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 August 13, 2018
Second Printing August 28, 2019

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

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-62443-4-2-2018.

This second printing contains a corrigendum, as follows:

3.3 Conventions

Replace, in the first sentence of the last paragraph

The SL-C(component), used throughout this document, signifies a capability required to meet a given SL rating for a given CR.

by

The SL-C(component), used throughout this document, signifies a capability required to meet a given SL rating for a given FR.

The editorial correction has been incorporated into the text.

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. McAvinew	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	Fieldcomm Group Inc. Asia-Pacific
H. Storey	Herman Storey Consulting
K. Unger	Advanced Operational Excellence Co.
I. Verhappen	Industrial Automation Networks
D. Visnich	Burns & McDonnell
I. Weber	Siemens AG DF FA
W. Weidman	Consultant
J. Weiss	Applied Control Solutions LLC
D. Zetterberg	Chevron Energy Technology Co.

CONTENTS

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-62443-2-1[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 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.

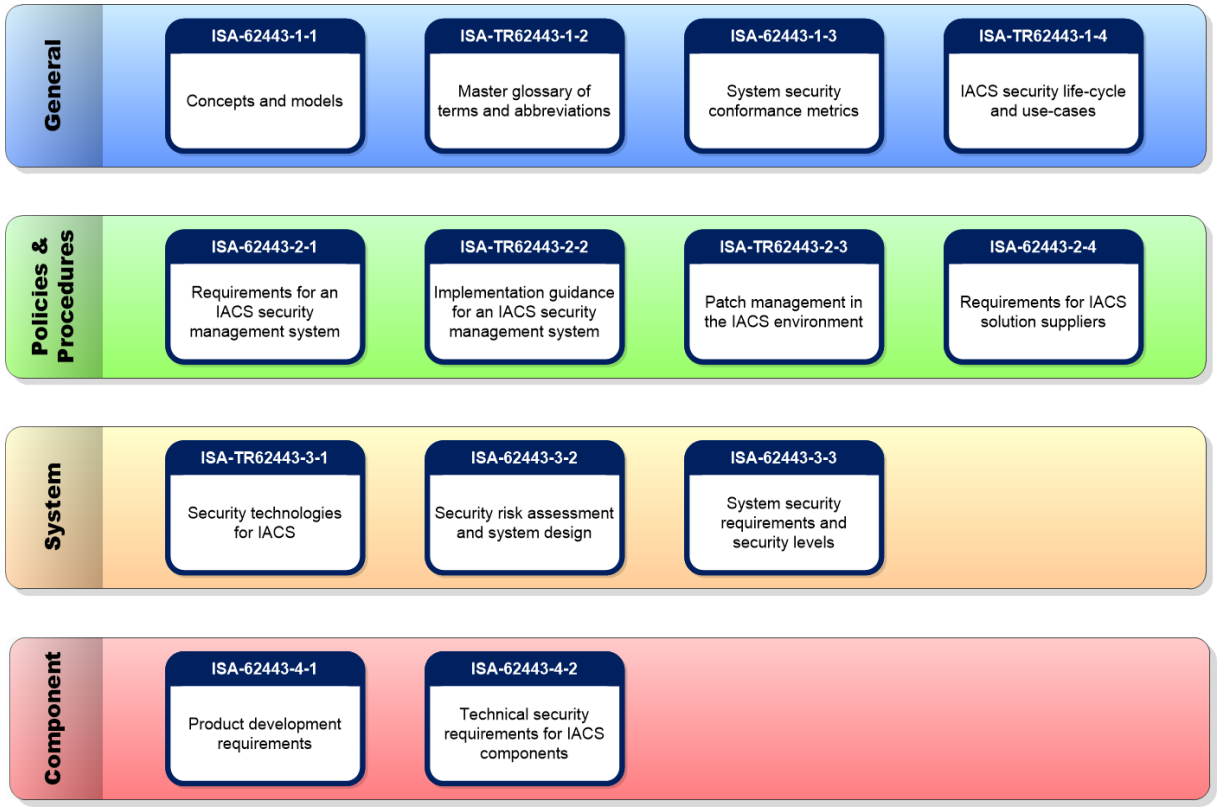

Figure 1 – ISA-62443 Work Products

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 FR. 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:

a) support the use of initial authenticator content;

b) support the recognition of changes to default authenticators made at installation time;

c) function properly with periodic authenticator change/refresh operation; and

d) protect authenticators from unauthorized disclosure and modification when stored, used and transmitted.

5.7.2 Rationale and supplemental guidance

In addition to an identifier (see 5.6) an authenticator is required to prove identity. Control system authenticators include, but are not limited to, tokens, symmetric keys, private keys (part of a public/private key pair), biometrics, passwords, physical keys and key cards. There should be security policies in place instructing that human users must take reasonable measures to safeguard authenticators, including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others and reporting lost or compromised authenticators immediately.

Authenticators have a lifecycle. When an account is created automatically a new authenticator needs to be created, in order for the account owner to be able to authenticate. For example, in a password-based system, the account has a password associated with it. Definition of the initial authenticator content could be interpreted as the administrator defining the initial password that the account management system sets for all new accounts. Being able to configure these initial values makes it harder for an attacker to guess the password between account creation and first account use (which should involve the setting of a new password by the account owner). Some control systems are installed with unattended installers that create all necessary accounts with default passwords and some embedded devices are shipped with default passwords. Over time, these passwords often become general knowledge and are documented on the Internet. Being able to change the default passwords protects the system against unauthorized users using default passwords to gain access. Passwords can be obtained from storage or from transmission when used in network authentication. The complexity of this can be increased by cryptographic protections such as encryption or hashing or by handshake protocols that do not require transmission of the password at all. Still, passwords might be subject to attacks, for example, brute force guessing or breaking the cryptographic protection of passwords in transit or storage. The window of opportunity can be reduced by changing/refreshing the passwords periodically. Similar considerations apply to authentication systems based on cryptographic keys. Enhanced protection can be achieved by using hardware mechanisms such as hardware security modules like trusted platform modules (TPMs).

The management of authenticators should be specified in applicable security policies and procedures, for example, constraints to change default authenticators, refresh periods, specification of the protection of authenticators or firecall procedures.

Besides the capabilities for authenticator management specified in this requirement, the strength of the authentication mechanism depends on the strength of the chosen authenticator (for example, password complexity or key length in public key authentication) and the policies for validating the authenticator in the authentication process (for example, how long a password is valid or which checks are performed in public key certificate validation). For the most common authentication mechanisms, password-based and public key authentication, 5.9, 5.10 and 5.11 provide further requirements.

Use of components for some operations may be restricted, requiring additional authentication (such as, tokens, keys and certificates) in order to perform some functions.

5.7.3 Requirement enhancements

(1) Hardware security for authenticators

The authenticators on which the component rely shall be protected via hardware mechanisms.

Note: Examples of hardware authentication include: Password protected memory, OTP memory, hardware data integrity checks, and device security boot mechanism.

5.7.4 Security levels

The requirements for the four security levels that relate to CR 1.5 are:

- SL-C(IAC,component) 1: CR 1.5
- SL-C(IAC,component) 2: CR 1.5
- SL-C(IAC,component) 3: CR 1.5 (1)
- SL-C(IAC,component) 4: CR 1.5 (1)

5.8 CR 1.6 – Wireless access management

The wireless access management requirements are network-component-specific and can be located as requirements for network-components in Clause 15.

5.9 CR 1.7 – Strength of password-based authentication

5.9.1 Requirement

For components that utilize password-based authentication, those components shall provide or integrate into a system that provides the capability to enforce configurable password strength according to internationally recognized and proven password guidelines.

5.9.2 Rationale and supplemental guidance

The ability to enforce configurable password strength, whether it is based on minimum length, variety of characters, or duration of time (the minimum being a one-time password) is necessary to assist in increasing the overall security of user chosen passwords. Generally accepted practices and recommendations can be found in documents such as NIST SP800-63-2, *Electronic Authentication Guideline* NIST SP800-63-2, *Electronic Authentication Guideline* [27].

5.9.3 Requirement enhancements

(1) Password generation and lifetime restrictions for human users

Components shall provide, or integrate into a system that provides, the capability to protect against any given human user account from reusing a password for a configurable number of generations. In addition, the component shall provide the capability to enforce password minimum and maximum lifetime restrictions for human users. These capabilities shall conform to commonly accepted security industry practices.

NOTE The component should provide the capability to prompt the user to change their password upon a configurable time prior to expiration.

(2) Password lifetime restrictions for all users (human, software process, or device)

Components shall provide, or integrate into a system that provides, the capability to enforce password minimum and maximum lifetime restrictions for all users.

5.9.4 Security levels

The requirements for the four security levels that relate to CR 1.7 are:

- SL-C(IAC,component) 1: CR 1.7
- SL-C(IAC,component) 2: CR 1.7
- SL-C(IAC,component) 3: CR 1.7 (1)
- SL-C(IAC,component) 4: CR 1.7 (1) (2)

5.10 CR 1.8 – Public key infrastructure certificates

5.10.1 Requirement

When public key infrastructure (PKI) is utilized, the component shall provide or integrate into a system that provides the capability to interact and operate in accordance with ISA-62443-3-3 [11] SR1.8.

5.10.2 Rationale and supplemental guidance

The selection of an appropriate PKI should consider the organization's certificate policy which should be based on the risk associated with a breach of confidentiality of the protected information. Guidance on the policy definition can be found in commonly accepted standards and guidelines, such as the Internet Engineering Task Force (IETF) Request for Comment (RFC) 3647 [31] for X.509-based PKI. For example, the appropriate location of a certification authority (CA), whether within the control system versus on the Internet, and the list of trusted CAs should be considered in the policy and depends on the network architecture (see also ISA-62443-2-1 [5]).

5.10.3 Requirement enhancements

None

5.10.4 Security levels

The requirements for the four security levels that relate to CR 1.8 are:

- SL-C(IAC,component) 1: Not selected
- SL-C(IAC,component) 2: CR 1.8
- SL-C(IAC,component) 3: CR 1.8
- SL-C(IAC,component) 4: CR 1.8

5.11 CR 1.9 – Strength of public key-based authentication

5.11.1 Requirement

For components that utilize public-key-based authentication, those components shall provide directly or integrate into a system that provides the capability within the same IACS environment to:

a) validate certificates by checking the validity of the signature of a given certificate;

b) validate the certificate chain or, in the case of self-signed certificates, by deploying leaf certificates to all hosts that communicate with the subject to which the certificate is issued;

c) validate certificates by checking a given certificate's revocation status;

d) establish user (human, software process or device) control of the corresponding private key;

e) map the authenticated identity to a user (human, software process or device); and

f) ensure that the algorithms and keys used for the public key authentication comply with 8.5 CR 4.3 – Use of cryptography.

5.11.2 Rationale and supplemental guidance

To meet the requirements in 5.11.1 does not necessarily require a real time connection to a certificate authority. Alternative out-of-band methods may be used to meet the requirements in 5.11.1. For example, a disconnected system could install and update certifications using manual out-of-band processes.

Public/private key cryptography strongly depends on the secrecy of a given subject's private key and proper handling of the trust relationships. When verifying a trust between two entities based on public key authentication, it is essential to trace the public key certificate to a trusted entity. A

common implementation error in certificate validation is to only check the validity of a certificate's signature, but not checking the trust in the signer. In a PKI setting, a signer is trusted if they are a trusted CA or have a certificate issued by a trusted CA, thus all verifiers need to trace certificates presented to them back to a trusted CA. If such a chain of trusted CAs cannot be established, the presented certificate should not be trusted.

If self-signed certificates are used instead of a PKI, the certificate subject itself signed its certificate, thus there never is a trusted third-party or CA. This should be compensated by deploying the self-signed public key certificates to all peers that need to validate them via an otherwise secured mechanism (for example, configuration of all peers in a trusted environment). Trusted certificates need to be distributed to peers through secure channels. During the validation process, a self-signed certificate should only be trusted if it is already present in the list of trusted certificates of the validating peer. The set of trusted certificates should be configured to the minimum necessary set.

In both cases, validation needs to also consider the possibility that a certificate is revoked. In a PKI setting this is typically done by maintaining certificate revocation lists (CRLs) or running an online certificate status protocol (OCSP) server. When revocation checking is not available due to control system constraints, mechanisms such as a short certificate lifetime can compensate for the lack of timely revocation information. Note that short lifetime certificates can sometimes create significant operational issues in a control system environment.

It is expected that most components will integrate into an IACS and leverage the key authentication mechanisms provided by the underlying IACS. When implementing public key authentication at the component-level of an IACS, protection of the key becomes a primary concern and objective of key storage on that component. Care should be taken in the implementation to assure that any private keys stored within the component cannot be retrieved or tampered with (See 5.7, CR 1.5 – Authenticator management).

NOTE Tamper resistant design methodologies and technologies are available to assist with designing a secure private key protection mechanism.

5.11.3 Requirement enhancements

(1) Hardware security for public key-based authentication

Components shall provide the capability to protect critical, long-lived private keys via hardware mechanisms.

5.11.4 Security levels

The requirements for the four security levels that relate to CR 1.9 are:

- SL-C(IAC,component) 1: Not selected
- SL-C(IAC,component) 2: CR 1.9
- SL-C(IAC,component) 3: CR 1.9 (1)
- SL-C(IAC,component) 4: CR 1.9 (1):

5.12 CR 1.10 – Authenticator feedback

5.12.1 Requirement

When a component provides an authentication capability the component shall provide the capability to obscure feedback of authenticator information during the authentication process.

5.12.2 Rationale and supplemental guidance

Obscuring feedback protects the information from possible exploitation by unauthorized individuals, for example, displaying asterisks or other random characters when a human user types in a username and/or password obscures feedback of authentication information. Other examples

include the entry of secure socket shell (SSH) token entry and one-time passwords. The authenticating entity should not provide any hint as to the reason for the authentication failure, such as “unknown user name.”

5.12.3 Requirement enhancements

None

5.12.4 Security levels

The requirements for the four SL levels that relate to CR 1.10 are:

- SL-C(IAC,component) 1: CR 1.10
- SL-C(IAC,component) 2: CR 1.10
- SL-C(IAC,component) 3: CR 1.10
- SL-C(IAC,component) 4: CR 1.10

5.13 CR 1.11 – Unsuccessful login attempts

5.13.1 Requirement

When a component provides an authentication capability the component shall provide the capability to:

a) enforce a limit of a configurable number of consecutive invalid access attempts by any user (human, software process or device) during a configurable time period; and

b) deny access for a specified period of time or until unlocked by an administrator when this limit has been reached.

Note: An administrator may unlock an account prior to the expiration of the timeout period.

5.13.2 Rationale and supplemental guidance

Due to the potential for denial of service, the number of consecutive invalid access attempts may be limited. If enabled, the application or device may automatically reset to zero the number of access attempts after a predetermined time period established by the applicable security policies and procedures. Resetting the access attempts to zero will allow users (human, software process or device) to gain access if they have the correct login credentials. Automatic denial of access for control system operator workstations or nodes should not be used when immediate operator responses are required in emergency situations. All lockout mechanisms should consider functional requirements for continuous operations so as to mitigate adverse denial of service operating conditions which could result in system failures or compromising the safety of the system. Allowing interactive logins to an account used for critical services could provide a potential for denial of service or other abuse.

5.13.3 Requirement enhancements

None

5.13.4 Security levels

The requirements for the four SL levels that relate to CR 1.11 are:

- SL-C(IAC,component) 1: CR 1.11
- SL-C(IAC,component) 2: CR 1.11
- SL-C(IAC,component) 3: CR 1.11
- SL-C(IAC,component) 4: CR 1.11

5.14 CR 1.12 – System use notification

5.14.1 Requirement

When a component provides local human user access/HMI, it shall provide the capability to display a system use notification message before authenticating. The system use notification message shall be configurable by authorized personnel.

5.14.2 Rationale and supplemental guidance

Privacy and security policies and procedures need to be consistent with applicable laws, directives, policies, regulations, standards and guidance. Often, the main justification for this requirement is legal prosecution of violators and proving intentional breach. This capability is thus necessary to support policy requirements, and might improve IACS security because it can be used as a deterrent. System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the control system. A warning banner implemented as a posted physical notice in the control system facility does not protect against remote login issues.

Examples of elements for inclusion in the system use notification message are:

a) that the individual is accessing a system owned by the asset owner;

b) that system usage may be monitored, recorded and subject to audit;

c) that unauthorized use of the system is prohibited and subject to criminal and/or civil penalties; and

d) that use of the system indicates consent to monitoring and recording.

5.14.3 Requirement enhancements

None

5.14.4 Security levels

The requirements for the four SL levels that relate to CR 1.12 are:

- SL-C(IAC,component) 1: CR 1.12
- SL-C(IAC,component) 2: CR 1.12
- SL-C(IAC,component) 3: CR 1.12
- SL-C(IAC,component) 4: CR 1.12

5.15 CR 1.13 – Access via untrusted networks

The access via untrusted networks requirements are component-specific and can be located as requirements for each specific component type in Clauses 12 through 15.

5.16 CR 1.14 – Strength of symmetric key-based authentication

5.16.1 Requirement

For components that utilize symmetric keys, the component shall provide the capability to:

a) establish the mutual trust using the symmetric key;

b) store securely the shared secret (the authentication is valid as long as the shared secret remains secret);

c) restrict access to the shared secret; and

d) ensure that the algorithms and keys used for the symmetric key authentication comply with CR 4.3 – Use of cryptography Subclause 8.5.

5.16.2 Rationale and supplemental guidance

Means should be defined for installing the keys into the component. This may include installing and managing the component key using out-of-band methods. This is necessary since a compromise of any symmetric keys that are stored within the component could lead to a full compromise of the system using those keys.

In practice, there are two basic ways to perform the secure authentication of a device to another: either using asymmetric cryptography (see 5.11) or by using symmetric cryptography. The choice between asymmetric and symmetric is dictated by several criteria, like key management, trust provisioning, legacy support and efficiency. Examples of symmetric key authentication schemes are Needham-Schröder or Kerberos. When symmetric key authentication is used, the party uses a secret key they have learned in the past (for example, through trust provisioning). The party proves their claimed identity by proving knowledge of the secret key (for example, by answering a challenge submitted by the other party, the examiner). The examiner has the knowledge of the same secret (also learned in the past through trust provisioning) and is able to compute the answer to the challenge performing the same cryptographic operations as the prover. The examiner can then compare the answer of the prover with its own computation. If they match, the examiner is convinced that the prover is the one they claim to be and the process can be conducted the other way around, switching roles, to achieve mutual-authentication. This mechanism is secure only if the shared secret is only known by the prover and the examiner and if the secret is diversified per prover. One instance of such a mechanism is the proper use of cipher-based message authentication code (CMAC) computations or alternatively the Galois counter mode (GCM)/Galois message authentication code (GMAC) operation modes.

5.16.3 Requirement enhancements

(1) Hardware security for symmetric key-based authentication

Components shall provide the capability to protect critical, long lived symmetric keys via hardware mechanisms.

5.16.4 Security levels

The requirements for the four SL levels that relate to CR 1.14 are:

- SL-C(IAC,control system) 1: Not selected
- SL-C(IAC,control system) 2: CR 1.14
- SL-C(IAC,control system) 3: CR 1.14 (1)
- SL-C(IAC,control system) 4: CR 1.14 (1)

6 FR 2 – Use control

6.1 Purpose and SL-C(UC) descriptions

Enforce the assigned privileges of an authenticated user (human, software process or device) to perform the requested action on the component and monitor the use of these privileges.

- SL 1 – Restrict use of the IACS according to specified privileges to protect against casual or coincidental misuse.
- SL 2 – Restrict use of the IACS according to specified privileges to protect against circumvention by entities using simple means with low resources, generic skills and low motivation.
- SL 3 – Restrict use of the IACS according to specified privileges to protect against circumvention by entities using sophisticated means with moderate resources, IACS specific skills and moderate motivation.

- SL 4 – Restrict use of the IACS according to specified privileges to protect against circumvention by entities using sophisticated means with extended resources, IACS specific skills and high motivation.

6.2 Rationale

Once the user is identified and authenticated, the component must restrict the allowed actions to the authorized use of the component. Asset owners and system integrators will have to assign, to each user (human, software process or device), group, role, etc. (see 4.5), the privileges defining the authorized use of the component. The goal of use control is to protect against unauthorized actions on the component's resources by verifying that the necessary privileges have been granted before allowing a user to perform the actions. Examples of actions are reading or writing data, downloading programs and setting configurations. Recommendations and guidelines should include mechanisms that will operate in mixed modes. For example, some component resources require strong use control protection, such as restrictive privileges, and others do not. By extension, use control requirements must be extended to data at rest. User privileges may vary based on time-of-day/date, location and means by which access is made.

6.3 CR 2.1 – Authorization enforcement

6.3.1 Requirement

Components shall provide an authorization enforcement mechanism for all identified and authenticated users based on their assigned responsibilities.

6.3.2 Rationale and supplemental guidance

Use control policies (for example, identity-based policies, role-based policies and rule-based policies) and associated read/write access enforcement mechanisms (for example, access control lists, access control matrices and cryptography) are employed to control usage between users (humans, software processes and devices) and assets (for example, devices, files, records, software processes, programs and domains).

After the control system has verified the identity of a user (human, software process or device) (see 5.3, CR 1.1 – Human user identification and authentication and 5.4, CR 1.2 – Software process and device identification and authentication), it also has to verify that a requested operation is actually permitted according to the defined security policies and procedures. For example, in a role-based access control policy, the control system would check which roles are assigned to a verified user or asset and which privileges are assigned to these roles – if the requested operation is covered by the permissions, it is executed, otherwise rejected. This allows the enforcement of segregation of duties and least privileges. Usage enforcement mechanisms should not be allowed to adversely affect the operational performance of the control system.

Planned or unplanned changes to control system components can have significant effects on the overall security of the control system. Accordingly, only qualified and authorized individuals should obtain the use of control system components for purposes of initiating changes, including upgrades and modifications.

6.3.3 Requirement enhancements

(1) Authorization enforcement for all users (humans, software processes and devices)

Components shall provide an authorization enforcement mechanism for all users based on their assigned responsibilities and least privilege.

(2) Permission mapping to roles

Components shall, directly or through a compensating security mechanism, provide for an authorized role to define and modify the mapping of permissions to roles for all human users.

NOTE 1 Roles should not be limited to fixed nested hierarchies in which a higher level role is a super set of a lesser privileged role. For example, a system administrator should not necessarily encompass operator privileges.

NOTE 2 This RE should be applicable to software processes and devices as well.

(3) Supervisor override

Components shall support a supervisor manual override for a configurable time or sequence of events.

NOTE Implementation of a controlled, audited and manual override of automated mechanisms in the event of emergencies or other serious events is often needed. This allows a supervisor to enable an operator to quickly react to unusual conditions without closing the current session and establishing a new session as a higher privilege human user.

(4) Dual approval

Components shall support dual approval when action can result in serious impact on the industrial process.

NOTE Dual approval should be limited to actions which require a very high level of confidence that they will be performed reliably and correctly. Requiring dual approval provides emphasis to the seriousness of consequences that would result from failure of a correct action. An example of a situation in which dual approval is required would be a change to a set point of a critical industrial process. Dual approval mechanisms should not be employed when an immediate response is necessary to safeguard HSE consequences, for example, emergency shutdown of an industrial process.

6.3.4 Security levels

The requirements for the four security levels that relate to CR 2.1 are:

- SL-C(UC,component) 1: CR 2.1
- SL-C(UC,component) 2: CR 2.1 (1) (2)
- SL-C(UC,component) 3: CR 2.1 (1) (2) (3)
- SL-C(UC,component) 4: CR 2.1 (1) (2) (3) (4)

6.4 CR 2.2 – Wireless use control

6.4.1 Requirement

If a component supports usage through wireless interfaces it shall provide the capability to integrate into the system that supports usage authorization, monitoring and restrictions according to commonly accepted industry practices.

6.4.2 Rationale and supplemental guidance

Wireless use control may be implemented in different devices that make up the system. Network devices may be one of the devices that assist with use control through controls such as network admission control. For devices and applications that utilize wireless networks those devices should be able to properly utilize wireless network protection such as network admission control. Components may also implement different limitations on access based on whether the access is from wireless devices or wired devices. This does place a need that the component be able to distinguish whether the interface is through wireless or not. Some network devices provide the capability to scan for unauthorized wireless network activity in the wireless spectrum. In order to prevent a negative impact on the performance of the control system functionality, it is a good practice to deploy dedicated devices to perform checks for unauthorized network activity.

6.4.3 Requirement enhancements

None

6.4.4 Security levels

The requirements for the four SL levels that relate to CR 2.2 are:

- SL-C(UC, component) 1: CR 2.2
- SL-C(UC, component) 2: CR 2.2

- SL-C(UC, component) 3: CR 2.2
- SL-C(UC, component) 4: CR 2.2

6.5 CR 2.3 – Use control for portable and mobile devices

There is no component level requirement associated with ISA-62443-3-3 SR 2.3.

6.6 CR 2.4 – Mobile code

The use control requirements for mobile code are component-specific and can be located as requirements for each specific component type in Clauses 12 through 15.

6.7 CR 2.5 – Session lock

6.7.1 Requirement

If a component provides a human user interface, whether accessed locally or via a network, the component shall provide the capability

a) to protect against further access by initiating a session lock after a configurable time period of inactivity or by manual initiation by the user (human, software process or device); and

b) for the session lock to remain in effect until the human user who owns the session, or another authorized human user, re-establishes access using appropriate identification and authentication procedures.

6.7.2 Rationale and supplemental guidance

Session locks are used to prevent access to specified workstations or nodes. Components should activate session lock mechanisms automatically after a configurable time period. In most cases, the session locks are configured at the system level. Session locks implemented as part of this requirement may be pre-empted or limited by remote session termination, as defined in CR 2.6 – Remote session termination.

6.7.3 Requirement enhancements

None

6.7.4 Security levels

The requirements for the four SL levels that relate to CR 2.5 are:

- SL-C(UC, component) 1: CR 2.5
- SL-C(UC, component) 2: CR 2.5
- SL-C(UC, component) 3: CR 2.5
- SL-C(UC, component) 4: CR 2.5

6.8 CR 2.6 – Remote session termination

6.8.1 Requirement

If a component supports remote sessions, the component shall provide the capability to terminate a remote session either automatically after a configurable time period of inactivity, manually by a local authority, or manually by the user (human, software process or device) who initiated the session.

6.8.2 Rationale and supplemental guidance

A remote session is initiated whenever a component is accessed across the boundary of a zone defined by the asset owner based on their risk assessment. This requirement may be limited to sessions that are used for component monitoring and maintenance activities (not critical operations) based on the risk assessment of the control system and security policies and

procedures. Some components may not allow sessions to be terminated as the session might be part of an essential function of the component.

6.8.3 Requirement enhancements

None

6.8.4 Security levels

The requirements for the four SL levels that relate to CR 2.6 are:

- SL-C(UC, component) 1: Not Selected
- SL-C(UC, component) 2: CR 2.6
- SL-C(UC, component) 3: CR 2.6
- SL-C(UC, component) 4: CR 2.6

6.9 CR 2.7 – Concurrent session control

6.9.1 Requirement

Components shall provide the capability to limit the number of concurrent sessions per interface for any given user (human, software process or device).

6.9.2 Rationale and supplemental guidance

A resource starvation DoS might occur if a limit is not imposed. There is a trade-off between potentially locking out a specific user versus locking out all users and services due to a lack of resources. Product supplier and/or system integrator guidance is likely required to provide sufficient information as to how the number of concurrent sessions value should be assigned.

6.9.3 Requirement enhancements

None

6.9.4 Security levels

The requirements for the four SL levels that relate to CR 2.7 are:

- SL-C(UC, component) 1: Not Selected
- SL-C(UC, component) 2: Not Selected
- SL-C(UC, component) 3: CR 2.7
- SL-C(UC, component) 4: CR 2.7

6.10 CR 2.8 – Auditable events

6.10.1 Requirement

Components shall provide the capability to generate audit records relevant to security for the following categories:

a) access control;

b) request errors;

c) control system events;

d) backup and restore event;

e) configuration changes; and

f) audit log events.

Individual audit records shall include:

a) timestamp;

b) source (originating device, software process or human user account);

c) category;

d) type;

e) event ID; and

f) event result.

6.10.2 Rationale and supplemental guidance

Devices may contain either embedded firmware or run an OS. While the intent of the requirement is to cover categories of events, at least all events from the above categories that can be generated by the firmware or OS are to be included.

NOTE Security event categories are only applicable if functionality itself is provided by the component.

6.10.3 Requirement enhancements

None

6.10.4 Security levels

The requirements for the four security levels that relate to CR 2.8 are:

- SL-C(UC,component) 1: CR 2.8
- SL-C(UC,component) 2: CR 2.8
- SL-C(UC,component) 3: CR 2.8
- SL-C(UC,component) 4: CR 2.8

6.11 CR 2.9 – Audit storage capacity

6.11.1 Requirement

Components shall

a) provide the capability to allocate audit record storage capacity according to commonly recognized recommendations for log management; and

b) provide mechanisms to protect against a failure of the component when it reaches or exceeds the audit storage capacity.

6.11.2 Rationale and supplemental guidance

Components should provide sufficient audit storage capacity, taking into account retention policy, the auditing to be performed and the online audit processing requirements. Components may rely on the system into which they are integrated to provide the majority of audit storage capacity. However, the components should provide enough local storage to buffer audit data until it can be sent to the system.

Guidelines to be considered may include NIST Special Publication (SP) 800-92 [26]. The audit storage capacity should be sufficient to retain logs for a period of time required by applicable policies and regulations or business requirements.

6.11.3 Requirement enhancements

(1) Warn when audit record storage capacity threshold reached

Components shall provide the capability to issue a warning when the allocated audit record storage reaches a configurable threshold.

6.11.4 Security levels

The requirements for the four SL levels that relate to CR 2.9 are:

- SL-C(UC,component) 1: CR 2.9
- SL-C(UC,component) 2: CR 2.9
- SL-C(UC,component) 3: CR 2.9 (1)
- SL-C(UC,component) 4: CR 2.9 (1)

6.12 CR 2.10 – Response to audit processing failures

6.12.1 Requirement

Components shall

a) provide the capability to protect against the loss of essential services and functions in the event of an audit processing failure; and

b) provide the capability to support appropriate actions in response to an audit processing failure according to commonly accepted industry practices and recommendations.

6.12.2 Rationale and supplemental guidance

Audit generation typically occurs at the source of the event. Audit processing involves transmission, possible augmentation (such as, the addition of a timestamp) and persistent storage of the audit records. Audit processing failures include, for example, software or hardware errors, failures in the audit capturing mechanisms and audit storage capacity being reached or exceeded. Guidelines to be considered when designing appropriate response actions may include the NIST SP 800-92, *Guide to Computer Security Log Management* [26]. It should be noted that either overwriting the oldest audit records or halting audit log generation are possible responses to audit storage capacity being exceeded but imply the loss of potentially essential forensic information. Also alerting personnel could be an appropriate supporting action in response to an audit processing failure.

6.12.3 Requirement enhancements

None

6.12.4 Security levels

The requirements for the four SL levels that relate to CR 2.10 are:

- SL-C(UC,component) 1: CR 2.10
- SL-C(UC,component) 2: CR 2.10
- SL-C(UC,component) 3: CR 2.10
- SL-C(UC,component) 4: CR 2.10

6.13 CR 2.11 – Timestamps

6.13.1 Requirement

Components shall provide the capability to create timestamps (including date and time) for use in audit records.

6.13.2 Rationale and supplemental guidance

A good reference for the format of timestamps is ISO 8601:2004, *Data elements and interchange formats – Information interchange – Representation of dates and times* [15]. Care should be taken when designing a system that periodic time-shift events, such as daylight savings time in some locations, are taken into account.

6.13.3 Requirement enhancements

(1) Time synchronization

Components shall provide the capability to create timestamps that are synchronized with a system wide time source.

(2) Protection of time source integrity

The time synchronization mechanism shall provide the capability to detect unauthorized alteration and cause an audit event upon alteration.

6.13.4 Security levels

The requirements for the four security levels that relate to CR 2.11 are:

- SL-C(UC,component) 1: CR 2.11
- SL-C(UC,component) 2: CR 2.11 (1)
- SL-C(UC,component) 3: CR 2.11 (1)
- SL-C(UC,component) 4: CR 2.11 (1) (2)

6.14 CR 2.12 – Non-repudiation

6.14.1 Requirement

If a component provides a human user interface, the component shall provide the capability to determine whether a given human user took a particular action.

Control elements that are not able to support such capability shall be listed in component documents.

6.14.2 Rationale and supplemental guidance

Examples of particular actions taken by a user include performing operator actions, changing control system configurations, creating information, sending a message, approving information (such as, indicating concurrence) and receiving a message. Non-repudiation protects against later false claims by a user of not having taken a specific action, by an author of not having authored a particular document, by a sender of not having transmitted a message, by a receiver of not having received a message or by a signatory of not having signed a document. Non-repudiation services can be used to determine if information originated from a user, if a user took specific actions (for example, sending an email and approving a work order) or received specific information. Non-repudiation services are obtained by employing various techniques or mechanisms (for example, user identification and authorization, digital signatures, digital message receipts and timestamps).

6.14.3 Requirement enhancements

(1) Non-repudiation for all users

Components shall provide the capability to determine whether a given user (human, software process or device) took a particular action.

6.14.4 Security levels

The requirements for the four SL levels that relate to CR 2.12 are:

- SL-C(UC,component) 1: CR 2.12
- SL-C(UC,component) 2: CR 2.12
- SL-C(UC,component) 3: CR 2.12
- SL-C(UC,component) 4: CR 2.12 (1)

6.15 CR 2.13 – Use of physical diagnostic and test interfaces

The use of physical diagnostic and test interfaces requirements are component-specific and can be located as requirements for each specific component type in Clauses 12 through 15.

7 FR 3 – System integrity

7.1 Purpose and SL-C(SI) descriptions

Ensure the integrity of the component to protect against unauthorized manipulation or modification.

- SL 1 – Protect the integrity of the IACS against casual or coincidental manipulation.
- SL 2 – Protect the integrity of the IACS against manipulation by someone using simple means with low resources, generic skills and low motivation.
- SL 3 – Protect the integrity of the IACS against manipulation by someone using sophisticated means with moderate resources, IACS specific skills and moderate motivation.
- SL 4 – Protect the integrity of the IACS against manipulation by someone using sophisticated means with extended resources, IACS specific skills and high motivation.

7.2 Rationale

Components often go through multiple testing cycles (unit testing, system testing, etc.) before they begin production to establish that the components will perform as intended before they even begin production. Once operational, asset owners are responsible for maintaining the integrity of the component. Using their risk assessment methodology, asset owners may assign different levels of integrity protection to different components, communication channels and information in their IACS. The integrity of physical assets should be maintained in both operational and non-operational states, such as during production, when in storage or during a maintenance shutdown. The integrity of logical assets should be maintained while in transit and at rest, such as being transmitted over a network or when residing in a data repository.

7.3 CR 3.1 – Communication integrity

7.3.1 Requirement

Components shall provide the capability to protect integrity of transmitted information.

7.3.2 Rationale and supplemental guidance

Many common network attacks are based on the manipulation of data in transmission, for example manipulation of network packets. Switched or routed networks provide a greater opportunity for attackers to manipulate packets as undetected access to these networks is generally easier and the switching and routing mechanisms themselves can also be manipulated in order to get more access to transmitted information. Manipulation in the context of a control system could include the change of measurement values communicated from a sensor to a receiver or the alteration of command parameters sent from a control application to an actuator.

Depending on the context (for example transmission within a local network segment versus transmission via untrusted networks) and the network type used in the transmission (for example transmission control protocol (TCP) / internet protocol (IP) versus local serial links), feasible and appropriate mechanisms will vary. On a small network with direct links (point-to-point), physical access protection to all nodes may be sufficient on lower SLs if the endpoints' integrity is protected as well (see 7.6, CR 3.4 – Software and information integrity), while on a network distributed in areas with regular physical presence of staff or on a wide area network physical access is likely not enforceable. If a commercial service is used to provide communication services as a commodity item rather than a fully dedicated service (for example a leased line versus a T1 link), it may be more difficult to obtain the necessary assurances regarding the implementation of needed security controls for communication integrity (for example because of legal restrictions). When it is

infeasible or impractical to meet the necessary security requirements it may be appropriate to implement either appropriate compensating countermeasures or explicitly accept the additional risk.

Industrial equipment is often subject to environmental conditions that can lead to integrity issues and/or false positive incidents. Many times the environment contains particulates, liquids, vibration, gases, radiation, and electromagnetic interference (EMI) that can cause conditions that affect the integrity of the communication wiring and signals. The network infrastructure should be designed to minimize these physical/environmental effects on communication integrity. For example, when particulate, liquids, and/or gases are an issue, it may be necessary to use a sealed registered jack 45 (RJ-45) or M12 connector instead of a commercial-grade RJ-45 connector on the wire. The cable itself may need to use a different jacket instead to handle the particulate, liquid, and/or gas as well. In cases where vibration is an issue, M12 connectors may be necessary to prevent the spring pins on an RJ-45 connector from disconnecting during use. In cases where radiation and/or EMI are an issue, it may be necessary to use shielded twisted pair or fiber cables to prevent any effect on the communication signals. It may also be necessary to perform a wireless spectrum analysis in these areas if wireless networking is planned to verify that it is a viable solution.

7.3.3 Requirement enhancements

(1) Communication authentication

Components shall provide the capability to verify the authenticity of received information during communication.

NOTE: Both Integrity protection and authentication of origin can be achieved without providing confidentiality protection.

7.3.4 Security levels

The requirements for the four SL levels that relate to CR 3.1 are:

- SL-C(SI, component) 1: CR 3.1
- SL-C(SI, component) 2: CR 3.1 (1)
- SL-C(SI, component) 3: CR 3.1 (1)
- SL-C(SI, component) 4: CR 3.1 (1)

7.4 CR 3.2 – Protection from malicious code

The protection from malicious code requirements are component-specific and can be located as requirements for each specific component type in Clauses 12 through 15.

7.5 CR 3.3 – Security functionality verification

7.5.1 Requirement

Components shall provide the capability to support verification of the intended operation of security functions according to ISA-62443-3-3 [11] SR3.3.

7.5.2 Rationale and supplemental guidance

The product supplier and/or system integrator should provide guidance on how to test the designed security controls. Asset owners need to be aware of the possible ramifications of running these verification tests during normal operations. Details of the execution of these verifications need to be specified with careful consideration of the requirements for continuous operations (for example, scheduling or prior notification).

Examples of security verification functions include:

- Verification of antivirus countermeasures by European Institute for Computer Antivirus Research (EICAR) testing of the control system file system. Antivirus software should

detect the EICAR test samples and appropriate incident handling procedures should be triggered.

- Verification of the identification, authentication and use control countermeasures by attempting access with an unauthorized account (for some functionality this could be automated).
- Verification of intrusion detection systems (IDSs) as a security control by including a rule in the IDS that triggers on irregular, but known non-malicious traffic. The test could then be performed by introducing traffic that triggers this rule and the appropriate IDS monitoring and incident handling procedures.
- Confirmation that audit logging is occurring as required by security policies and procedures and has not been disabled by an internal or external entity.

7.5.3 Requirement enhancements

(1) Security functionality verification during normal operation

Components shall provide the capability to support verification of the intended operation of security functions during normal operations.

NOTE This RE needs to be carefully implemented to avoid detrimental effects. It may not be suitable for safety systems.

7.5.4 Security levels

The requirements for the four SL levels that relate to CR 3.3 are:

- SL-C(SI, component) 1: CR 3.3
- SL-C(SI, component) 2: CR 3.3
- SL-C(SI, component) 3: CR 3.3
- SL-C(SI, component) 4: CR 3.3 (1)

7.6 CR 3.4 – Software and information integrity

7.6.1 Requirement

Components shall provide the capability to perform or support integrity checks on software, configuration and other information as well as the recording and reporting of the results of these checks or be integrated into a system that can perform or support integrity checks.

7.6.2 Rationale and supplemental guidance

Integrity verification methods are employed to detect, record, report and protect against software and information tampering that may occur if other protection mechanisms (such as authorization enforcement) have been circumvented. Components should employ formal or recommended integrity mechanisms (such as cryptographic hashes). For example, such mechanisms could be used to monitor field devices for their latest configuration information to detect security breaches (including unauthorized changes).

7.6.3 Requirement enhancements

(1) Authenticity of software and information

Components shall provide the capability to perform or support authenticity checks on software, configuration and other information as well as the recording and reporting of the results of these checks or be integrated into a system that can perform or support authenticity checks.

(2) Automated notification of integrity violations

If the component is performing the integrity check, it shall be capable of automatically providing notification to a configurable entity upon discovery of an attempt to make an unauthorized change.

7.6.4 Security levels

The requirements for the four SL levels that relate to CR 3.4 are:

- SL-C(SI, component) 1: CR 3.4
- SL-C(SI, component) 2: CR 3.4 (1)
- SL-C(SI, component) 3: CR 3.4 (1) (2)
- SL-C(SI, component) 4: CR 3.4 (1) (2)

7.7 CR 3.5 – Input validation

7.7.1 Requirement

Components shall validate the syntax, length and content of any input data that is used as an industrial process control input or input via external interfaces that directly impacts the action of the component.

7.7.2 Rationale and supplemental guidance

Rules for checking the valid syntax of input data such as set points should be in place to verify that this information has not been tampered with and is compliant with the specification. Inputs passed to interpreters should be pre-screened to prevent the content from being unintentionally interpreted as commands. Note that this is a security CR, thus it does not address human error, for example supplying a legitimate integer number which is outside the expected range.

Generally accepted industry practices for input data validation include out-of-range values for a defined field type, invalid characters in data fields, missing or incomplete data and buffer overflow. Additional examples where invalid inputs lead to system security issues include SQL injection attacks, cross-site scripting or malformed packets (as commonly generated by protocol fuzzers). Guidelines to be considered should include well-known guidelines such as the Open Web Application Security Project (OWASP) Code Review Guide [28].

7.7.3 Requirement enhancements

None

7.7.4 Security levels

The requirements for the four SL levels that relate to CR 3.5 are:

- SL-C(SI, component) 1: CR 3.5
- SL-C(SI, component) 2: CR 3.5
- SL-C(SI, component) 3: CR 3.5
- SL-C(SI, component) 4: CR 3.5

7.8 CR 3.6 – Deterministic output

7.8.1 Requirement

Components that physically or logically connect to an automation process shall provide the capability to set outputs to a predetermined state if normal operation as defined by the component supplier cannot be maintained.

7.8.2 Rationale and supplemental guidance

The deterministic behavior of control system outputs as a result of threat actions against the control system devices and software is an important characteristic to ensure the integrity of normal operations. Ideally, the device continues to operate normally while under attack, but if the control system cannot maintain normal operation, then the control system outputs need to fail to a

predetermined state. The appropriate predetermined state of control system outputs is device dependent and could be one of the following user configurable options:

- Unpowered – the outputs fail to the unpowered state;
- Hold – the outputs fail to the last-known good value; or
- Fixed – the outputs fail to a fixed value that is determined by the asset owner or an application; or
- Dynamic – the outputs fail to one of the above options based on the current state.

7.8.3 Requirement enhancements

None

7.8.4 Security levels

The requirements for the four SL levels that relate to CR 3.6 are:

- SL-C(SI, component) 1: CR 3.6
- SL-C(SI, component) 2: CR 3.6
- SL-C(SI, component) 3: CR 3.6
- SL-C(SI, component) 4: CR 3.6

7.9 CR 3.7 – Error handling

7.9.1 Requirement

Components shall identify and handle error conditions in a manner that does not provide information that could be exploited by adversaries to attack the IACS.

7.9.2 Rationale and supplemental guidance

The product supplier and/or system integrator should carefully consider the structure and content of error messages. Error messages generated by the component should provide timely and useful information without revealing potentially harmful information that could be used by adversaries to exploit the IACS. Disclosure of this information should be justified by the necessity for timely resolution of error conditions. Guidelines to be considered could include well-known guidelines such as the OWASP Code Review Guide.

NOTE: A good example of an error message that could help adversaries attack an IACS would be to provide details of why authentication with the system failed. For example stating invalid user or invalid password in the feedback would help an adversary attack the IACS and thus should not be provided.

7.9.3 Requirement enhancements

None

7.9.4 Security levels

The requirements for the four SL levels that relate to CR 3.7 are:

- SL-C(SI, component) 1: CR 3.7
- SL-C(SI, component) 2: CR 3.7
- SL-C(SI, component) 3: CR 3.7
- SL-C(SI, component) 4: CR 3.7

7.10 CR 3.8 – Session integrity

7.10.1 Requirement

Components shall provide mechanisms to protect the integrity of communications sessions including:

a) the capability to invalidate session identifiers upon user logout or other session termination (including browser sessions);

b) the capability to generate a unique session identifier for each session and recognize only session identifiers that are system-generated; and

c) the capability to generate unique session identifiers with commonly accepted sources of randomness.

7.10.2 Rationale and supplemental guidance

This control focuses on communications protection at the session, versus packet, level. The intent of this control is to establish grounds for confidence at each end of a communications session in the ongoing identity of the other party and in the validity of the information being transmitted. For example, this control addresses man-in-the-middle attacks including session hijacking, insertion of false information into a session or replay attacks. Use of session integrity mechanisms can have a significant overhead and therefore their use should be considered in light of requirements for real-time communications.

Session hijacking and other man-in-the-middle attacks or injections of false information often take advantage of easy-to-guess session IDs (keys or other shared secrets) or use of session IDs that were not properly invalidated after session termination. Therefore the validity of a session authenticator should be tightly connected to the lifetime of a session. Employing randomness in the generation of unique session IDs helps to protect against brute-force attacks to determine future session IDs.

7.10.3 Requirement enhancements

None

7.10.4 Security levels

The requirements for the four SL levels that relate to CR 3.8 are:

- SL-C(SI, component) 1: Not selected
- SL-C(SI, component) 2: CR 3.8
- SL-C(SI, component) 3: CR 3.8
- SL-C(SI, component) 4: CR 3.8

7.11 CR 3.9 – Protection of audit information

7.11.1 Requirement

Components shall protect audit information, audit logs, and audit tools (if present) from unauthorized access, modification and deletion.

7.11.2 Rationale and supplemental guidance

Audit information includes all information (for example, audit records, audit settings and audit reports) needed to successfully audit control system activity. The audit information is important for error correction, security breach recovery, investigations and related efforts. Mechanisms for enhanced protection against modification and deletion include the storage of audit information to hardware-enforced write-once media.

7.11.3 Requirement enhancements

(1) Audit records on write-once media

Components shall provide the capability to store audit records on hardware-enforced write-once media.

7.11.4 Security levels

The requirements for the four SL levels that relate to CR 3.9 are:

- SL-C(SI, component) 1: Not selected
- SL-C(SI, component) 2: CR 3.9
- SL-C(SI, component) 3: CR 3.9
- SL-C(SI, component) 4: CR 3.9 (1)

7.12 CR 3.10 – Support for updates

The support for updates requirements are component-specific and can be located as requirements for each specific device type in Clauses 12 through 15.

7.13 CR 3.11 – Physical tamper resistance and detection

The physical tamper resistance and detection requirements are component -specific and can be located as requirements for each specific device type in Clauses 12 through 15.

7.14 CR 3.12 – Provisioning product supplier roots of trust

The provisioning product supplier roots of trust requirements are component -specific and can be located as requirements for each specific device type in Clauses 12 through 15.

7.15 CR 3.13 – Provisioning asset owner roots of trust

The provisioning asset owner roots of trust requirements are component -specific and can be located as requirements for each specific device type in Clauses 12 through 15.

7.16 CR 3.14 – Integrity of the boot process

The integrity of the boot process requirements are component-specific and can be located as requirements for each specific device type in Clauses 12 through 15.

8 FR 4 – Data confidentiality

8.1 Purpose and SL-C(DC) descriptions

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

- 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.

8.2 Rationale

Some component-generated information, whether at rest or in transit, is of a confidential or sensitive nature. This implies that some communication channels and datastores require protection against eavesdropping and unauthorized access.

8.3 CR 4.1 – Information confidentiality

8.3.1 Requirement

Components shall

a) provide the capability to protect the confidentiality of information at rest for which explicit read authorization is supported; and

b) support the protection of the confidentiality of information in transit as defined in ISA-62443-3-3 [11] SR 4.1.

8.3.2 Rationale and supplemental guidance

The decision whether a given information should be protected or not depends on the context and cannot be made at product design. However, the fact that an organization limits access to information by configuring explicit read authorizations in the control system is an indicator that this information should be protected by the organization. Thus, all information for which the component supports the capability to assign explicit read authorizations should be considered potentially sensitive and thus the component should also provide the capability to protect its confidentiality.

Confidentiality of information in transit requires system level capabilities which the component should be able to support.

For confidentiality protection, 8.5 CR 4.3 – Use of cryptography provides further requirements.

8.3.3 Requirement enhancements

None

8.3.4 Security levels

The requirements for the four SL levels that relate to CR 4.1 are:

- SL-C(DC, component) 1: CR 4.1
- SL-C(DC, component) 2: CR 4.1
- SL-C(DC, component) 3: CR 4.1
- SL-C(DC, component) 4: CR 4.1

8.4 CR 4.2 – Information persistence

8.4.1 Requirement

Components shall provide the capability to erase all information, for which explicit read authorization is supported, from components to be released from active service and/or decommissioned.

8.4.2 Rationale and supplemental guidance

Removal of a control system component from active service should not provide the opportunity for unintentional release of information for which explicit read authorization is supported. An example of such information can include authentication information and network configuration information stored in non-volatile storage or other cryptographic information that would facilitate unauthorized or malicious activity.

Information produced by the actions of a user or role (or the actions of a software process acting on behalf of a user or role) should not be disclosed to a different user or role in an uncontrolled fashion. Control of control system information or data persistence prevents information stored on a shared resource from being unintentionally disclosed after that resource has been released back to the control system.

8.4.3 Requirement enhancements

(1) Erase of shared memory resources

Components shall provide the capability to protect against unauthorized and unintended information transfer via volatile shared memory resources.

NOTE Volatile memory resources are those that generally do not retain information after being released to memory management. However, there are attacks against random access memory (RAM) which might extract key material or other confidential data before it is actually over-written. Therefore, when volatile shared memory is released back to the control system for use by a different user, all unique data and connections to unique data need to be purged from the resource so it is not visible or accessible to the new user.

(2) Erase verification

Components shall provide the capability to verify that the erasure of information occurred.

8.4.4 Security levels

The requirements for the four SL levels that relate to CR 4.2 are:

- SL-C(DC, component) 1: Not Selected
- SL-C(DC, component) 2: CR 4.2
- SL-C(DC, component) 3: CR 4.2 (1) (2)
- SL-C(DC, component) 4: CR 4.2 (1) (2)

8.5 CR 4.3 – Use of cryptography

8.5.1 Requirement

If cryptography is required, the component shall use cryptographic security mechanisms according to internationally recognized and proven security practices and recommendations.

8.5.2 Rationale and supplemental guidance

The selection of cryptographic protection should be based on a threat and risk analysis which covers the value of the information being protected, the consequences of the confidentiality and integrity of the information being breached, the time period during which the information is confidential and control system operating constraints. This can involve either information at rest, in transit, or both. Note that backups are an example of information at rest, and should be considered as part of a data confidentiality and integrity assessment process. The control system product supplier should document the practices and procedures relating to cryptographic key establishment and management. The control system should utilize established and tested encryption and hash algorithms, such as the advanced encryption standard (AES) and the secure hash algorithm (SHA) series, and key sizes based on an assigned standard. Key generation needs to be performed using an effective random number generator. The security policies and procedures for key management need to address periodic key changes, key destruction, key distribution and encryption key backup in accordance with defined standards. Generally accepted practices and recommendations can be found in documents such as NIST SP 800-57, *Recommendation for Key Management, Part 1: General* [25]. Implementation requirements can be found for example in FIPS 140-2, *Security Requirements for Cryptographic Modules* [24] or ISO/IEC 19790, *Information technology – Security techniques – Security requirements for cryptographic modules* [17].

This CR, along with 5.10, CR 1.8 – Public key infrastructure certificates may be applicable when meeting many other requirements defined within this document.

8.5.3 Requirement enhancements

None

8.5.4 Security levels

The requirements for the four security levels that relate to CR 4.3 are:

- SL-C(DC,component) 1: CR 4.3
- SL-C(DC,component) 2: CR 4.3
- SL-C(DC,component) 3: CR 4.3
- SL-C(DC,component) 4: CR 4.3

9 FR 5 – Restricted data flow

9.1 Purpose and SL-C(RDF) descriptions

Segment the control system via zones and conduits to limit the unnecessary flow of data.

- SL 1 – Prevent the casual or coincidental circumvention of zone and conduit segmentation.
- SL 2 – Prevent the intended circumvention of zone and conduit segmentation by entities using simple means with low resources, generic skills and low motivation.
- SL 3 – Prevent the intended circumvention of zone and conduit segmentation by entities using sophisticated means with moderate resources, IACS specific skills and moderate motivation.
- SL 4 – Prevent the intended circumvention of zone and conduit segmentation by entities using sophisticated means with extended resources, IACS specific skills and high motivation.

9.2 Rationale

Using their risk assessment methodology defined in ISA-62443-3-2, asset owners should determine necessary information flow restrictions and thus, by extension, determine the configuration of the conduits used to deliver this information. Derived prescriptive recommendations and guidelines should include mechanisms that range from disconnecting control system networks from business or public networks to using unidirectional gateways, single stateful firewalls or DMZ configurations to manage the flow of information.

9.3 CR 5.1 – Network segmentation

9.3.1 Requirement

Components shall support a segmented network to support zones and conduits, as needed, to support the broader network architecture based on logical segmentation and criticality.

9.3.2 Rationale and supplemental guidance

Network segmentation is used by organizations for a variety of purposes, including cyber security. The main reasons for segmenting networks are to reduce the exposure, or ingress, of network traffic into a control system and reduce the spread, or egress, of network traffic from a control system. This improves overall system response and reliability as well as provides a measure of cyber security protection. It also allows different network segments within the control system, including critical control systems and safety-related systems, to be segmented from other systems for an additional level of protection.

Access from the control system to the World Wide Web should be clearly justified based on control system operational requirements.

Network segmentation and the level of protection it provides will vary greatly depending on the overall network architecture used by an asset owner in their facility and even system integrators within their control systems. Logically segmenting networks based on their functionality provides some measure of protection, but may still lead to single-points-of-failure if a network device is compromised. Physically segmenting networks provides another level of protection by removing that single-point-of-failure case, but will lead to a more complex and costly network design. These trade-offs will need to be evaluated during the network design process (see ISA-62443-2-1).

In response to an incident, it may be necessary to break the connections between different network segments. In that event, the services necessary to support essential operations should be maintained in such a way that the devices can continue to operate properly and/or shutdown in an orderly manner. This may require that some servers may need to be duplicated on the control system network to support normal network features, for example dynamic host configuration protocol (DHCP), domain name service (DNS) or local CAs. It may also mean that some critical control systems and safety-related systems be designed from the beginning to be completely isolated from other networks.

9.3.3 Requirement enhancements

None

9.3.4 Security levels

The requirements for the four SL levels that relate to CR 5.1 are:

- SL-C(RDF, component) 1: CR 5.1
- SL-C(RDF, component) 2: CR 5.1
- SL-C(RDF, component) 3: CR 5.1
- SL-C(RDF, component) 4: CR 5.1

9.4 CR 5.2 – Zone boundary protection

The zone boundary protection requirements are network-component-specific and can be located as requirements for network devices in Clause 15.

9.5 CR 5.3 – General-purpose person-to-person communication restrictions

The general-purpose person-to-person communication restriction requirements are network-component-specific and can be located as requirements for network devices later in Clause 15.

9.6 CR 5.4 – Application partitioning

There is no component level requirement associated with ISA-62443-3-3 SR 5.4.

10 FR 6 – Timely response to events

10.1 Purpose and SL-C(TRE) descriptions

Respond to security violations by notifying the proper authorities, reporting needed evidence of the violation and taking timely corrective action when incidents are discovered.

- SL 1 – Monitor the operation of the components of the IACS, and respond to incidents when discovered, by collecting and providing the forensic evidence when queried.
- SL 2 – Monitor the operation of the components of the IACS, and respond to incidents when discovered, by actively collecting and periodically reporting forensic evidence.
- SL 3 – Monitor the operation of the components of the IACS, and respond to incidents when discovered, by actively collecting and pushing forensic evidence to the proper authorities.

- SL 4 – Monitor the operation of the components of the IACS, and respond to incidents when discovered, by actively collecting and pushing forensic evidence to the proper authorities in near real-time.

10.2 Rationale

Although a system may begin operation in a secure state, it is important to be able to monitor the system to ensure that it remains in that secure state. If an event impacts the security of a system, timely notification of the event may be critical to mitigating the associated risk. Asset owners should establish security policies and procedures and proper lines of communication and control needed to respond to security violations. Derived prescriptive recommendations and guidelines should include mechanisms that collect, report, preserve and automatically correlate the forensic evidence to ensure timely corrective action. The use of monitoring tools and techniques should not adversely affect the operational performance of the control system.

10.3 CR 6.1 – Audit log accessibility

10.3.1 Requirement

Components shall provide the capability for authorized humans and/or tools to access audit logs on a read-only basis.

10.3.2 Rationale and supplemental guidance

The applications and devices may generate audit records about events occurring in that application or device (see 6.10). Access to these audit logs is necessary to support filtering audit logs, identifying and removing information that is redundant, reviewing and reporting activity during after-the-fact investigations of security incidents. In general, audit reduction and report generation should be performed on a separate information system. Manual access to the audit records (such as, screen views or printouts) is sufficient for meeting the base requirement, but is insufficient for higher SLs. Programmatic access is commonly used to provide the audit log information to analysis mechanisms such as security information and event management (SIEM). See relevant SRs in Clauses 5, 6 and 9 regarding the creation of, protection of and access to audit logs.

10.3.3 Requirement enhancements

(1) Programmatic access to audit logs

Components shall provide programmatic access to audit records by either using an application programming interface (API) or sending the audit records to a centralized system

10.3.4 Security levels

The requirements for the four SL levels that relate to CR 6.1 are:

- SL-C(TRE, component) 1: CR 6.1
- SL-C(TRE, component) 2: CR 6.1
- SL-C(TRE, component) 3: CR 6.1 (1)
- SL-C(TRE, component) 4: CR 6.1 (1)

10.4 CR 6.2 – Continuous monitoring

10.4.1 Requirement

Components shall provide the capability to be continuously monitored using commonly accepted security industry practices and recommendations to detect, characterize and report security breaches in a timely manner.

10.4.2 Rationale and supplemental guidance

Control system monitoring capability can be achieved through a variety of tools and techniques (for example, IDS, intrusion prevention system (IPS), protection from malicious code mechanisms

and network monitoring mechanisms). As attacks become more sophisticated, these monitoring tools and techniques will need to become more sophisticated as well, including for example behavior-based IDS/IPS.

Monitoring devices should be strategically deployed within the control system (for example, at selected perimeter locations and near server farms supporting critical applications) to collect essential information. Monitoring mechanisms may also be deployed at ad hoc locations within the control system to track specific transactions.

Monitoring should include appropriate reporting mechanisms to allow for a timely response to events. To keep the reporting focused and the amount of reported information to a level that can be processed by the recipients, mechanisms such as SIEM are commonly applied to correlate individual events into aggregate reports that establish a larger context in which the raw events occurred.

10.4.3 Requirement enhancements

None

10.4.4 Security levels

The requirements for the four SL levels that relate to CR 6.2 are:

- SL-C(TRE, component) 1: Not Selected
- SL-C(TRE, component) 2: CR 6.2
- SL-C(TRE, component) 3: CR 6.2
- SL-C(TRE, component) 4: CR 6.2

11 FR 7 – Resource availability

11.1 Purpose and SL-C(RA) descriptions

Ensure the availability of components against the degradation or denial of essential services.

- SL 1 – Ensure that the component operates reliably under normal production conditions and prevents denial-of-service situations caused by the casual or coincidental actions of an entity.
- SL 2 – Ensure that the component operates reliably under normal and abnormal production conditions and prevents denial-of-service situations by entities using simple means with low resources, generic skills and low motivation.
- SL 3 – Ensure that the component operates reliably under normal, abnormal, and extreme production conditions and prevents denial-of-service situations by entities using sophisticated means with moderate resources, IACS specific skills and moderate motivation.
- SL 4 – Ensure that the component operates reliably under normal, abnormal, and extreme production conditions and prevents denial-of-service situations by entities using sophisticated means with extended resources, IACS specific skills and high motivation.

11.2 Rationale

The aim of this series of CRs is to ensure that the component is resilient against various types of DoS events. This includes the partial or total unavailability of component functionality at various levels. In particular, security incidents in the component should not affect essential functions or other safety-related functions.

11.3 CR 7.1 – Denial of service protection

11.3.1 Requirement

Components shall provide the capability to maintain essential functions when operating in a degraded mode as the result of a DoS event.

11.3.2 Rationale and supplemental guidance

Components may be subjected to different forms of DoS situations. When these occur the component should be designed in such a manner that it maintains essential functions necessary for continued safe operations while in a degraded mode.

11.3.3 Requirement enhancements

(1) Manage communication load from component

Components shall provide the capability to mitigate the effects of information and/or message flooding types of DoS events.

11.3.4 Security levels

The requirements for the four SL levels that relate to CR 7.1 are:

- SL-C(RA, component) 1: CR 7.1
- SL-C(RA, component) 2: CR 7.1 (1)
- SL-C(RA, component) 3: CR 7.1 (1)
- SL-C(RA, component) 4: CR 7.1 (1)

11.4 CR 7.2 – Resource management

11.4.1 Requirement

Components shall provide the capability to limit the use of resources by security functions to protect against resource exhaustion.

11.4.2 Rationale and supplemental guidance

Resource management (for example, network segmentation or priority schemes) prevents a lower-priority software process from delaying or interfering with the control system servicing any higher-priority software process. For example, initiating network scans, patching and/or antivirus checks on an operating system can cause severe disruption to normal operations. Traffic rate limiting schemes should be considered as a mitigation technique.

11.4.3 Requirement enhancements

None

11.4.4 Security levels

The requirements for the four SL levels that relate to CR 7.2 are:

- SL-C(RA, component) 1: CR 7.2
- SL-C(RA, component) 2: CR 7.2
- SL-C(RA, component) 3: CR 7.2
- SL-C(RA, component) 4: CR 7.2

11.5 CR 7.3 – Control system backup

11.5.1 Requirement

Components shall provide the capability to participate in system level backup operations in order to safeguard the component state (user- and system-level information). The backup process shall not affect the normal component operations.

11.5.2 Rationale and supplemental guidance

The availability of up-to-date backups is essential for recovery from a control system failure and/or mis-configuration. Automating this function ensures that all required files are captured, reducing operator overhead.

When designing to support a backup capability, consideration should be given to information that will be stored in backups. Some of this information may contain cryptographic keys and other information that is protected through security controls while part of the system. Once the information is placed into a backup it most likely will not have the same controls in place to protect it. Thus the component backup ability needs to include the mechanisms to support the necessary protection of the information that is contained in the backup. This may include encryption of the backup, encryption of the sensitive data as part of the backup procedure or not including the sensitive information as part of the backup. If the backup is encrypted it is important not to include the cryptographic keys as part of the backup but to backup the cryptographic keys as part of a separate more secure backup procedure.

11.5.3 Requirement enhancements

(1) Backup integrity verification

Components shall provide the capability to validate the integrity of backed up information prior to the initiation of a restore of that information.

11.5.4 Security levels

The requirements for the four SL levels that relate to CR 7.3 are:

- SL-C(RA, component) 1: CR 7.3
- SL-C(RA, component) 2: CR 7.3 (1)
- SL-C(RA, component) 3: CR 7.3 (1)
- SL-C(RA, component) 4: CR 7.3 (1)

11.6 CR 7.4 – Control system recovery and reconstitution

11.6.1 Requirement

Components shall provide the capability to be recovered and reconstituted to a known secure state after a disruption or failure.

11.6.2 Rationale and supplemental guidance

Component recovery and reconstitution to a known secure state means that all system parameters (either default or configurable) are set to secure values, security-critical patches are reinstalled, security-related configuration settings are reestablished, system documentation and operating procedures are available, components are reinstalled and configured with established settings, information from the most recent, known secure backups is loaded and the system is fully tested and functional.

11.6.3 Requirement enhancements

None

11.6.4 Security levels

The requirements for the four SL levels that relate to CR 7.4 are:

- SL-C(RA, component) 1: CR 7.4
- SL-C(RA, component) 2: CR 7.4
- SL-C(RA, component) 3: CR 7.4
- SL-C(RA, component) 4: CR 7.4

11.7 CR 7.5 - Emergency Power

There is no component level requirement associated with ISA-62443-3-3 SR 7.5.

11.8 CR 7.6 – Network and security configuration settings

11.8.1 Requirement

Components shall provide the capability to be configured according to recommended network and security configurations as described in guidelines provided by the control system supplier. The component shall provide an interface to the currently deployed network and security configuration settings.

11.8.2 Rationale and supplemental guidance

These configuration settings are the adjustable parameters of the control system components. By default, the component should be configured to the recommended settings. In order for a component to detect and correct any deviations from the approved and/or recommended configuration settings, the component needs to support monitoring and control of changes to the configuration settings in accordance with security policies and procedures.

11.8.3 Requirement enhancements

(1) Machine-readable reporting of current security settings

Components shall provide the capability to generate a report listing the currently deployed security settings in a machine-readable format.

11.8.4 Security levels

The requirements for the four SL levels that relate to CR 7.6 are:

- SL-C(RA, component) 1: CR 7.6
- SL-C(RA, component) 2: CR 7.6
- SL-C(RA, component) 3: CR 7.6 (1)
- SL-C(RA, component) 4: CR 7.6 (1)

11.9 CR 7.7 – Least functionality

11.9.1 Requirement

Components shall provide the capability to specifically restrict the use of unnecessary functions, ports, protocols and/or services.

11.9.2 Rationale and supplemental guidance

Components are capable of providing a wide variety of functions and services. Some of the functions and services provided may not be necessary to support IACS functionality. Therefore, by default, functions beyond a baseline configuration should be disabled. Additionally, it is sometimes convenient to provide multiple services from a single component of a control system, but doing so increases the risk compared to limiting the services provided by any one component.

11.9.3 Requirement enhancements

None

11.9.4 Security levels

The requirements for the four SL levels that relate to CR 7.7 are:

- SL-C(RA, component) 1: CR 7.7
- SL-C(RA, component) 2: CR 7.7
- SL-C(RA, component) 3: CR 7.7
- SL-C(RA, component) 4: CR 7.7

11.10 CR 7.8 – Control system component inventory

11.10.1 Requirement

Components shall provide the capability to support a control system component inventory according to ISA-62443-3-3 [11] SR 7.8.

11.10.2 Rationale and supplemental guidance

Components may bring their own set of components into the overall control system. When this is the case then those components need to provide a mechanism to augment the overall component inventory which is compatible with ISA-62443-2-4 [8] SP.06.02.

11.10.3 Requirement enhancements

None

11.10.4 Security levels

The requirements for the four SL levels that relate to CR 7.8 are:

- SL-C(RA, component) 1: Not Selected
- SL-C(RA, component) 2: CR 7.8
- SL-C(RA, component) 3: CR 7.8
- SL-C(RA, component) 4: CR 7.8

12 Software application requirements

12.1 Purpose

The purpose of this set of requirements is to document requirements that are specific to software applications.

12.2 SAR 2.4 – Mobile code

12.2.1 Requirement

In the event that a software application utilizes mobile code technologies, that application shall provide the capability to enforce a security policy for the usage of mobile code technologies. The security policy shall allow, at a minimum, the following actions for each mobile code technology used on the software application:

a) Control execution of mobile code;

b) Control which users (human, software process, or device) are allowed to transfer mobile code to/from the application;

c) Control the execution of mobile code based on the results of an integrity check prior to the code being executed.

12.2.2 Rationale and supplemental guidance

Mobile code technologies include, but are not limited to, Java, JavaScript, ActiveX, portable document format (PDF), Postscript, Shockwave movies, Flash animations and VBScript. Usage restrictions apply to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations. Control procedures should prevent the development, acquisition or introduction of unacceptable mobile code within the control system in which the component resides. For example, mobile code exchanges may be disallowed directly within the control system, but may be allowed in a controlled adjacent environment maintained by IACS personnel.

12.2.3 Requirement enhancements

(1) Mobile code authenticity check

The application shall provide the capability to enforce a security policy that allows the device to control execution of mobile code based on the results of an authenticity check prior to the code being executed.

12.2.4 Security levels

The requirements for the four SL levels that relate to SAR 2.4 are:

- SL-C(UC, component) 1: SAR 2.4
- SL-C(UC, component) 2: SAR 2.4 (1)
- SL-C(UC, component) 3: SAR 2.4 (1)
- SL-C(UC, component) 4: SAR 2.4 (1)

12.3 SAR 3.2 – Protection from malicious code

12.3.1 Requirement

The application product supplier shall qualify and document which protection from malicious code mechanisms are compatible with the application and note any special configuration requirements.

12.3.2 Rationale and supplemental guidance

Protection from malicious code (for example, viruses, worms, Trojan horses and spyware) may be provided by the control system application or by an external service or application. Control system applications need to be compatible with mechanisms designed to protect them from malicious code. This requirement does not imply that the product supplier is to qualify and document all malicious code protection mechanisms which are compatible with the application but implies that the product supplier is to qualify and document at least one mechanism.

12.3.3 Requirement enhancements

None

12.3.4 Security levels

The requirements for the four SL levels that relate to SAR 3.2 are:

- SL-C(SI, component) 1: SAR 3.2
- SL-C(SI, component) 2: SAR 3.2
- SL-C(SI, component) 3: SAR 3.2
- SL-C(SI, component) 4: SAR 3.2

13 Embedded device requirements

13.1 Purpose

The purpose of this set of requirements is to document requirements that are specific to embedded devices.

13.2 EDR 2.4 – Mobile code

13.2.1 Requirement

In the event that an embedded device utilizes mobile code technologies, the embedded device shall provide the capability to enforce a security policy for the usage of mobile code technologies. The security policy shall allow, at a minimum, the following actions for each mobile code technology used on the embedded device:

a) Control execution of mobile code;

b) Control which users (human, software process, or device) are allowed to upload mobile code to the device;

c) Control the execution of mobile code based on the results of an integrity check prior to the code being executed.

13.2.2 Rationale and supplemental guidance

Mobile code technologies include, but are not limited to, Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations and VBScript. Usage restrictions apply to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations. Control procedures should prevent the development, acquisition or introduction of unacceptable mobile code within the control system in which the component resides. For example, mobile code exchanges may be disallowed directly within the control system, but may be allowed in a controlled adjacent environment maintained by IACS personnel.

13.2.3 Requirement enhancements

(1) Mobile code authenticity check

The embedded device shall provide the capability to enforce a security policy that allows the device to control execution of mobile code based on the results of an authenticity check prior to the code being executed

13.2.4 Security levels

The requirements for the four SL levels that relate to EDR 2.4 are:

- SL-C(UC, component) 1: EDR 2.4
- SL-C(UC, component) 2: EDR 2.4 (1)
- SL-C(UC, component) 3: EDR 2.4 (1)
- SL-C(UC, component) 4: EDR 2.4 (1)

13.3 EDR 2.13 – Use of physical diagnostic and test interfaces

13.3.1 Requirement

Embedded devices shall protect against unauthorized use of the physical factory diagnostic and test interface(s) (e.g. JTAG Debugging).

13.3.2 Rationale and supplemental guidance

Factory diagnostic and test interface(s) are created at various locations within the embedded device to assist the embedded device's developers and factory personnel as they test the

functional implementation, and when errors are discovered to subsequently remove them from the embedded device. However, these same interfaces must be carefully protected from access by unauthorized entities to protect the essential functionality provided by the embedded device to the IACS.

If a diagnostic and test interface does not provide an ability to control the embedded device or to access non-public information, then it will not need an authentication mechanism. This shall be determined via a threat and risk assessment. An example of this would be JTAG debugging, in which JTAG is used to take control of the processor and execute arbitrary commands, versus a JTAG boundary scan where JTAG is used to simply read information (which may be publicly available information).

There may be cases where the factory diagnostic and test interface(s) use network communications with the device. When this is the case those interfaces are to be subjected to all of the requirements of this document.

13.3.3 Requirement enhancements

(1) Active monitoring

Embedded devices shall provide active monitoring of the device's diagnostic and test interface(s) and generate an audit log entry when attempts to access these interface(s) are detected.

13.3.4 Security levels

The requirements for the four SL levels that relate to EDR 2.13 are:

- SL-C(SI, component) 1: Not Selected
- SL-C(SI, component) 2: EDR 2.13
- SL-C(SI, component) 3: EDR 2.13 (1)
- SL-C(SI, component) 3: EDR 2.13 (1)

13.4 EDR 3.2 – Protection from malicious code

13.4.1 Requirement

The embedded device shall provide the capability to protect from installation and execution of unauthorized software.

13.4.2 Rationale and supplemental guidance

Unauthorized software may contain malicious code and thus be harmful to the component. If an embedded device is able to utilize a compensating control, it need not directly support protection from malicious code. It is assumed that the IACS will be responsible for providing the required safeguards. However, for scenarios such as having a local universal serial bus (USB) host access, the need for protection from malicious code should be determined by a risk assessment.

Detection mechanisms should be able to detect integrity violations of application binaries and data files. Techniques may include, but are not limited to, binary integrity and attributes monitoring, hashing and signature techniques.

Prevention techniques may include, but are not limited to, removable media control, sandbox techniques and specific computing platforms mechanisms such as restricted firmware update capabilities, No Execute (NX) bit, data execution prevention (DEP), address space layout randomization (ASLR), stack corruption detection and mandatory access controls. See 10.4 for an associated requirement involving control system monitoring tools and techniques.

13.4.3 Requirement enhancements

None

13.4.4 Security levels

The requirements for the four SL levels that relate to EDR 3.2 are:

- SL-C(SI, component) 1: EDR 3.2
- SL-C(SI, component) 2: EDR 3.2
- SL-C(SI, component) 3: EDR 3.2
- SL-C(SI, component) 4: EDR 3.2

13.5 EDR 3.10 – Support for updates

13.5.1 Requirement

The embedded device shall support the ability to be updated and upgraded.

13.5.2 Rationale and supplemental guidance

Embedded devices over their installed lifetime may have the need for installation of updates and upgrades. There will be cases where embedded devices are supporting or executing essential functions as well. When this is the case the embedded device needs to have mechanisms in place to support patching and updating without impacting the essential functions of high availability systems (see 4.2 CCSC 1 Support of essential functions). One example for providing this capability would be to support redundancy within the embedded device.

13.5.3 Requirement enhancements

(1) Update authenticity and integrity

The embedded device shall validate the authenticity and integrity of any software update or upgrade prior to installation.

13.5.4 Security levels

The requirements for the four SL levels that relate to EDR 3.10 are:

- SL-C(SI, component) 1: EDR 3.10
- SL-C(SI, component) 2: EDR 3.10 (1)
- SL-C(SI, component) 3: EDR 3.10 (1)
- SL-C(SI, component) 4: EDR 3.10 (1)

13.6 EDR 3.11 – Physical tamper resistance and detection

13.6.1 Requirement

The embedded device shall provide tamper resistance and detection mechanisms to protect against unauthorized physical access into the device

13.6.2 Rationale and supplemental guidance

The purpose of tamper resistance mechanisms is to prevent an attempt by an attacker to execute an unauthorized physical action against an IACS device. Secondary to prevention, detection and response are essential should a tampering event occur.

Tamper resistance mechanisms are most effectively used in combinations to prevent access to any critical components. Tamper resistance consists of using specialized materials to make tampering of a device or module difficult. This can include such features as hardened enclosures, locks, encapsulation, or security screws. Putting in place tight airflow paths will increase the difficulty of probing the product internals.

The purpose of tamper evidence is to ensure that visible or electronic evidence remains when a tampering event occurs. Many simple evidence techniques are comprised of seals and tapes to make it obvious that there has been physical tampering. More sophisticated techniques include switches.

13.6.3 Requirement enhancements

(1) Notification of a tampering attempt

The embedded device shall be capable of automatically providing notification to a configurable set of recipients upon discovery of an attempt to make an unauthorized physical access. All notifications of tampering shall be logged as part of the overall audit logging function.

13.6.4 Security levels

The requirements for the four SL levels that relate to EDR 3.11 are:

- SL-C(SI, component) 1: Not Selected
- SL-C(SI, component) 2: EDR 3.11
- SL-C(SI, component) 3: EDR 3.11 (1)
- SL-C(SI, component) 4: EDR 3.11 (1)

13.7 EDR 3.12 – Provisioning product supplier roots of trust

13.7.1 Requirement

Embedded devices shall provide the capability to provision and protect the confidentiality, integrity, and authenticity of product supplier keys and data to be used as one or more “roots of trust” at the time of manufacture of the device.

13.7.2 Rationale and supplemental guidance

In order for a component to be able to validate the authenticity and integrity of the hardware, software, and data provided by the product supplier, it must possess a trusted source of data to perform the validation process. This trusted source of data is referred to as the “root of trust” for the system. This trusted source of data may be a set of cryptographic hashes of “known good” software, or it may be the public portion of an asymmetric cryptographic key pair to be used in the validation of cryptographic signatures. This trusted data is often used to validate critical software, firmware, and data prior to booting the firmware or operating system of a component, in order to validate that the component will boot into a “known good” state in which all security mechanisms are known to be operational and uncompromised. “Root of trust” data is often protected via hardware mechanisms, preventing any modification of the data during normal operations of the component. Modification of product supplier root of trust data is typically limited to the product supplier’s provisioning process, where the product supplier has a trusted process to perform the provisioning of the data. Instead, information to be validated against the root of trust is submitted to the validation process through a hardware or software API which performs the validation and returns the results without exposing the protected data.

13.7.3 Requirement Enhancements

None

13.7.4 Security levels

The requirements for the four SL levels that relate to EDR 3.12 are:

- SL-C(SI, component) 1: Not Selected
- SL-C(SI, component) 2: EDR 3.12
- SL-C(SI, component) 3: EDR 3.12

- SL-C(SI, component) 3: EDR 3.12

13.8 EDR 3.13 – Provisioning asset owner roots of trust

13.8.1 Requirement

Embedded devices shall

a) provide the capability to provision and protect the confidentiality, integrity, and authenticity of asset owner keys and data to be used as “roots of trust”; and

b) support the capability to provision without reliance on components that may be outside of the device’s security zone.

13.8.2 Rationale and supplemental guidance

Product suppliers have established mechanisms to ensure that the software and firmware on their components is authentic, and the integrity of that software and firmware has not been compromised. This allows the product supplier to provide the asset owner with a “known good” state from which to operate. However, many product suppliers also provide mechanisms for asset owners to extend the functionality of their devices through the use of mobile code, user programs, or other such means. In order to protect the security of the component, it is important that these extensions to the component’s functionality also be validated to ensure that they are authorized, and that the asset owner has approved of their origins.

In order to perform these validations the component must contain data that provides a way to differentiate between valid and invalid origins. The list of valid and invalid origins will differ from asset owner to asset owner, and it is unlikely that a product supplier will have a complete list of every possible valid origin at time of manufacture. Therefore it is important that the product supplier provide a way for the asset owner to securely provision their own “roots of trust” which provide the ability to distinguish between origins allowed by the asset owner’s security policy, and those that are not. The authenticity and integrity of these “roots of trust” must be protected so that malicious actors cannot add additional roots of trust that grant them the ability to operate on the component.

A root of trust can also be used as a basis communications security, such as communications integrity required by CR 3.1 – Communication integrity or communications confidentiality required by CR 4.1 – Information confidentiality.

Requirements such as EDR 2.4 – Mobile code require the component to complete authenticity checks on mobile code prior to the execution of mobile code. The roots of trust provided by this requirement provide the data necessary to validate the origin and integrity of mobile code, allowing the component to independently determine if the code is allowed to execute.

13.8.3 Requirement Enhancements

None

13.8.4 Security levels

The requirements for the four SL levels that relate to EDR 3.13 are:

- SL-C(SI, component) 1: Not Selected
- SL-C(SI, component) 2: EDR 3.13
- SL-C(SI, component) 3: EDR 3.13
- SL-C(SI, component) 4: EDR 3.13

13.9 EDR 3.14 – Integrity of the boot process

13.9.1 Requirement

Embedded devices shall verify the integrity of the firmware, software, and configuration data needed for the component's boot and runtime processes prior to use.

13.9.2 Rationale and supplemental guidance

In order to make assurances to an asset owner that a component's security functionality has not been compromised, it is necessary to ensure that the component's software and firmware has not been tampered with, and that the software and firmware is valid to execute on the component. Therefore the component must perform checks to validate the integrity of the component's firmware and/or software prior to use during the boot process, to ensure that the component does not boot into an insecure or invalid operating state that could damage the component or provide a path for a malicious actor to gain access to additional components, assets, or data.

13.9.3 Requirement enhancements

(1) Authenticity of the boot process

Embedded devices shall use the component's product supplier roots of trust to verify the authenticity of the firmware, software, and configuration data needed for the component's boot process prior to it being used in the boot process.

13.9.4 Security levels

The requirements for the four SL levels that relate to EDR 3.14 are:

- SL-C(SI, component) 1: EDR 3.14
- SL-C(SI, component) 2: EDR 3.14 (1)
- SL-C(SI, component) 3: EDR 3.14 (1)
- SL-C(SI, component) 4: EDR 3.14 (1)

14 Host device requirements

14.1 Purpose

The purpose of this set of requirements is to document requirements that are specific to host devices.

14.2 HDR 2.4 – Mobile code

14.2.1 Requirement

In the event that a host device utilizes mobile code technologies, that host device shall provide the capability to enforce a security policy for the usage of mobile code technologies. The security policy shall allow, at a minimum, the following actions for each mobile code technology used on the host device:

a) Control execution of mobile code;

b) Control which users (human, software process, or device) are allowed to upload mobile code to the host device; and

c) Control the code execution based upon integrity checks on the mobile code and prior to the code being executed.

14.2.2 Rationale and supplemental guidance

Mobile code technologies include, but are not limited to, Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations and VBScript. Usage restrictions apply to both the selection and use of mobile code installed on servers and mobile code downloaded and

executed on individual workstations. Control procedures should prevent the development, acquisition or introduction of unacceptable mobile code within the control system in which the host device resides. For example, mobile code exchanges may be disallowed directly with the control system, but may be allowed in a controlled adjacent environment maintained by IACS personnel.

Mobile code could be secured by adding integrity, authenticity, and authorization checks to the code itself (application layer), or for “just-in-time” code execution through transmitting the mobile code via a secure communications tunnel which provides these attributes, or any mechanism equivalent to these options.

14.2.3 Requirement enhancements

(1) Mobile code authenticity check

The host device shall provide the capability to enforce a security policy that allows the device to control execution of mobile code based on the results of an authenticity check prior to the code being executed.

14.2.4 Security levels

The requirements for the four SL levels that relate to HDR 2.4 are:

- SL-C(UC, component) 1: HDR 2.4
- SL-C(UC, component) 2: HDR 2.4(1)
- SL-C(UC, component) 3: HDR 2.4 (1)
- SL-C(UC, component) 4: HDR 2.4 (1)

14.3 HDR 2.13 – Use of physical diagnostic and test interfaces

14.3.1 Requirement

Host devices shall protect against unauthorized use of the physical factory diagnostic and test interface(s) (e.g. JTAG debugging).

14.3.2 Rationale and supplemental guidance

Factory diagnostic and test interface(s) are created at various locations within the host device to assist the component’s developers and factory personnel as they test the functional implementation, and when errors are discovered to subsequently remove them from the component. However, these same interfaces must be carefully protected from access by unauthorized entities to protect the essential functionality provided by the component to the IACS.

There may be cases where the factory diagnostic and test interface(s) use network communications with the device. When this is the case those interfaces are to be subjected to all of the requirements of this document.

If a diagnostic and test interface does not provide an ability to control the host device or to access non-public information, then it will not need an authentication mechanism. This shall be determined via a threat and risk assessment. An example of this would be JTAG debugging, in which JTAG is used to take control of the processor and execute arbitrary commands, versus a JTAG boundary scan where JTAG is used to simply read information (which may be publicly available information).

14.3.3 Requirement enhancements

(1) Active monitoring

Host devices shall provide active monitoring of the device’s diagnostic and test interface(s) and generate an audit log entry when attempts to access these interface(s) are detected.

14.3.4 Security levels

The requirements for the four SL levels that relate to HDR 2.13 are:

- SL-C(SI, component) 1: Not Selected
- SL-C(SI, component) 2: HDR 2.13
- SL-C(SI, component) 3: HDR 2.13 (1)
- SL-C(SI, component) 3: HDR 2.13 (1)

14.4 HDR 3.2 – Protection from malicious code

14.4.1 Requirement

There shall be mechanisms on host devices that are qualified by the IACS product supplier to provide protection from malicious code. The IACS product supplier shall document any special configuration requirements related to protection from malicious code.

14.4.2 Rationale and supplemental guidance

Host devices need to support the use of malicious code protection (against, for example, viruses, worms, Trojan horses and spyware). The product supplier should qualify and document the configuration of protection from malicious code mechanisms so that the primary mission of the control system is maintained.

14.4.3 Requirement enhancements

(1) Report version of code protection

The host device shall automatically report the software and file versions of protection from malicious code in use (as part of overall logging function).

14.4.4 Security levels

The requirements for the four SL levels that relate to HDR 3.2 are:

- SL-C(SI, component) 1: HDR 3.2
- SL-C(SI, component) 2: HDR 3.2 (1)
- SL-C(SI, component) 3: HDR 3.2 (1)
- SL-C(SI, component) 4: HDR 3.2 (1)

14.5 HDR 3.10 – Support for updates

14.5.1 Requirement

Host devices shall support the ability to be updated and upgraded.

14.5.2 Rationale and supplemental guidance

Host devices over their installed lifetime may have the need for installation of updates and upgrades. There will be cases where host devices are supporting or executing essential functions as well. When this is the case the host device should have mechanisms in place to support patching and updating without impacting the essential functions of high availability systems (see 4.2 CCSC 1 Support of essential functions). One example for providing this capability would be to support redundancy within the host device.

14.5.3 Requirement enhancements

(1) Update authenticity and integrity

Host devices shall validate the authenticity and integrity of any software update or upgrade prior to installation.

14.5.4 Security levels

The requirements for the four SL levels that relate to HDR 3.10 are:

- SL-C(SI, component) 1: HDR 3.10

- SL-C(SI, component) 2: HDR 3.10 (1)
- SL-C(SI, component) 3: HDR 3.10 (1)
- SL-C(SI, component) 4: HDR 3.10 (1)

14.6 HDR 3.11 – Physical tamper resistance and detection

14.6.1 Requirement

Host devices shall provide the capability to support tamper resistance and detection mechanisms to protect against unauthorized physical access into the device.

14.6.2 Rationale and supplemental guidance

The purpose of tamper resistance mechanisms is to prevent an attempt by an attacker to execute an unauthorized physical action against an IACS device. Secondary to prevention, detection and response are essential should a tampering event occur.

Tamper resistance mechanisms are most effectively used in combinations to prevent access to any critical components. Tamper resistance consists of using specialized materials to make tampering of a device or module difficult. This can include such features as hardened enclosures, locks, encapsulation, or security screws. Putting in place tight airflow paths will increase the difficulty of probing the product internals.

The purpose of tamper evidence is to ensure that visible or electronic evidence remains when a tampering event occurs. Many simple evidence techniques are comprised of seals and tapes to make it obvious that there has been physical tampering. More sophisticated techniques include switches.

14.6.3 Requirement enhancements

(1) Notification of a tampering attempt

Host devices shall be capable of automatically providing notification to a configurable set of recipients upon discovery of an attempt to make an unauthorized physical access. All notifications of tampering shall be logged as part of the overall audit logging function.

14.6.4 Security levels

The requirements for the four SL levels that relate to HDR 3.11 are:

- SL-C(SI, component) 1: Not Selected
- SL-C(SI, component) 2: HDR 3.11
- SL-C(SI, component) 3: HDR 3.11 (1)
- SL-C(SI, component) 4: HDR 3.11 (1)

14.7 HDR 3.12 – Provisioning product supplier roots of trust

14.7.1 Requirement

Host devices shall provide the capability to provision and protect the confidentiality, integrity, and authenticity of product supplier keys and data to be used as one or more “roots of trust” at the time of manufacture of the device.

14.7.2 Rationale and supplemental guidance

In order for a component to be able to validate the authenticity and integrity of the hardware, software, and data provided by the product supplier, it must possess a trusted source of data to perform the validation process. This trusted source of data is referred to as the “root of trust” for the system. This trusted source of data may be a set of cryptographic hashes of “known good” software, or it may be the public portion of an asymmetric cryptographic key pair to be used in the validation of cryptographic signatures. This trusted data is often used to validate critical software,

firmware, and data prior to booting the firmware or operating system of a component, in order to validate that the component will boot into a “known good” state in which all security mechanisms are known to be operational and uncompromised. “Root of trust” data can be protected by software or hardware implemented mechanisms to prevent any modification of the data during normal operations of the component. Modification of product supplier root of trust data is typically limited to the product supplier’s provisioning process, where the product supplier has a trusted process to perform the provisioning of the data. Instead, information to be validated against the root of trust is submitted to the validation process through a hardware or software API which performs the validation and returns the results without exposing the protected data.

14.7.3 Requirement Enhancements

None

14.7.4 Security levels

The requirements for the four SL levels that relate to HDR 3.12 are:

- SL-C(SI, component) 1: Not Selected
- SL-C(SI, component) 2: HDR 3.12
- SL-C(SI, component) 3: HDR 3.12
- SL-C(SI, component) 3: HDR 3.12

14.8 HDR 3.13 – Provisioning asset owner roots of trust

14.8.1 Requirement

Host devices shall

a) provide the capability to provision and protect the confidentiality, integrity, and authenticity of asset owner keys and data to be used as “roots of trust”; and

b) support the capability to provision without reliance on components that may be outside of the device’s security zone.

14.8.2 Rationale and supplemental guidance

Product suppliers have established mechanisms to ensure that the software and firmware on their components is authentic, and the integrity of that software and firmware has not been compromised. This allows the product supplier to provide the asset owner with a “known good” state from which to operate. However, many product suppliers also provide mechanisms for asset owners to extend the functionality of their devices through the use of mobile code, user programs, or other such means. In order to protect the security of the component, it is important that these extensions to the component’s functionality also be validated to ensure that they are authorized, and that the asset owner has approved of their origins.

In order to perform these validations the component must contain data that provides a way to differentiate between valid and invalid origins. The list of valid and invalid origins will differ from asset owner to asset owner, and it is unlikely that a product supplier will have a complete list of every possible valid origin at time of manufacture. Therefore it is important that the product supplier provide a way for the asset owner to securely provision their own “roots of trust” which provide the ability to distinguish between origins allowed by the asset owner’s security policy, and those that are not. The authenticity and integrity of these “roots of trust” must be protected so that malicious actors cannot add additional roots of trust that grant them the ability to operate on the component.

Requirements such as HDR 2.4 – Mobile code require the component to complete authenticity checks on mobile code prior to the execution of mobile code. The roots of trust provided by this

requirement provide the data necessary to validate the origin and integrity of mobile code, allowing the component to independently determine if the code is allowed to execute.

A root of trust can also be used as a basis communications security, such as communications integrity required by CR 3.1 – Communication integrity or communications confidentiality required by CR 4.1 – Information confidentiality.

14.8.3 Requirement Enhancements

None

14.8.4 Security levels

The requirements for the four SL levels that relate to HDR 3.13 are:

- SL-C(SI, component) 1: Not Selected
- SL-C(SI, component) 2: HDR 3.13
- SL-C(SI, component) 3: HDR 3.13
- SL-C(SI, component) 4: HDR 3.13

14.9 HDR 3.14 – Integrity of the boot process

14.9.1 Requirement

Host devices shall verify the integrity of the firmware, software, and configuration data needed for component's boot process prior to it being used in the boot process.

14.9.2 Rationale and supplemental guidance

In order to make assurances to an asset owner that a component's security functionality has not been compromised, it is necessary to ensure that the component's software and firmware has not been tampered with, and that the software and firmware is valid to execute on the component. Therefore the component must perform checks to validate the integrity and authenticity of the component's firmware and/or software prior to the boot process, to ensure that the component does not boot into an insecure or invalid operating state that could damage the component or provide a path for a malicious actor to gain access to additional components, assets, or data.

14.9.3 Requirement enhancements

(1) Authenticity of the boot process

Host devices shall use the component's product supplier roots of trust to verify the authenticity of the firmware, software, and configuration data needed for component's boot process prior to it being used in the boot process.

14.9.4 Security levels

The requirements for the four SL levels that relate to HDR 3.14 are:

- SL-C(SI, component) 1: HDR 3.14
- SL-C(SI, component) 2: HDR 3.14 (1)
- SL-C(SI, component) 3: HDR 3.14 (1)
- SL-C(SI, component) 4: HDR 3.14 (1)

15 Network device requirements

15.1 Purpose

The purpose of this set of requirements is to document requirements that are specific to network devices.

15.2 NDR 1.6 – Wireless access management

15.2.1 Requirement

A network device supporting wireless access management shall provide the capability to identify and authenticate all users (humans, software processes or devices) engaged in wireless communication.

15.2.2 Rationale and supplemental guidance

Any wireless technology can, and in most cases should, be considered just another communication protocol option. Thus, it should be subject to the same IACS security requirements as any other communication type utilized by the IACS. However, from a security point of view, there is at least one significant difference between wired and wireless communications. Physical security countermeasures are typically less effective when using wireless.

15.2.3 Requirement enhancements

(1) Unique identification and authentication

The network device shall provide the capability to uniquely identify and authenticate all users (humans, software processes or devices) engaged in wireless communication.

15.2.4 Security levels

The requirements for the four SL levels that relate to NDR 1.6 are:

- SL-C(UC, component) 1: NDR 1.6
- SL-C(UC, component) 2: NDR 1.6 (1)
- SL-C(UC, component) 3: NDR 1.6 (1)
- SL-C(UC, component) 4: NDR 1.6 (1)

15.3 NDR 1.13 – Access via untrusted networks

15.3.1 Requirement

The network device supporting device access into a network shall provide the capability to monitor and control all methods of access to the network device via untrusted networks.

15.3.2 Rationale and supplemental guidance

The network device should protect against unauthorized connections or subversion of authorized connections.

Examples of access to the network device via untrusted networks typically include remote access methods (such as, dial-up, broadband and wireless) as well as connections from a company's office (non-control system) network. The network device may provide ACL (Access Control List) functionality to restrict access by:

Layer 2 forwarding devices such as Ethernet switches:

a) MAC address

b) VLAN

Layer 3 forwarding devices such as routers, gateways and firewalls:

a) IP address

b) Port and protocol

c) Virtual Private Networks

15.3.3 Requirement enhancements

(1) Explicit access request approval

The network device shall provide the capability to deny access requests via untrusted networks unless explicitly approved by an assigned role.

15.3.4 Security levels

The requirements for the four SL levels that relate to NDR 1.13 are:

- SL-C(UC, component) 1: NDR 1.13
- SL-C(UC, component) 2: NDR 1.13
- SL-C(UC, component) 3: NDR 1.13 (1)
- SL-C(UC, component) 4: NDR 1.13 (1)

15.4 NDR 2.4 – Mobile code

15.4.1 Requirement

In the event that a network device utilizes mobile code technologies, the network device shall provide the capability to enforce a security policy for the usage of mobile code technologies. The security policy shall allow, at a minimum, the following actions for each mobile code technology used on the network device:

a) Control execution of mobile code;

b) Control which users (human, software process, or device) are allowed to transfer mobile code to/from the network device; and

c) Control the code execution based upon integrity checks on mobile code and prior to the code being executed

15.4.2 Rationale and supplemental guidance

Mobile code technologies include, but are not limited to, Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations and VBScript. Usage restrictions apply to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations. Control procedures should prevent the development, acquisition or introduction of unacceptable mobile code within the control system in which the component resides. For example, mobile code exchanges may be disallowed directly within the control system but may be allowed in a controlled adjacent environment maintained by IACS personnel.

Mobile code could be secured by adding integrity, authenticity, and authorization checks to the code itself (application layer), or for “just-in-time” code execution through transmitting the mobile code via a secure communications tunnel which provides these attributes, or any mechanism equivalent to these options.

15.4.3 Requirement enhancements

(1) Mobile code authenticity check

The network device shall provide the capability to enforce a security policy that allows the device to control execution of mobile code based on the results of an authenticity check prior to the code being executed

15.4.4 Security levels

The requirements for the four SL levels that relate to NDR 2.4 are:

- SL-C(UC, component) 1: NDR 2.4
- SL-C(UC, component) 2: NDR 2.4(1)

- SL-C(UC, component) 3: NDR 2.4 (1)
- SL-C(UC, component) 4: NDR 2.4 (1)

15.5 NDR 2.13 – Use of physical diagnostic and test interfaces

15.5.1 Requirement

Network devices shall protect against unauthorized use of the physical factory diagnostic and test interface(s) (e.g. JTAG debugging).

15.5.2 Rationale and supplemental guidance

Factory diagnostic and test interface(s) are created at various locations within the component to assist the component's developers and factory personnel as they test the functional implementation, and when errors are discovered to subsequently remove them from the component. However, these same interfaces must be carefully protected from access by unauthorized entities to protect the essential functionality provided by the component to the IACS.

There may be cases where the factory diagnostic and test interface(s) use network communications with the device. When this is the case those interfaces are to be subjected to all of the requirements of this document.

Note that if a diagnostic and test interface does not provide the ability to control the product, or to access non-public information, then it will not need an authentication mechanism. This should be determined via a threat assessment. An example of this would be JTAG debugging, in which JTAG is used to take control of the processor and execute arbitrary commands, versus a JTAG boundary scan where JTAG is used to simply read information (which may be publicly available information).

15.5.3 Requirement enhancements

(1) Active monitoring

Network devices shall provide active monitoring of the device's diagnostic and test interface(s) and generate an audit log entry when attempts to access these interface(s) are detected.

15.5.4 Security levels

The requirements for the four SL levels that relate to NDR 2.13 are:

- SL-C(SI, component) 1: Not Selected
- SL-C(SI, component) 2: NDR 2.13
- SL-C(SI, component) 3: NDR 2.13 (1)
- SL-C(SI, component) 3: NDR 2.13 (1)

15.6 NDR 3.2 – Protection from malicious code

15.6.1 Requirement

The network device shall provide for protection from malicious code.

15.6.2 Rationale and supplemental guidance

If a network device is able to utilize a compensating control, it need not directly support protection from malicious code. One such possible compensating control would be the use of network packet filtering devices to identify and remove malicious code while in transit. It is assumed that the IACS will be responsible for providing the required safeguards. However, for scenarios such as having a local USB host access, the need for protection from malicious code should be evaluated.

15.6.3 Requirement enhancements

None

15.6.4 Security levels

The requirements for the four SL levels that relate to NDR 3.2 are:

- SL-C(SI, component) 1: NDR 3.2
- SL-C(SI, component) 2: NDR 3.2
- SL-C(SI, component) 3: NDR 3.2
- SL-C(SI, component) 4: NDR 3.2

15.7 NDR 3.10 – Support for updates

15.7.1 Requirement

Network devices shall support the ability to be updated and upgraded.

15.7.2 Rationale and supplemental guidance

Network devices over their installed lifetime may require installation of updates and upgrades. There will be cases where network devices are supporting or executing essential functions as well. When this is the case the network device should have mechanisms in place to support patching and updating without impacting the essential functions of high availability systems (see 4.2 CCSC 1 Support of essential functions). One example for providing this capability would be to support redundancy within the network device.

15.7.3 Requirement enhancements

(1) Update authenticity and integrity

Network devices shall validate the authenticity and integrity of any software update or upgrade prior to installation.

15.7.4 Security levels

The requirements for the four SL levels that relate to NDR 3.10 are:

- SL-C(SI, component) 1: NDR 3.10
- SL-C(SI, component) 2: NDR 3.10 (1)
- SL-C(SI, component) 3: NDR 3.10 (1)
- SL-C(SI, component) 4: NDR 3.10 (1)

15.8 NDR 3.11 – Physical tamper resistance and detection

15.8.1 Requirement

Network devices shall provide tamper resistance and detection mechanisms to protect against unauthorized physical access into the device

15.8.2 Rationale and supplemental guidance

The purpose of tamper resistance mechanisms is to prevent an attempt by an attacker to execute an unauthorized physical action against an IACS device. Secondary to prevention, detection and response are essential should a tampering event occur.

Tamper resistance mechanisms are most effectively used in combinations to prevent access to any critical components. Tamper resistance consists of using specialized materials to make tampering of a device or module difficult. This can include such features as hardened enclosures, locks, encapsulation, or security screws. Putting in place tight airflow paths will increase the difficulty of probing the product internals.

The purpose of tamper evidence is to ensure that visible or electronic evidence remains when a tampering event occurs. Many simple evidence techniques are comprised of seals and tapes to

make it obvious that there has been physical tampering. More sophisticated techniques include switches.

15.8.3 Requirement enhancements

(1) Notification of a tampering attempt

Network devices shall be capable of automatically providing notification to a configurable set of recipients upon discovery of an attempt to make an unauthorized physical access. All notifications of tampering shall be logged as part of the overall audit logging function.

15.8.4 Security levels

The requirements for the four SL levels that relate to NDR 3.11 are:

- SL-C(SI, component) 1: Not Selected
- SL-C(SI, component) 2: NDR 3.11
- SL-C(SI, component) 3: NDR 3.11 (1)
- SL-C(SI, component) 4: NDR 3.11 (1)

15.9 NDR 3.12 – Provisioning product supplier roots of trust

15.9.1 Requirement

Network devices shall provide the capability to provision and protect the confidentiality, integrity, and authenticity of product supplier keys and data to be used as one or more “roots of trust” at the time of manufacture of the device.

15.9.2 Rationale and supplemental guidance

In order for a component to be able to validate the authenticity and integrity of the hardware, software, and data provided by the product supplier, it must possess a trusted source of data to perform the validation process. This trusted source of data is referred to as the “root of trust” for the system. This trusted source of data may be a set of cryptographic hashes of “known good” software, or it may be the public portion of an asymmetric cryptographic key pair to be used in the validation of cryptographic signatures. This trusted data is often used to validate critical software, firmware, and data prior to booting the firmware or operating system of a component, in order to validate that the component will boot into a “known good” state in which all security mechanisms are known to be operational and uncompromised. “Root of trust” data is often protected by software or hardware implemented mechanisms to prevent any modification of the data during normal operations of the component. Modification of product supplier root of trust data is typically limited to the product supplier’s provisioning process, where the product supplier has a trusted process to perform the provisioning of the data. Instead, information to be validated against the root of trust is submitted to the validation process through a hardware or software API which performs the validation and returns the results without exposing the protected data.

15.9.3 Requirement Enhancements

None

15.9.4 Security levels

The requirements for the four SL levels that relate to NDR 3.12 are:

- SL-C(SI, component) 1: Not Selected
- SL-C(SI, component) 2: NDR 3.12
- SL-C(SI, component) 3: NDR 3.12
- SL-C(SI, component) 3: NDR 3.12

15.10 NDR 3.13 – Provisioning asset owner roots of trust

15.10.1 Requirement

Network devices shall

a) provide the capability to provision and protect the confidentiality, integrity, and authenticity of asset owner keys and data to be used as “roots of trust”; and

b) support the capability to provision without reliance on components that may be outside of the device’s security zone.

15.10.2 Rationale and supplemental guidance

Product suppliers have established mechanisms to ensure that the software and firmware on their components is authentic, and the integrity of that software and firmware has not been compromised. This allows the product supplier to provide the asset owner with a “known good” state from which to operate. However, many product suppliers also provide mechanisms for asset owners to extend the functionality of their devices through the use of mobile code, user programs, or other such means. In order to protect the security of the component, it is important that these extensions to the component’s functionality also be validated to ensure that they are authorized, and that the asset owner has approved of their origins.

In order to perform these validations the component must contain data that provides a way to differentiate between valid and invalid origins. The list of valid and invalid origins will differ from asset owner to asset owner, and it is unlikely that a product supplier will have a complete list of every possible valid origin at time of manufacture. Therefore it is important that the product supplier provide a way for the asset owner to securely provision their own “roots of trust” which provide the ability to distinguish between origins allowed by the asset owner’s security policy, and those that are not. The authenticity and integrity of these “roots of trust” must be protected so that malicious actors cannot add additional roots of trust that grant them the ability to operate on the component.

Requirements such as NDR 2.4 – Mobile coderequire the component to complete authenticity checks on mobile code prior to the execution of mobile code. The roots of trust provided by this requirement provide the data necessary to validate the origin and integrity of mobile code, allowing the component to independently determine if the code is allowed to execute.

A root of trust is used to provide communications security, such as communications integrity required by CR 3.1 – Communication integrity or communications confidentiality required by CR 4.1 – Information confidentiality.

15.10.3 Requirement Enhancements

None

15.10.4 Security levels

The requirements for the four SL levels that relate to NDR 3.13 are:

- SL-C(SI, component) 1: Not Selected
- SL-C(SI, component) 2: NDR 3.13
- SL-C(SI, component) 3: NDR 3.13
- SL-C(SI, component) 4: NDR 3.13

15.11 NDR 3.14 – Integrity of the boot process

15.11.1 Requirement

Network devices shall verify the integrity of the firmware, software, and configuration data needed for component's boot process prior to it being used in the boot process.

15.11.2 Rationale and supplemental guidance

In order to make assurances to an asset owner that a component's security functionality has not been compromised, it is necessary to ensure that the component's software and firmware has not been tampered with, and that the software and firmware is valid to execute on the component. Therefore the component must perform checks to validate the integrity and authenticity of the component's firmware and/or software prior to the boot process, to ensure that the component does not boot into an insecure or invalid operating state that could damage the component or provide a path for a malicious actor to gain access to additional components, assets, or data.

15.11.3 Requirement enhancements

(1) Authenticity of the boot process

Network devices shall use the component's product supplier roots of trust to verity the authenticity of the firmware, software, and configuration data needed for component's boot process prior to it being used in the boot process.

15.11.4 Security levels

The requirements for the four SL levels that relate to NDR 3.14 are:

- SL-C(SI, component) 1: NDR 3.14
- SL-C(SI, component) 2: NDR 3.14 (1)
- SL-C(SI, component) 3: NDR 3.14 (1)
- SL-C(SI, component) 4: NDR 3.14 (1)

15.12 NDR 5.2 – Zone boundary protection

15.12.1 Requirement

A network device at a zone boundary shall provide the capability to monitor and control communications at zone boundaries to enforce the compartmentalization defined in the risk-based zones and conduits model.

15.12.2 Rationale and supplemental guidance

Any connections to outside each security zone should occur through managed interfaces consisting of appropriate boundary protection devices (for example, proxies, gateways, routers, firewalls, unidirectional gateways, guards and encrypted tunnels) arranged in an effective architecture (for example, firewalls protecting application gateways residing in a DMZ). Control system boundary protections at any designated alternate processing sites should provide the same levels of protection as that of the primary site.

15.12.3 Requirement enhancements

(1) Deny all, permit by exception

The network component shall provide the capability to deny network traffic by default and allow network traffic by exception (also termed deny all, permit by exception).

(2) Island mode

The network component shall provide the capability to protect against any communication through the control system boundary (also termed island mode).

NOTE Examples of when this capability may be used include where a security violation and/or breach has been detected within the control system, or an attack is occurring at the enterprise level.

(3) Fail close

The network component shall provide the capability to protect against any communication through the control system boundary when there is an operational failure of the boundary protection mechanisms (also termed fail close).

NOTE Examples of when this capability may be used include scenarios where a hardware failure or power failure causes boundary protection devices to function in a degraded mode or fail entirely.

15.12.4 Security levels

The requirements for the four SL levels that relate to NDR 5.2 are:

- SL-C(SI, component) 1: NDR 5.2
- SL-C(SI, component) 2: NDR 5.2 (1)
- SL-C(SI, component) 3: NDR 5.2 (1) (2) (3)
- SL-C(SI, component) 4: NDR 5.2 (1) (2) (3)

15.13 NDR 5.3 – General purpose, person-to-person communication restrictions

15.13.1 Requirement

A network device at a zone boundary shall provide the capability to protect against general purpose, person-to-person messages from being received from users or systems external to the control system.

15.13.2 Rationale and supplemental guidance

General purpose, person-to-person communications systems include but are not limited to: email systems, forms of social media (Twitter, Facebook, picture galleries, etc.) or any message systems that permit the transmission of any type of executable file. These systems are usually utilized for private purposes that are not related to control system operations, and therefore the risks imposed by these systems normally outweigh any perceived benefit.

These types of general purpose communications systems are commonly used as attack vectors to introduce malware to the control system, pass information for which read authorization exists to locations external to the control system and introduce excessive network loading that can be used to create security problems or launch attacks on the control system.

Network devices could realize such restrictions, for example, by blocking specific communications based on port numbers and source and/or target address as well as more in depth checks by application layer firewalls.

15.13.3 Requirement enhancements

None

15.13.4 Security levels

The requirements for the four SL levels that relate to NDR 5.3 are:

- SL-C(SI, component) 1: NDR 5.3
- SL-C(SI, component) 2: NDR 5.3
- SL-C(SI, component) 3: NDR 5.3
- SL-C(SI, component) 4: NDR 5.3

This page intentionally left blank.

Annex A
(informative)
Device categories

A.1 Device categories

The devices described in these categories are intended as representative samples for each category, and not an exhaustive list.

A.1.1 Device category: embedded device

A.1.1.1 Programmable Logic Controller (PLC) (expanded from the Electropedia definition 351-32-34 [19])

The term PLC is commonly used in the process and discrete manufacturing industries. A PLC is a device that typically resides on the lower levels of the automation system (such as level 1 and 2 of the Purdue Enterprise Reference Architecture in ANSI/ISA-95.00.01 [22]). PLCs commonly use ruggedized hardware to allow for operation in industrial environments and are commonly based on commercial real-time operating systems (RTOS). Increasingly Smart sensor and actuators are also receiving forms of process control capability. PLCs and smart sensor/actuators are programmed to execute control logic based on inputs from the process (obtained from instrumentation like traditional temperature sensors, pressure sensors, vibration sensors, etc.). The control logic's output is used to control the industrial process (through actuators such as valves, pumps, etc.). The programming is usually done using engineering software commonly run on host devices (for example, laptops or PC workstations). A common programming language for control logic is IEC 61131-3, *Programmable controllers – Part 3: Programming languages* [20]. In larger systems, PLCs often also communicate the process conditions as obtained from sensors to higher-level servers and/or operator workstations and receive instructions from higher-level control functions or operator workstations, which are translated into or forwarded as commands to actuators. For the communication to higher-level functions such as control servers or operator workstations, modern PLCs use Ethernet and Transmission Control Protocol (TCP)/Internet Protocol (IP)-based protocols, while for the communication to the instrumentation commonly industry standard fieldbuses are used (some of which are also available on Ethernet carriers, but usually don't use the TCP/IP stack). Special PLCs are used for executing safety functions which ensure that the process under control remains within the bounds of safe operation at all times. PLCs, especially executing safety functions, should meet hard real-time and high integrity and availability requirements.

A.1.1.2 Intelligent electronic device (expanded from the definition in IEC TR 61850-1:2013, *Communication networks and systems for power utility automation – Part 1: Introduction and overview* [21])

An intelligent electronic device (IED) is conceptually very similar to a PLC, but the term is more commonly used in power systems (specifically substation automation). An IED receives measurements from the power equipment (for example, transformers, switches and circuit breakers) and executes control logic or protection functions. Similar to PLCs, IEDs are commonly programmed and parameterized using engineering software commonly run on host devices (for example laptops and PC workstations). A modern standard way of describing the configuration of IEDs and their functions is defined in the IEC 61850 standard. The output of the logic executed by IEDs is transmitted to actuators (switches, circuit breakers, etc.). As opposed to PLCs, IEDs commonly also have a HMI which allows a human user standing in front of the IED to use the IED's functionality (often a subset necessary to support essential functions). Also, substations, and therefore the IEDs used therein, have to be able to operate in complete isolation (such as without any communication to higher-level systems outside the substation or even without any communication to other IEDs or station-level workstations or servers). Modern IEDs usually use Ethernet and TCP/IP-based protocols to communicate to higher-level components, while communication to other IEDs may be done using Ethernet-based protocols (in some cases TCP/IP-

based, often directly on Ethernet) or fieldbuses (some of which are available also on Ethernet carriers, but don't use the TCP/IP stack). Similar to PLCs, IEDs should meet hard real-time and high integrity and availability requirements.

A.1.2 Device category: network device

A.1.2.1 Switch (expanded from Electropedia definition 732-01-22)

A switch is a device in computer networks that links multiple network segments or network nodes together. A switch typically is located at layer 2 (data link layer) of the OSI model (see ISO/IEC 7498-1 [14]). Modern switches, especially those designed for use in larger networks, typically provide interfaces for configuration management and network management. These interfaces may support the configuration of the switch (for example web-based via HTTP/HTTPS, file-based via FTP/SFTP, command-line-based via SSH or via simple network management protocol (SNMP)) as well as log and event management (for example via syslog).

A.1.2.2 Virtual Private Network (VPN) terminator (expanded from Electropedia definition 732-01-10)

Virtual private networks are logical networks that allow for the extension of private networks across distances that are bridged by public networks. The use of the public network to cover the distance is transparent/invisible to the VPN users. VPNs are established by creating a logical tunnel at the border of the two segments of the private network. The tunnel is established by VPN terminators, which are devices located at the network border. The data packets from one segment are encapsulated (commonly also encrypted) at the VPN terminator at then sent through a public network to the peer VPN terminator. There, the encapsulation is removed (usually involving decryption) and the original packet is recovered and forwarded into the local network segment. VPNs are also often used to allow roaming users secure access to resources on their home network. In this scenario, a client software on the roaming device acts as a local VPN terminator, encapsulating (and usually encrypting) all data packets and forwarding them to the VPN terminator on the home network border. Establishment of the tunnel between VPN terminators should be authenticated, which, in the scenario of roaming users, typically is a user-based authentication. Hence, VPN terminators may be used to collect data about roaming users, which may allow tracing their location and other privacy related data.

A.1.3 Device category: host device/application

A.1.3.1 Operator workstation

Operator workstations are used in control systems to display process information to human users or operators and to allow them to interact with the control system (for example initiate operational actions on the process, such as opening a valve, closing a switch, modifying process set points, etc.). Depending on the respective operational requirements, operator workstations are often required to be continuously available (at least a minimum set of workstations out of all installed ones) to allow for an uninterrupted view of the process conditions and the opportunity to interact with the process immediately, if necessary. In order to obtain the data to be displayed and to send the commands issued by the human user, operator workstations typically communicate with control servers and connectivity servers in the control systems, sometimes they also directly communicate with PLCs. This communication is commonly using Ethernet and TCP/IP-based protocols. Operator workstations typically do not have to meet hard-real time requirements but have high integrity and (at least as a set of operator workstations) high availability requirements. They are typically built from COTS PC hardware and run COTS client operating systems.

A.1.3.2 Data historian

Data historians are used in control systems to collect and maintain long-term process history data. This data is commonly collected from control servers or directly from PLCs using protocols based on Ethernet and TCP/IP. The data may be used in a variety of analyses, for example, for process optimization or performance reporting but may also be used in reporting to regulatory entities such as emission reporting or documentation of the product's production process integrity (for example,

as required by the US Food and Drug Administration (FDA) regulations for pharmaceutical products). They are typically built from COTS PC/server hardware and run COTS client/server operating systems. Data is commonly stored using COTS database products. Communication to data access clients and data sources is commonly using TCP/IP-based protocols. Depending on the criticality of the process history from a business perspective, data historians have moderate availability and integrity requirements and typically no hard real-time requirements.

This page intentionally left blank.

Annex B
(informative)
Mapping of CRs and REs to FR SLs 1-4

B.1 Overview

This annex is intended to provide overall guidance to the reader as to how SL levels 0 to 4 are differentiated on an FR-by-FR basis via the defined CRs and their associated REs.

B.2 SL mapping table

Table B.1 indicates which component level requirements apply to which FRs for a given component security level capability SL – SL-C(xx, component). For a given FR, the required component level requirements to meet a given SL-C are denoted by a check mark.

As an example, to achieve SL-1 in FR 7, a component must satisfy the base requirements of CRs 7.1 through 7.7. Note that satisfying CR 7.8 is not necessary to meet SL-1 because it is not selected until SL-2 and higher security levels. Meeting SL-1 in this way is also denoted SL-C(RA, component) = 1, to indicate that the component has a capability security level of 1 in Resource Availability, or Foundational Requirement 7.

To meet SL-2 in FR 7, or SL-C(RA, component) = 2, a component must satisfy all requirements from SL-1, and additionally satisfy CR 7.1 RE(1), CR 7.3 RE(1), and the base requirement for CR 7.8. Similarly, to meet SL-3 in FR 7, or SL-C (RA, component) = 3, a component must satisfy all requirements from SL-2, and additionally satisfy CR 7.6 RE(1).

To meet SL-4 in FR7, or SL-C(RA, component) = 4, a component must satisfy all requirements from SL-3. There are no base requirements or requirement enhancements in FR 7 that are unique to SL-4, and thus all components which meet SL-3 also inherently meet SL-4.

Refer to ISA-62443-3-3:2013 Annex A for how a full SL vector that includes all foundational requirements would be denoted.

For clarification the following acronyms are used in the table:

- CR – Component requirement which is common to all types of components
- SAR – Software application requirement
- EDR – Embedded device requirement
- HDR – Host device requirement
- NDR – Network device requirement

Table B.1 – Mapping of CRs and REs to FR SL levels 1-4

SRs and Res	SL 1	SL 2	SL 3	SL 4
FR 1 – Identification and authentication control (IAC)				
CR 1.1 – Human user identification and authentication	✓	✓	✓	✓
RE (1) Unique identification and authentication:		✓	✓	✓
RE (2) Multifactor authentication for all interfaces			✓	✓

Table B.1 (cont'd) – Mapping of SRs and REs to FR SL levels 1-4

SRs and Res	SL 1	SL 2	SL 3	SL 4
CR 1.2 – Software process and device identification and authentication		✓	✓	✓
RE (1) Unique identification and authentication			✓	✓
CR 1.3 – Account management	✓	✓	✓	✓
CR 1.4 – Identifier management	✓	✓	✓	✓
CR 1.5 – Authenticator management	✓	✓	✓	✓
RE (1) Hardware security for authenticators			✓	✓
NDR 1.6 – Wireless access management	✓	✓	✓	✓
RE (1) Unique identification and authentication		✓	✓	✓
CR 1.7 – Strength of password-based authentication	✓	✓	✓	✓
RE (1) Password generation and lifetime restrictions for human users			✓	✓
RE (2) Password lifetime restrictions for all users (human, software process, or device)				✓
CR 1.8 – Public key infrastructure certificates		✓	✓	✓
CR 1.9 – Strength of public key-based authentication		✓	✓	✓
RE (1) Hardware security for public key-based authentication			✓	✓
CR 1.10 – Authenticator feedback	✓	✓	✓	✓
CR 1.11 – Unsuccessful login attempts	✓	✓	✓	✓
CR 1.12 – System use notification	✓	✓	✓	✓
NDR 1.13 – Access via untrusted networks	✓	✓	✓	✓
RE (1) Explicit access request approval			✓	✓
CR 1.14 – Strength of symmetric key-based authentication		✓	✓	✓
RE (1) Hardware security for symmetric key-based authentication			✓	✓
FR 2 – Use control (UC)				
CR 2.1 – Authorization enforcement	✓	✓	✓	✓

Table B.1 (cont'd) – Mapping of SRs and REs to FR SL levels 1-4

SRs and Res	SL 1	SL 2	SL 3	SL 4
RE (1) Authorization enforcement for all users (humans, software processes and devices)		✓	✓	✓
RE (2) Permission mapping to roles		✓	✓	✓
RE (3) Supervisor override			✓	✓
RE (4) Dual approval				✓
CR 2.2 – Wireless use control	✓	✓	✓	✓
CR 2.3 – Use control for portable and mobile devices				
SAR 2.4 – Mobile code	✓	✓	✓	✓
RE (1) Mobile code authenticity check		✓	✓	✓
EDR 2.4 – Mobile code	✓	✓	✓	✓
RE (1) Mobile code authenticity check		✓	✓	✓
HDR 2.4 – Mobile code	✓	✓	✓	✓
RE (1) Mobile code authenticity check		✓	✓	✓
NDR 2.4 – Mobile code	✓	✓	✓	✓
RE (1) Mobile code authenticity check		✓	✓	✓
CR 2.5 – Session lock	✓	✓	✓	✓
CR 2.6 – Remote session termination		✓	✓	✓
CR 2.7 – Concurrent session control			✓	✓
CR 2.8 – Auditable events	✓	✓	✓	✓
CR 2.9 – Audit storage capacity	✓	✓	✓	✓
RE (1) Warn when audit record storage capacity threshold reached			✓	✓
CR 2.10 – Response to audit processing failures	✓	✓	✓	✓
CR 2.11 – Timestamps	✓	✓	✓	✓
RE (1) Time synchronization		✓	✓	✓
RE (2) Protection of time source integrity				✓

Table B.1 (cont'd) – Mapping of SRs and REs to FR SL levels 1-4

SRs and Res	SL 1	SL 2	SL 3	SL 4
CR 2.12 – Non-repudiation	✓	✓	✓	✓
RE (1) Non-repudiation for all users				✓
EDR 2.13 – Use of physical diagnostic and test interfaces		✓	✓	✓
RE (1) Active monitoring			✓	✓
HDR 2.13 – Use of physical diagnostic and test interfaces		✓	✓	✓
RE (1) Active monitoring			✓	✓
NDR 2.13 – Use of physical diagnostic and test interfaces		✓	✓	✓
RE (1) Active monitoring			✓	✓
FR 3 – System integrity (SI)				
CR 3.1 – Communication integrity	✓	✓	✓	✓
RE (1) Communication authentication		✓	✓	✓
SAR 3.2 – Protection from malicious code	✓	✓	✓	✓
EDR 3.2 – Protection from malicious code	✓	✓	✓	✓
HDR 3.2 – Protection from malicious code	✓	✓	✓	✓
RE (1) Report version of code protection		✓	✓	✓
NDR 3.2 – Protection from malicious code	✓	✓	✓	✓
CR 3.3 – Security functionality verification	✓	✓	✓	✓
RE (1) Security functionality verification during normal operation				✓
CR 3.4 – Software and information integrity	✓	✓	✓	✓
RE (1) Authenticity of software and information		✓	✓	✓
RE (2) Automated notification of integrity violations			✓	✓
CR 3.5 – Input validation	✓	✓	✓	✓
CR 3.6 – Deterministic output	✓	✓	✓	✓
CR 3.7 – Error handling	✓	✓	✓	✓

Table B.1 (cont'd) – Mapping of SRs and REs to FR SL levels 1-4

SRs and Res	SL 1	SL 2	SL 3	SL 4
CR 3.8 – Session integrity		✓	✓	✓
CR 3.9 – Protection of audit information		✓	✓	✓
RE (1) Audit records on write-once media				✓
EDR 3.10 – Support for updates	✓	✓	✓	✓
RE (1) Update authenticity and integrity		✓	✓	✓
HDR 3.10 – Support for updates	✓	✓	✓	✓
RE (1) Update authenticity and integrity		✓	✓	✓
NDR 3.10 – Support for updates	✓	✓	✓	✓
RE (1) Update authenticity and integrity		✓	✓	✓
EDR 3.11 – Physical tamper resistance and detection		✓	✓	✓
RE (1) Notification of a tampering attempt			✓	✓
HDR 3.11 – Physical tamper resistance and detection		✓	✓	✓
RE (1) Notification of a tampering attempt			✓	✓
NDR 3.11 – Physical tamper resistance and detection		✓	✓	✓
RE (1) Notification of a tampering attempt			✓	✓
EDR 3.12 – Provisioning product supplier roots of trust		✓	✓	✓
HDR 3.12 – Provisioning product supplier roots of trust		✓	✓	✓
NDR 3.12 – Provisioning product supplier roots of trust		✓	✓	✓
EDR 3.13 – Provisioning asset owner roots of trust		✓	✓	✓
HDR 3.13 – Provisioning asset owner roots of trust		✓	✓	✓
NDR 3.13 – Provisioning asset owner roots of trust		✓	✓	✓
EDR 3.14 – Integrity of the boot process	✓	✓	✓	✓
RE (1) Authenticity of the boot process		✓	✓	✓
HDR 3.14 – Integrity of the boot process	✓	✓	✓	✓

Table B.1 (cont'd) – Mapping of SRs and REs to FR SL levels 1-4

SRs and Res	SL 1	SL 2	SL 3	SL 4
RE (1) Authenticity of the boot process		✓	✓	✓
NDR 3.14 – Integrity of the boot process	✓	✓	✓	✓
RE (1) Authenticity of the boot process		✓	✓	✓
FR 4 – Data confidentiality (DC)				
CR 4.1 – Information confidentiality	✓	✓	✓	✓
CR 4.2 – Information persistence		✓	✓	✓
RE (1) Erase of shared memory resources			✓	✓
RE (2) Erase verification			✓	✓
CR 4.3 – Use of cryptography	✓	✓	✓	✓
FR 5 – Restricted data flow (RDF)				
CR 5.1 – Network segmentation	✓	✓	✓	✓
NDR 5.2 – Zone boundary protection	✓	✓	✓	✓
RE (1) Deny all, permit by exception		✓	✓	✓
RE (2) Island mode			✓	✓
RE (3) Fail close			✓	✓
NDR 5.3 – General purpose, person-to-person communication restrictions	✓	✓	✓	✓
FR 6 – Timely response to events (TRE)				
CR 6.1 – Audit log accessibility	✓	✓	✓	✓
RE (1) Programmatic access to audit logs			✓	✓
CR 6.2 – Continuous monitoring		✓	✓	✓
FR 7 – Resource availability (RA)				
CR 7.1 – Denial of service protection	✓	✓	✓	✓
RE (1) Manage communication load from component		✓	✓	✓
CR 7.2 – Resource management	✓	✓	✓	✓
CR 7.3 – Control system backup	✓	✓	✓	✓
RE (1) Backup integrity verification		✓	✓	✓

Table B.1 (cont'd) – Mapping of SRs and REs to FR SL levels 1-4

SRs and Res	SL 1	SL 2	SL 3	SL 4
CR 7.4 – Control system recovery and reconstitution	✓	✓	✓	✓
CR 7.5 - Emergency Power				
CR 7.6 – Network and security configuration settings	✓	✓	✓	✓
RE (1) Machine-readable reporting of current security settings			✓	✓
CR 7.7 – Least functionality	✓	✓	✓	✓
CR 7.8 – Control system component inventory		✓	✓	✓

BIBLIOGRAPHY

NOTE 1 This bibliography includes references to sources used in the creation of this document as well as references to sources that may aid the reader in developing a greater understanding of cyber security as a whole and developing a management system. Not all references in this bibliography are referred to throughout the text of this document. The references have been broken down into different categories depending on the type of source they are.

References to other parts, both existing and anticipated, of the ISA-62443 series:

NOTE 2 Some of these references are normative references (see Clause 2), published documents, in development, or anticipated. They are all listed here for completeness of the currently authorized parts of the ISA-62443 series.

[1] ANSI/ISA-62443-1-1, *Security for industrial automation and control systems, Part 1-1: Concepts and models*[3]

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

[3] ISA-62443-1-3, *Security for industrial automation and control systems, Part 1-3: System security conformance metrics*

[4] ISA-TR62443-1-4, *Security for industrial automation and control systems, Part 1-4: IACS security life-cycle and use-cases*

[5] ANSI/ISA-62443-2-1, *Security for industrial automation and control systems, Part 2-1: Requirements for an IACS security management system*[3]

[6] ISA-TR62443-2-2, *Security for industrial automation and control systems, Part 2-2: Implementation guidance for an IACS security management system*

[7] ANSI/ISA-TR62443-2-3, *Security for industrial automation and control systems, Part 2-3: Patch management in the IACS environment*

[8] ANSI/ISA-62443-2-4, *Security for industrial automation and control systems, Part 2-4: Requirements for IACS solution suppliers*

[9] ISA-TR62443-3-1, *Security for industrial automation and control systems, Part 3-1: Security technologies for IACS*[3]

[10] ISA-62443-3-2, *Security for industrial automation and control systems, Part 3-2: Security risk assessment and system design*

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

[12] ANSI/ISA-62443-4-1, *Security for industrial automation and control systems, Part 4-1: Product development requirements*

NOTE 3 This document is ANSI/ISA-62443-4-2, *Security for industrial automation and control systems: Part 4-2, Technical security requirements and for IACS components*

Other standards references:

[13] ISO/IEC Directives, *Part 2, Rules for the structure and drafting of ISO and IEC documents*

———————

[3] Currently under revision.

[14] ISO/IEC 7498-1:1994, *Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model*

[15] ISO 8601:2004, *Data elements and interchange formats – Information interchange – Representation of dates and times*

[16] ISO/IEC 15408-1:2009, *Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model*

[17] ISO/IEC 19790, *Information technology – Security techniques – Security requirements for cryptographic modules*

[18] ISO/IEC 27002:2013, *Information technology – Security techniques – Code of practice for information security controls*

[19] IEC 60050, *International Electrotechnical Vocabulary*, or *Electropedia*

[20] IEC 61131-3, *Programmable controllers – Part 3: Programming languages*

[21] IEC TR 61850-1:2013, *Communication networks and systems for power utility automation – Part 1: Introduction and overview*

[22] ANSI/ISA-95.00.01-2010 (IEC 62264-1 Mod) *Enterprise-Control System Integration – Part 1: Models and Terminology*

[23] ISO/IEC 11889-1:2015, Trusted platform module library – Part1: Architecture

Other documents and published resources:

[24] FIPS 140-2, *Security Requirements for Cryptographic Modules*

[25] NIST SP 800-57, *Recommendation for Key Management, Part 1: General*

[26] NIST SP 800-92, *Guide to Computer Security Log Management*

[27] NIST SP800-63-2, *Electronic Authentication Guideline*

Websites:

[28] OWASP Code Review Guide, available at https://www.owasp.org/index.php/Code_Review_Guide

This page intentionally left blank.

Developing and promulgating technically sound consensus standards and recommended practices is one of ISA's primary goals. To achieve this goal the Standards and Practices Department relies on the technical expertise and efforts of volunteer committee members, chairmen, and reviewers. ISA is an American National Standards Institute (ANSI) accredited organization. ISA administers United States Technical Advisory Groups (USTAGs) and provides secretariat support for International Electrotechnical Commission (IEC) and International Organization for Standardization (ISO) committees that develop process measurement and control standards. To obtain additional information on the Society's standards program, please write:

ISA

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

ISBN: 978-1-64331-025-1