X	
Tatsuaki Takebe	KPMG Consulting Co., Ltd.		X
Bradley Taylor	The Catholic University of America		X
Zachary Tudor	Idaho National Laboratory		X
Joseph Weiss	Applied Control Solutions LLC		X
Ludwig Winkel	Siemens AG		X

This standard was approved for publication by the ISA Standards and Practices Board on 12 July 2018.

NAME

COMPANY

M. Wilkins, Vice President	Yokogawa UK Ltd.
D. Bartusiak	ExxonMobil Research & Engineering
D. Brandl	BR&L Consulting
P. Brett	Honeywell Inc.
E. Cosman	OIT Concepts, LLC
D. Dunn	T.F. Hudgins, Inc. - Allied Reliability Group
J. Federlein	Federlein & Assoc. LLC
B. Fitzpatrick	Wood PLC
J.-P. Hauet	Hauet.com
D. Lee	Avid Solutions Inc.
G. Lehmann	AECOM
T. McAviney	Consultant
V. Mezzano	Fluor Corp.
C. Monchinski	Automated Control Concepts Inc.
G. Nasby	City of Guelph Water Services
M. Nixon	Emerson Process Management
D. Reed	Rockwell Automation
N. Sands	DuPont Company

H. Sasajima
H. Storey
K. Unger
I. Verhappen
D. Visnich
I. Weber
W. Weidman
J. Weiss
D. Zetterberg

Fieldcomm Group Inc. Asia-Pacific
Herman Storey Consulting
Advanced Operational Excellence Co.
Industrial Automation Networks
Burns & McDonnell
Siemens AG DF FA
Consultant
Applied Control Solutions LLC
Chevron Energy Technology Co.

CONTENTS

0	Introduction	13
0.1	Overview.....	13
0.2	Purpose and intended audience	13
1	Scope	17
2	Normative references	17
3	Terms, definitions, abbreviated terms, acronyms, and conventions	17
3.1	Terms and definitions.....	17
3.2	Abbreviated terms and acronyms	23
3.3	Conventions.....	25
4	Common Component Security Constraints	26
4.1	Overview.....	26
4.2	CCSC 1 Support of essential functions.....	26
4.3	CCSC 2 Compensating countermeasures.....	26
4.4	CCSC 3 Least privilege	27
4.5	CCSC 4 Software development process	27
5	FR 1 – Identification and authentication control	27
5.1	Purpose and SL-C(IAC) descriptions.....	27
5.2	Rationale	27
5.3	CR 1.1 – Human user identification and authentication	27
5.4	CR 1.2 – Software process and device identification and authentication	28
5.5	CR 1.3 – Account management.....	29
5.6	CR 1.4 – Identifier management.....	30
5.7	CR 1.5 – Authenticator management.....	30
5.8	CR 1.6 – Wireless access management	32
5.9	CR 1.7 – Strength of password-based authentication	32
5.10	CR 1.8 – Public key infrastructure certificates	33
5.11	CR 1.9 – Strength of public key-based authentication	33
5.12	CR 1.10 – Authenticator feedback.....	34
5.13	CR 1.11 – Unsuccessful login attempts	35
5.14	CR 1.12 – System use notification	36
5.15	CR 1.13 – Access via untrusted networks	36
5.16	CR 1.14 – Strength of symmetric key-based authentication	36
6	FR 2 – Use control.....	37
6.1	Purpose and SL-C(UC) descriptions.....	37
6.2	Rationale	38
6.3	CR 2.1 – Authorization enforcement.....	38
6.4	CR 2.2 – Wireless use control	39
6.5	CR 2.3 – Use control for portable and mobile devices	40
6.6	CR 2.4 – Mobile code.....	40
6.7	CR 2.5 – Session lock.....	40
6.8	CR 2.6 – Remote session termination	40
6.9	CR 2.7 – Concurrent session control	41

Copyright International Society of Automation

6.10	CR 2.8 – Auditable events.....	41
6.11	CR 2.9 – Audit storage capacity	42
6.12	CR 2.10 – Response to audit processing failures	43
6.13	CR 2.11 – Timestamps.....	43
6.14	CR 2.12 – Non-repudiation.....	44
6.15	CR 2.13 – Use of physical diagnostic and test interfaces	45
7	FR 3 – System integrity	45
7.1	Purpose and SL-C(SI) descriptions	45
7.2	Rationale	45
7.3	CR 3.1 – Communication integrity	45
7.4	CR 3.2 – Protection from malicious code.....	46
7.5	CR 3.3 – Security functionality verification	46
7.6	CR 3.4 – Software and information integrity	47
7.7	CR 3.5 – Input validation.....	48
7.8	CR 3.6 – Deterministic output	48
7.9	CR 3.7 – Error handling	49
7.10	CR 3.8 – Session integrity.....	50
7.11	CR 3.9 – Protection of audit information.....	50
7.12	CR 3.10 – Support for updates.....	51
7.13	CR 3.11 – Physical tamper resistance and detection	51
7.14	CR 3.12 – Provisioning product supplier roots of trust	51
7.15	CR 3.13 – Provisioning asset owner roots of trust	51
7.16	CR 3.14 – Integrity of the boot process	51
8	FR 4 – Data confidentiality	51
8.1	Purpose and SL-C(DC) descriptions.....	51
8.2	Rationale	52
8.3	CR 4.1 – Information confidentiality	52
8.4	CR 4.2 – Information persistence	52
8.5	CR 4.3 – Use of cryptography	53
9	FR 5 – Restricted data flow	54
9.1	Purpose and SL-C(RDF) descriptions.....	54
9.2	Rationale	54
9.3	CR 5.1 – Network segmentation	54
9.4	CR 5.2 – Zone boundary protection.....	55
9.5	CR 5.3 – General-purpose person-to-person communication restrictions.....	55
9.6	CR 5.4 – Application partitioning	55
10	FR 6 – Timely response to events	55
10.1	Purpose and SL-C(TRE) descriptions.....	55
10.2	Rationale	56
10.3	CR 6.1 – Audit log accessibility	56
10.4	CR 6.2 – Continuous monitoring.....	56
11	FR 7 – Resource availability.....	57
11.1	Purpose and SL-C(RA) descriptions.....	57
11.2	Rationale	57

11.3	CR 7.1 – Denial of service protection	58
11.4	CR 7.2 – Resource management.....	58
11.5	CR 7.3 – Control system backup	59
11.6	CR 7.4 – Control system recovery and reconstitution	59
11.7	CR 7.5 - Emergency Power	60
11.8	CR 7.6 – Network and security configuration settings.....	60
11.9	CR 7.7 – Least functionality	60
11.10	CR 7.8 – Control system component inventory	61
12	Software application requirements	61
12.1	Purpose	61
12.2	SAR 2.4 – Mobile code.....	61
12.3	SAR 3.2 – Protection from malicious code.....	62
13	Embedded device requirements	63
13.1	Purpose	63
13.2	EDR 2.4 – Mobile code	63
13.3	EDR 2.13 – Use of physical diagnostic and test interfaces	63
13.4	EDR 3.2 – Protection from malicious code	64
13.5	EDR 3.10 – Support for updates.....	65
13.6	EDR 3.11 – Physical tamper resistance and detection.....	65
13.7	EDR 3.12 – Provisioning product supplier roots of trust.....	66
13.8	EDR 3.13 – Provisioning asset owner roots of trust.....	67
13.9	EDR 3.14 – Integrity of the boot process	68
14	Host device requirements.....	68
14.1	Purpose	68
14.2	HDR 2.4 – Mobile code	68
14.3	HDR 2.13 – Use of physical diagnostic and test interfaces	69
14.4	HDR 3.2 – Protection from malicious code	70
14.5	HDR 3.10 – Support for updates	70
14.6	HDR 3.11 – Physical tamper resistance and detection	71
14.7	HDR 3.12 – Provisioning product supplier roots of trust	71
14.8	HDR 3.13 – Provisioning asset owner roots of trust.....	72
14.9	HDR 3.14 – Integrity of the boot process.....	73
15	Network device requirements	73
15.1	Purpose	73
15.2	NDR 1.6 – Wireless access management.....	74
15.3	NDR 1.13 – Access via untrusted networks	74
15.4	NDR 2.4 – Mobile code	75
15.5	NDR 2.13 – Use of physical diagnostic and test interfaces	76
15.6	NDR 3.2 – Protection from malicious code	76
15.7	NDR 3.10 – Support for updates	77
15.8	NDR 3.11 – Physical tamper resistance and detection	77
15.9	NDR 3.12 – Provisioning product supplier roots of trust	78
15.10	NDR 3.13 – Provisioning asset owner roots of trust.....	79
15.11	NDR 3.14 – Integrity of the boot process.....	80

15.12 NDR 5.2 – Zone boundary protection	80
15.13 NDR 5.3 – General purpose, person-to-person communication restrictions	81
Annex A (informative) Device categories	83
A.1 Device categories	83
A.1.1 Device category: embedded device	83
A.1.2 Device category: network device	84
A.1.3 Device category: host device/application	84
Annex B (informative) Mapping of CRs and REs to FR SLs 1-4	87
B.1 Overview.....	87
B.2 SL mapping table	87
Figure 1 – ISA-62443 Work Products	15

FOREWORD

This document is part of a multipart standard that addresses the issue of security for the components which are contained in industrial automation and control systems (IACS). It has been developed by working group 04, task group 4 of the ISA99 committee in cooperation with IEC TC65/WG10.

This document prescribes the security requirements for the components that are used to build control systems. These security requirements are derived from the system requirements for IACS defined in ISA-62443-3-3:2013 [1]¹ and as such, assigns component security levels (SLs) which are based on the system security levels.

¹ Numbers in brackets indicate references in the Bibliography.

This page intentionally left blank.

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 this 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 choosing to deploy business information technology (IT) cyber security solutions to address IACS security may not fully comprehend the results of their 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 countermeasures should not have the potential to cause loss of essential services and functions, including emergency procedures. (IT security countermeasures, 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 the risk assessment, as required by ISA-62443-2-1² [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 provides the cyber security technical requirements for the components that make up an IACS, specifically the embedded devices, network components, host components and software applications. This document derives its requirements from the IACS System security requirements described in ISA-62443-3-3 [11]. The intent of this document is to specify security capabilities that enable a component to mitigate threats for a given security level (SL) without the assistance of compensating countermeasures.

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 integrity and availability needed by IACS.

0.2 Purpose and intended audience

The IACS community audience for this document is intended to be asset owners, system integrators, product suppliers, and, where appropriate, compliance authorities. Compliance

² Many documents in the ISA-62443 series are currently under review or in development.

authorities include government agencies and regulators with the legal authority to perform audits to verify compliance with governing laws and regulations.

System integrators will use this document to assist them in procuring control system components that make up an IACS solution. The assistance will be in the form of helping system integrators specify the appropriate security capability level of the individual components they require. The primary standards for system integrators are ISA-62443-2-1 [5], ISA-62443-2-4 [8], ISA-62443-3-2 [10] and ISA-62443-3-3 [11] that provide organizational and operational requirements for a security management system and guide them through the process of defining security zones for a system and the target security capability levels (SL-T) for those zones. Once the SL-T for each zone has been defined, components that provide the necessary security capabilities can be used to achieve the SL-T for each zone.

Product suppliers will use this document to understand the requirements placed on control system components for specific security capability level (SL-C)s of those components. A component may not provide a required capability itself but may be designed to integrate with a higher level entity and thus benefit from that entity's capability - for example an embedded device may not be maintaining a user directory itself, but may integrate with a system wide authentication and authorization service and thus still meet the requirements to provide individual user authentication, authorization and management capabilities. This document will guide product suppliers as to which requirements can be allocated and which requirements need to be native in the components. As defined in Practice 8 of ISA-62443-4-1 [12], the product supplier will provide documentation of how to properly integrate the component into a system to meet a specific SL-T.

The component requirements (CRs) in this document are derived from the system requirements (SRs) in ISA-62443-3-3 [11]. The requirements in ISA-62443-3-3 [11] are referred to as SRs, which are derived from the overall foundational requirements (FRs) defined in ISA-62443-1-1 [1]. CRs may also include a set of requirement enhancements (REs). The combination of CRs and REs is what will determine the target security level that a component is capable of.

This document provides component requirements for four types of components: software application, embedded device, host device and network device. Thus the CRs for each type of component will be designated as follows:

- Software application requirements (SAR);
- Embedded device requirements (EDR);
- Host device requirements (HDR); and
- Network device requirements (NDR).

The majority of the requirements in this document are the same for the four types of components and are thus designated simply as a CR. When there are unique component-specific requirements then the generic requirement will state that the requirements are component-specific and are located in the component-specific requirements clauses of this standard.

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

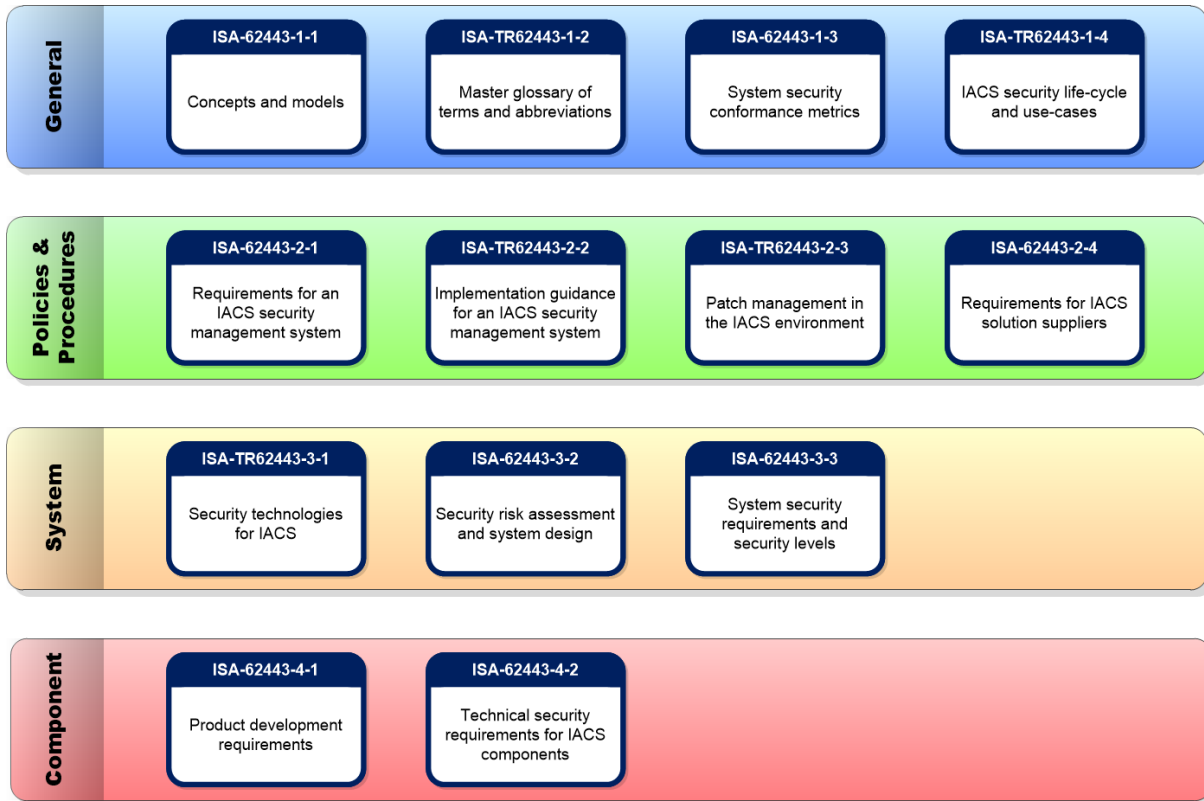


Figure 1 – ISA-62443 Work Products

This page intentionally left blank.

1 Scope

This document in the ISA-62443 series provides detailed technical control system component requirements (CRs) associated with the seven foundational requirements (FRs) described in ISA-62443-1-1 [1] including defining the requirements for control system capability security levels and their components, SL-C(component).

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

- a) Identification and authentication control (IAC),
- b) Use control (UC),
- c) System integrity (SI),
- d) Data confidentiality (DC),
- e) Restricted data flow (RDF),
- f) Timely response to events (TRE), and
- g) Resource availability (RA).

These seven FRs are the foundation for defining control system security capability levels. Defining security capability levels for the control system component is the goal and objective of this document as opposed to SL-T or achieved SLs (SL-A), which are out of scope.

NOTE Refer to ISA-62443-2-1 [5] for an equivalent set of non-technical, program-related, capability requirements necessary for fully achieving a SL-T(control system).

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 – *Security for industrial automation and control systems, Part 1-1: Concepts and models* [1]

ISA-TR62443-1-2, *Security for industrial automation and control systems, Part 1-2: Master glossary of terms and abbreviations* [2]

ISA-62443-3-3:2013 – *Security for industrial automation and control systems, Part 3-3: System security requirements and security levels* [11]

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) and U.S. National Institute of Standards and Technology (NIST) sources, sometimes with minor modifications to enhance suitability for IACS security requirements.

3.1.1 asset

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

Note 1 to entry: In this specific case, an asset is any item that should be protected as part of the IACS security management system.

Note 2 to entry: An asset is not limited to the IACS alone, but can also include the physical assets under its control

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 document, an asset owner also includes the operator of the IACS.

3.1.3**attack**

unauthorized attempt to compromise the confidentiality, integrity or availability of an IACS 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**

the verification of the claimed identity of an entity

Note 1 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 an entity

Note 1 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 through authentication of origin and verification of integrity

Note 1 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 1 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 1 to entry: Examples include:

- (component-level): locked cabinet around a controller that otherwise might be exposed to unauthorized access via its physical data interfaces;
- (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 product supplier's programmable logic controller (PLC) cannot meet the access control capabilities from an asset owner, so the product supplier puts a firewall in front of the PLC and sells it as a system.

3.1.11

component

entity belonging to an IACS that exhibits the characteristics of one or more of a host device, network device, software application, or embedded device

3.1.12

conduit

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

Note 1 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

assurance that information is not disclosed to unauthorized individuals, processes, or devices

Note 1 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 that supports the establishment of a session

3.1.15

control system

hardware and software components of an IACS

3.1.16

countermeasure

action, device, procedure or technique that reduces a threat, a vulnerability or the consequences of an attack by minimizing the harm the attack can cause or by discovering and reporting it so that corrective action can be taken

Note 1 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" and "control system".

3.1.17

degraded mode

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

Note 1 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.

3.1.18

device

discrete physical asset that provides a set of capabilities

Note 1 to entry: Examples include controllers, human-machine interfaces (HMIs), PLCs, remote terminal units (RTUs), transmitters, actuators, valves, network switches, etc.

Note 2 to entry: A device may exhibit the characteristics of one or more of a host device, network device, software application, or embedded device

3.1.19

embedded device

special purpose device designed to directly monitor or control an industrial process

Note 1 to entry: Typical attributes limited storage, limited number of exposed services, programmed through an external interface, embedded operating systems (OSs) or firmware equivalent, real-time scheduler, may have an attached control panel, and may have a communications interface.

Note 2 to entry: Examples include PLCs, wired or wireless field sensor devices, wired or wireless field actuator devices, safety instrumented system (SIS) controllers, distributed control system (DCS) controllers.

3.1.20

environment

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

3.1.21

essential function

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

Note 1 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.

3.1.22

event

occurrence of or change to a particular set of circumstances

Note 1 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).

3.1.23

firecall

method established to provide emergency access to a secure control system

Note 1 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.

3.1.24

host device

general purpose device running an operating system (for example Microsoft Windows OS or Linux) capable of hosting one or more software applications, data stores or functions from one or more suppliers

Note 1 to entry: Typical attributes include filesystem(s), programmable services, no real time scheduler and full HMI (keyboard, mouse, etc.).

3.1.25

identifier

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

3.1.26

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

3.1.27

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

3.1.28

integrity

property of protecting the accuracy and completeness of assets

3.1.29

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

3.1.30

mobile code

program transferred between assets that can be executed without explicit installation by the recipient

Note 1 to entry: Examples of mobile code include JavaScript, VBScript, Java applets, ActiveX controls, Flash animations, Shockwave movies, and Microsoft Office macros.

3.1.31

mobile device

intelligent electronic device intended for use while being transported

Note 1 to entry: Examples of mobile devices include laptop computers, mobile robots, smart phones, hand-held programmers, tablet computers and personal digital assistants.

3.1.32

network device

device that facilitates data flow between devices, or restricts the flow of data, but may not directly interact with a control process

Note 1 to entry: Typical attributes include embedded OS or firmware, no HMI, no real-time scheduler and configured through an external interface.

3.1.33

non-repudiation

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

Note 1 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.

3.1.34

product supplier

manufacturer of hardware and/or software product

Note 1 to entry: Used in place of the generic word “vendor” to provide differentiation.

3.1.35**remote access**

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

3.1.36**role**

set of connected behaviors, privileges and obligations that may be assigned to a user or group of users (humans, software processes or devices) of an IACS

Note 1 to entry: The privileges to perform certain operations are assigned to specific roles.

3.1.37**safety instrumented system**

system used to implement one or more safety-related functions

3.1.38**security level**

level corresponding to the required set of countermeasures and inherent security properties of devices and systems for a zone or conduit based on assessment of risk for the zone or conduit

3.1.39**session**

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

Note 1 to entry: Typically a session has clearly defined start and end processes.

3.1.40**session ID**

identifier used to indicate a specific session

3.1.41**set point**

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

3.1.42**software application**

one or more software programs and their dependencies that are used to interface with the process or the control system itself (for example, configuration software and historian)

Note 1 to entry: Software applications typically execute on host devices or embedded devices.

Note 2 to entry: Dependencies are any software programs that are necessary for the software application to function such as database packages, reporting tools, or any third party or open source software.

3.1.43**system integrator**

service provider that specializes in bringing together component subsystems into a whole and ensuring that those subsystems perform in accordance with project specifications

Note 1 to entry: This may also include other system supplier designations such as General Automation Contractor, Main Automation Contractor, Main Instrument Vendor, and similar.

3.1.44**threat**

set of circumstances and associated sequence of events 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

3.1.45

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.

3.1.46

untraceability

assurance that information cannot be used to track the time or location of a specific user

3.1.47

untrusted

not meeting predefined requirements to be trusted

Note 1 to entry: An entity may simply be declared as untrusted.

3.1.48

update

incremental hardware or software change in order to address security vulnerabilities, bugs, reliability or operability issues

3.1.49

upgrade

incremental hardware or software change in order to add new features

3.1.50

zone

collection of entities that represents partitioning of a System under Consideration on the basis of their functional, logical and physical (including location) relationship

Note 1 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

ANSI	American National Standards Institute
API	Application programming interface
ASLR	Address space layout randomization
AVA_VAN	Common Criteria Class AVA Vulnerability Assessment
CA	Certification authority
CMAC	Cipher-based Message Authentication Code
COTS	Commercial off the shelf
CR	Component requirement
DC	Data confidentiality
DCS	Distributed control system
DEP	Data execution prevention
DMZ	Demilitarized zone
DoS	Denial of service
EAL	Evaluated assurance level
EDR	Embedded device requirement

EICAR	European Institute for Computer Antivirus Research
FAT7	Factory acceptance testing
FDA	[US] Food and Drug Administration
FIPS	[US NIST] Federal Information Processing Standard
FR	Foundational requirement
FTP	File transfer protocol
GCM	Galois/Counter mode
GMAC	Galois message authentication code
HDR	Host device requirement
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)
ID	Identifier
IDS	Intrusion detection system
IED	Intelligent electronic device
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IM	Instant messaging
IP	Internet protocol
IPS	Intrusion prevention system
ISA	International Society of Automation
ISO	International Organization for Standardization
IT	Information technology
JTAG	Joint Test Action Group
NDR	Network device requirement
NIST	U.S. National Institute of Standards and Technology
NX	No Execute
OS	Operating system
OWASP	Open Web Application Security Project
PC	Personal computer
PDF	Portable document format
PII	Personally identifiable information
PKI	Public key infrastructure
PLC	Programmable logic controller
PUF	Physically uncloneable function
RA	Resource availability

RADIUS	Remote authentication dial-in user service
RAM	Random access memory
RDF	Restricted data flow
RE	Requirement enhancement
RTOS	Real-time operating system
RTU	Remote terminal unit
SAR	Software application requirements
SAT	Site acceptance testing
SFTP	Secure FTP
SI	System integrity
SIEM	Security information and event management
SIF	Safety instrumented function
SIS	Safety instrumented system
SL	Security level
SL-A	Achieved security level
SL-C	Capability security level
SL-T	Target security level
SNMP	Simple network management protocol
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
VPN	Virtual private network

3.3 Conventions

This document expands the SRs and REs defined in ISA-62443-3-3 [11] into a series of CRs and REs for the components contained within an IACS. To maintain ease of tracing the CRs to the SRs in ISA-62443-3-3 [11] the CR numbering will match the associated SR. This will cause some gaps and non-sequential numbering in this document. 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 types of components of an IACS as defined in this document are: software applications, host devices, embedded devices and network devices. The majority of the CRs and REs are applicable to all four types of components and are combined into a single Component Requirement (CR). Some CRs and REs are unique to a specific type of component. These component-type specific requirements have been separated into separate clauses for ease of reference. Requirements specific to software applications, embedded devices, host devices, and network devices are covered beginning with clause 12. Where a component meets the definition of one or more of

software application, host device, embedded device or network device, that component is expected to meet all of the requirements listed for each of the component types it satisfies.

Each of the seven FRs defined in ISA-62443-1-1 [1] has a defined set of four security levels (SLs). These SLs are derived from the system security levels defined in ISA-62443-3-3 [11]. A component's security level is described per FR, using the notation SL-C(FR, component), with a corresponding value of 0 through 4. The control system capability level 0 for a particular FR is implicitly defined as no requirements. The baseline requirement and REs, if present, for each FR are then mapped to the component capability security level, SL-C(FR, component) 1 to 4.

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 CR and RE assignments are thus based on an incremental increase in overall component security for that particular FR based on knowledge and expertise from the team creating this document.

The SL-C(component), used throughout this document, signifies a capability required to meet a given SL rating for a given CR. A complete description of the SL vector concept can be found in ISA-62443-3-3 [11].

4 Common Component Security Constraints

4.1 Overview

When reading, specifying and implementing the component CRs detailed in Clauses 5 through 15 of this document, there are a number of common constraints that shall be adhered to. This section documents those common constraints that are to be applied during the implementation of the requirements described in this document.

4.2 CCSC 1 Support of essential functions

The components of the system shall adhere to specific constraints as described in clause 4 of ISA-62443-3-3 [11].

4.3 CCSC 2 Compensating countermeasures

There will be cases where one or more requirements specified in the document cannot be met without the assistance of a compensating countermeasure that is external to the component. When this is the case the documentation for that component shall describe the appropriate countermeasures applied by the system to allow the requirement to be met when the component is integrated into a system.

4.4 CCSC 3 Least privilege

When required and appropriate, one or more system components (software applications, embedded devices, host devices and network devices) shall provide the capability for the system to enforce the concept of least privilege. Individual system components shall provide the granularity of permissions and flexibility of mapping those permissions to roles sufficient to support it. Individual accountability shall be available when required.

NOTE: Granularity of permissions and assignment is dependent on the type of device and the product documentation for the device should define this in the product documentation.

4.5 CCSC 4 Software development process

All of the components defined in this document shall be developed and supported following the secure product development processes described in ISA-62443-4-1 [12].

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), prior to allowing them access to the system or assets.

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

5.2 Rationale

Identification of users is used in conjunction with authorization mechanisms to implement access control for a component. Verifying the identity of users requesting access is necessary to protect against unauthorized users from gaining access to the component. Recommendations and guidelines should include mechanisms that will operate in mixed modes. For example, some components on a communication channel require strong access control, such as strong authentication mechanisms, and others do not. By extension, access control requirements need to be extended to data at rest.

It is recommended that the number of identification and authentication mechanisms within a single zone is minimized. The use of multiple identification and authentication mechanisms makes the task of authentication and identification management more difficult to administer.

5.3 CR 1.1 – Human user identification and authentication

5.3.1 Requirement

Components shall provide the capability to identify and authenticate all human users according to ISA-62443-3-3 [11] SR 1.1 on all interfaces capable of human user access. This capability shall enforce such identification and authentication on all interfaces that provide human user access to the component to support segregation of duties and least privilege in accordance with applicable security policies and procedures. This capability may be provided locally by the component or by integration into a system level identification and authentication system.

Note: Applicable security policies are a local matter.

5.3.2 Rationale and supplemental guidance

All human users need to be identified and authenticated for all access to the component. Authentication of the identity of these users should be accomplished by using methods such as passwords, tokens, biometrics or physically keyed lids etc., and 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 component. This requirement comes in addition to the requirement of having such an authentication and identification at the system level.

Interfaces capable of human user access are local user interfaces such as touchscreens, push buttons, keyboards, etc. as well as network protocols designed for human user interactions such as hypertext transfer protocol (HTTP), HTTP secure (HTTPS), file transfer protocol (FTP), secure FTP (SFTP), protocols used for device configuration tools (which are sometimes proprietary and other times use open protocols). User identification and authentication may be role-based or group-based (such as, for some component interfaces, several users may share the same identity). User identification and authentication should not hamper fast, local emergency actions.

In order to support IAC policies, as defined according to ISA-62443-2-1 [5], the component should verify the identity of all human users as a first step. In a second step, the permissions assigned to the identified human user should be enforced (see 6.3).

5.3.3 Requirement enhancements

(1) Unique identification and authentication:

Components shall provide the capability to uniquely identify and authenticate all human users.

(2) Multifactor authentication for all interfaces

Components shall provide the capability to employ multifactor authentication for all human user access to the component.

5.3.4 Security levels

The requirements for the four security levels that relate to CR 1.1 are:

- SL-C(IAC,component) 1: CR 1.1
- SL-C(IAC,component) 2: CR 1.1 (1)
- SL-C(IAC,component) 3: CR 1.1 (1) (2)
- SL-C(IAC,component) 4: CR 1.1 (1) (2)

5.4 CR 1.2 – Software process and device identification and authentication

5.4.1 Requirement

Components shall provide the capability to identify itself and authenticate to any other component (software application, embedded devices, host devices and network devices), according to ISA-62443-3-3 [11] SR1.2.

If the component, as in the case of an application, is running in the context of a human user, in addition, the identification and authentication of the human user according to ISA-62443-3-3 [11] SR1.1 may be part of the component identification and authentication process towards the other components.

5.4.2 Rationale and supplemental guidance

The function of identification and authentication is to map a known identity to an unknown software process or device (henceforth referred to as an entity in 5.4.2) so as to make it known before

allowing any data exchange. Allowing rogue entities to send and receive control system specific data can result in detrimental behavior of the control system.

All entities should be identified and authenticated for all access to the control system. Authentication of the identity of such entities should be accomplished by using methods such as passwords, tokens or location (physical or logical). This requirement should be applied to both local and remote access to the control system. However, in some scenarios where individual entities are used to connect to different target systems (for example, remote vendor support), it may be technically infeasible for an entity to have multiple identities. In these cases, compensating countermeasures would have to be applied.

Special attention needs to be made when identifying and authenticating portable and mobile devices. These types of devices are a known method of introducing undesired network traffic, malware and/or information exposure to control systems, including otherwise isolated networks.

Where entities function as a single group, identification and authentication may be role-based, group-based or entity-based. 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). For example, in common protection and control schemes, a group of devices jointly execute the protection functions and communicate with multicast messages among the devices in the group. In these cases, group authentication based on shared accounts or shared symmetric keys are commonly used.

In order to support identification and authentication control policies as defined according to ISA-62443-2-1 [5], the control system verifies the identity of all entities as a first step. In a second step, the permissions assigned to the identified entity are enforced (see 6.3, CR 2.1 – Authorization enforcement).

5.4.3 Requirement enhancements

(1) Unique identification and authentication

Components shall provide the capability to uniquely identify and authenticate itself to any other component.

5.4.4 Security levels

The requirements for the four security levels that relate to CR 1.2 are:

- SL-C(IAC,component) 1: Not Selected
- SL-C(IAC,component) 2: CR 1.2
- SL-C(IAC,component) 3: CR 1.2 (1)
- SL-C(IAC,component) 4: CR 1.2 (1)

5.5 CR 1.3 – Account management

5.5.1 Requirement

Components shall provide the capability to support the management of all accounts directly or integrated into a system that manages accounts according to ISA-62443-3-3 [11] SR 1.3.

5.5.2 Rationale and supplemental guidance

A component may provide this capability by integrating into a higher level account management system. If the capability is not integrated into a higher level account management system then the component is expected to provide the capability natively.

A common approach meeting this requirement would be a component that delegates the valuation of authentication to a directory server (for example, LDAP or Active Directory) which provides the account management capabilities required by ISA-62443-3-3 [11] SR 1.3.

When a component integrates into a higher level system to provide the account management capabilities there needs to be consideration for the impact to the component in the event that the higher level system capability becomes unavailable.

5.5.3 Requirement enhancements

None

5.5.4 Security levels

The requirements for the four security levels that relate to CR 1.3 are:

- SL-C(IAC,component) 1: CR 1.3
- SL-C(IAC,component) 2: CR 1.3
- SL-C(IAC,component) 3: CR 1.3
- SL-C(IAC,component) 4: CR 1.3

5.6 CR 1.4 – Identifier management

5.6.1 Requirement

Components shall provide the capability to integrate into a system that supports the management of identifiers and/or provide the capability to support the management of identifiers directly according to ISA-62443-3-3 [11] SR 1.4.

5.6.2 Rationale and supplemental guidance

Accounts created under CR 1.3 – Account management require the use of one or more identifiers to distinctly identify each account. These identifiers must be unique and unambiguous as to the account with which they are associated. Some examples of identifiers in common use are account names, UNIX user ids, Microsoft Windows account globally unique identifiers (GUID), and bound X.509 certificates. A component may provide a local capability to associate identifiers with accounts. If the component is integrated into a system that enforces a system-wide security policy it is highly recommended that identifiers be associated with the same account across all components in the system. In order to accomplish this a component must be able to integrate into a system-wide identifier management capability.

5.6.3 Requirement enhancements

None

5.6.4 Security levels

The requirements for the four security levels that relate to CR 1.4 are:

- SL-C(IAC,component) 1: CR 1.4
- SL-C(IAC,component) 2: CR 1.4
- SL-C(IAC,component) 3: CR 1.4
- SL-C(IAC,component) 4: CR 1.4

5.7 CR 1.5 – Authenticator management

5.7.1 Requirement

Components shall provide the capability to: