Standards
Certification
Education & Training
Publishing
Conferences & Exhibits

Setting the Standard for Automation™

AMERICAN NATIONAL STANDARD

ANSI/ISA-62443-3-2-2020

Security for industrial automation and control systems, Part 3-2: Security risk assessment for system design

Approved August 11, 2020

ANSI/ISA-62443-3-2-2020
Security for industrial automation and control systems,
Part 3-2: Security risk assessment for system design

ISBN: 978-1-64331-116-6

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-62443-3-2-2020.

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.

The following people served as active members of ISA99 Working Group 04, Task Group 03 for the preparation of this document:

Name	Company	Contributor	Reviewer
John Cusimano, TG Chair	aeSolutions	X	
Rahul Bhojani, Former TG Chair	BP	X	
Jens Braband	Siemens	X	
Eric Byres	aDolus Inc.		X
Maarten de Caluwé	The Dow Chemical Company	X	
Eric Cosman	OIT Concepts LLC		X
William J. Cotter	3M Co.		X
Ed Crawford	Chevron		X
Paul Didier	Cisco	X	
Bob Evans	Individual	X	
Jim Gilsinn	Kenexis		X
Andrew Ginter	Waterfall		X
Thomas Good	DuPont		X
Vic Hammond	Argonne National Laboratory		X
Jean-Pierre Hauet	KB Intelligence		X
Dennis Holstein	OPUS Consulting Group		X
Eric Hopp	Rockwell		X
Siv Hilde Houmb	Secure-NOK AS	X	
Dave Johnson	Exida	X	
Joel Langill	AECOM		X
John Lellis	Individual	X	
Suzanne Lightman	NIST	X	
Ken Keiser	E&Y	X	
Pierre Kobes	Siemens	X	
Michael Medoff	Exida		X
Kenny Mesker	Chevron	X	
Johan Nye	ICS Guru LLC		X
Bryan Owen	OSISoft Inc.		X
Dennis Parker	Chevron	X	
Michal Paulski	Accenture	X	
Jeff Potter	Independent Consultant	X	
Judith Rossebo	ABB	X	
Ragnar Schierholz	ABB	X	
Omar Sherin	Q-Cert		X
Kevin Staggs	Honeywell		X
Leon C. Steinocher	Redstone Investors		X
Tatsuaki Takebe	Yokogawa		X
Hal Thomas	Exida		X
Ludwig A. Winkel	Siemens		X

This standard was approved for publication by the ISA Standards and Practices Board on August 3, 2020.

NAME	AFFILIATION
C. Monchinski, Vice President	Automated Control Concepts Inc.
D. Bartusiak	ExxonMobil Research & Engineering
D. Brandl	BR&L Consulting
P. Brett	Honeywell Inc.
E. Cosman	OIT Concepts, LLC
D. Dunn	Waldemar S. Nelson & Co.
J. Federlein	Federlein & Assoc LLC
B. Fitzpatrick	Wood PLC
J-P Hauet	Hauet.com
D. Lee	Emerson Automation Solutions
G. Lehmann	AECOM
T. McAvinew	Consultant
V. Mezzano	Fluor Corporation
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
I. Verhappen	Industrial Automation Networks
D. Visnich	Burns & McDonnell
W. Weidman	Consultant
J. Weiss	Applied Control Solutions LLC
M. Wilkins	Yokogawa UK Ltd.
D. Zetterberg	Chevron Energy Technology Company

This page intentionally left blank.

CONTENTS

FOREWORD

This document is part of a multipart standard that addresses the issue of security for industrial automation and control systems. It has been developed by ISA99 Working Group 04, Task Group 03.

This document prescribes the requirements to perform cyber security risk assessment of an IACS in order to inform the organization of the initial risk, residual risk and target security level (SL-T) for the system under consideration (SUC). The standard also prescribes the requirements to utilize the output of the risk assessment to produce a cyber security requirement specification (CRS) to guide system design.

This page intentionally left blank.

INTRODUCTION

There is no simple recipe for how to secure an industrial automation and control system (IACS) and there is good reason for this. It is because security is a matter of risk management. Every IACS presents a different risk to the organization depending upon the threats it is exposed to, the likelihood of those threats arising, the inherent vulnerabilities in the system and the consequences if the system were to be compromised. Furthermore, every organization that owns and operates an IACS has a different tolerance for risk.

This document strives to define a set of engineering measures that will guide an organization through the process of assessing the risk of a particular IACS and identifying and applying security countermeasures to reduce that risk to tolerable levels.

A key concept in this document is the application of IACS security zones and conduits. Zones and conduits are introduced in ISA-62443-1-1. Readers are encouraged to familiarize themselves with these concepts prior to reading this document.

Figure 1 illustrates the relationship of the different parts of ISA-62443 that were in existence or planned as of the date of circulation of this document. Those that are normatively referenced are included as normative references and those that are referenced for informational purposes or that are in development are listed in the Bibliography.

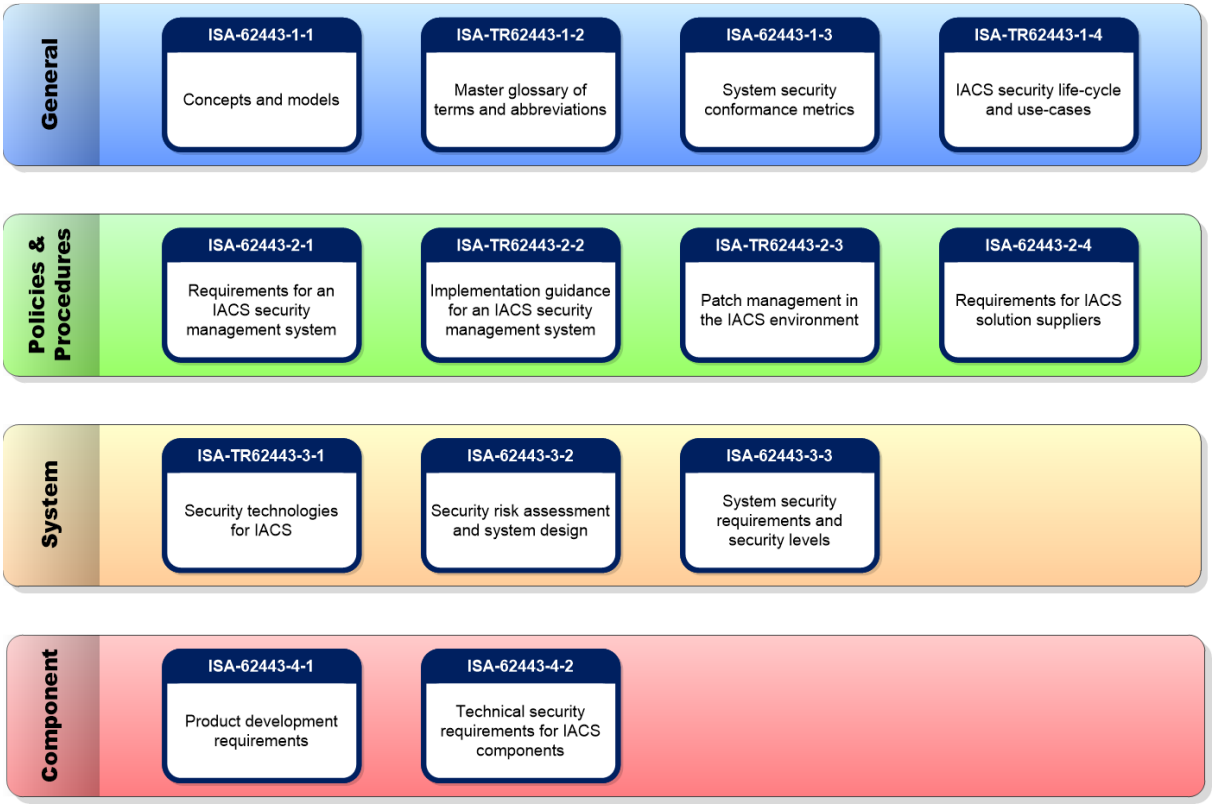

Figure 1 – Parts of the ISA-62443 series

Purpose and intended audience

The audience for this document is intended to include the asset owner, system integrator, product supplier, service provider, and compliance authority.

Usage within other parts of the ISA-62443 series

This document provides a basis for specifying security countermeasures by aligning the target security levels (SL-Ts) identified in this standard with the required capability security levels (SL-Cs) specified in ISA-62443-3-3.

1 Scope

This document establishes requirements for:

- defining a system under consideration (SUC) for an industrial automation and control system (IACS);
- partitioning the SUC into zones and conduits;
- assessing risk for each zone and conduit;
- establishing the target security level (SL-T) for each zone and conduit; and
- documenting the security requirements.

2 Normative references

ISA-62443-1-1, *Security for industrial automation and control systems Part 1-1: Terminology, concepts, and models*

ISA-62443-2-1, *Security for industrial automation and control systems Part 2-1: Establishing an industrial automation and control systems security program*

ISA-62443-3-3, *Security for industrial automation and control systems Part 3-3: System security requirements and security levels*

3 Terms, definitions, abbreviated terms, acronyms and conventions

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions given in ISA-62443-1-2 [1][1] and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at https://www.iso.org/obp
- IEC Electropedia: available at http://www.electropedia.org/

3.1.1
channel
specific logical or physical communication link between assets

Note 1 to entry: A channel facilitates the establishment of a connection.

3.1.2
compliance authority
entity with jurisdiction to determine the adequacy of a security assessment or the effectiveness of implementation as specified in a governing document

Note 1 to entry: Examples of compliance authorities include government agencies, regulators, external and internal auditors.

3.1.3
conduit
logical grouping of communication channels that share common security requirements connecting two or more zones

[1] Numbers in brackets indicate references in the Bibliography.

3.1.4
confidentiality
preservation of authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information

3.1.5
consequence
result of an incident, usually described in terms of health and safety effects, environmental impacts, loss of property, loss of information (for example, intellectual property), and/or business interruption costs, that occurs from a particular incident

3.1.6
countermeasure
action, device, procedure, or technique that reduces a threat, a vulnerability, or the consequences of an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken

Note 1 to entry: The term “control” is also used to describe this concept in some contexts. The term countermeasure has been chosen for this standard to avoid confusion with the word control in the context of “process control.”

3.1.7
cyber security
measures taken to protect a computer or computer system against unauthorized access or attack

Note 1 to entry: IACS are computer systems.

3.1.8
dataflow
movement of data through a system comprised of software, hardware, or a combination of both

3.1.9
external network
network that is connected to the SUC that is not part of the SUC

3.1.10
impact
measure of the ultimate loss or harm associated with a consequence

Note 1 to entry: Impact may be expressed in terms of numbers of injuries and/or fatalities, extent of environmental damage and/or magnitude of losses such as property damage, material loss, loss of intellectual property, lost production, market share loss, and recovery costs.

EXAMPLE: The consequence of the incident was a spill. The impact of the spill was a $100,000 fine and $25,000 in clean-up expenses.

3.1.11
likelihood
chance of something happening

Note 1 to entry: In risk management terminology, the word “likelihood” is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as a probability or a frequency over a given time period).

Note 2 to entry: A number of factors are considered when estimating likelihood in information system risk management such as the motivation and capability of the threat source, the history of similar threats, known vulnerabilities, the attractiveness of the target, etc.

[SOURCE: ISO Guide 73 [15], 3.6.1.1 and ISO/IEC 27005 [14], 3.7]

3.1.12
process hazard analysis
set of organized and systematic assessments of the potential hazards associated with an industrial process

3.1.13
residual risk
risk that remains after existing countermeasures are implemented (such as, the net risk or risk after countermeasures are applied)

3.1.14
risk
expectation of loss expressed as the likelihood that a particular threat will exploit a particular vulnerability with a particular consequence

3.1.15
security level
SL
measure of confidence that the SUC, security zone or conduit is free from vulnerabilities and functions in the intended manner

3.1.16
security perimeter
logical or physical boundary surrounding all the assets that are controlled and protected by the security zone

3.1.17
system under consideration
SUC
defined collection of IACS assets that are needed to provide a complete automation solution. including any relevant network infrastructure assets

Note 1 to entry: An SUC consists of one or more zones and related conduits. All assets within a SUC belong to either a zone or conduit.

3.1.18
threat
circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image or reputation) and/or organizational assets including IACS

Note 1 to entry: Circumstances include individuals who, contrary to security policy, intentionally or unintentionally prevent access to data or cause the destruction, disclosure, or modification of data such as control logic/parameters, protection logic/parameters or diagnostics.

3.1.19
threat environment
summary of information about threats, such as threat sources, threat vectors and trends, that have the potential to adversely impact a defined target (for example, company, facility or SUC)

3.1.20
threat source
intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally exploit a vulnerability

3.1.21
threat vector
path or means by which a threat source can gain access to an asset

3.1.22
tolerable risk
level of risk deemed acceptable to an organization

Note 1 to entry: Organizations should include consideration of legal requirements when establishing tolerable risk. Additional guidance on establishing tolerable risk can be found in ISO 31000 [16] and NIST SP 800-39 [18].

3.1.23
unmitigated cyber security risk
level of cyber security risk that is present in a system before any cyber security countermeasures are considered

Note 1 to entry: This level helps identify how much cyber security risk reduction is required to be provided by any countermeasure.

3.1.24
vulnerability
flaw or weakness in a system's design, implementation or operation and management that could be exploited to violate the system's integrity or security policy

3.1.25
zone
grouping of logical or physical assets based upon risk or other criteria, such as criticality of assets, operational function, physical or logical location, required access (for example, least privilege principles) or responsible organization

Note 1 to entry: Collection of logical or physical assets that represents partitioning of a system under consideration on the basis of their common security requirements, criticality (for example, high financial, health, safety, or environmental impact), functionality, logical and physical (including location) relationship.

3.2 Abbreviated terms and acronyms

This subclause defines the abbreviated terms and acronyms used in this document.

ANSI	American National Standards Institute
BPCS	Basic process control system
CERT	Computer emergency response team
CRS	Cyber security requirements specification
DCS	Distributed control system
HMI	Human machine interface
HSE	Health, safety and environment
HVAC	Heating, ventilation and air-conditioning
IACS	Industrial automation and control system(s)
ICS-CERT	Industrial control system CERT
IEC	International Electrotechnical Commission
IIoT	Industrial Internet of Things
IPL	Independent protection layer
ISA	International Society of Automation
ISAC	Information Sharing and Analysis Centers
ISO	International Organization for Standardization
MES	Manufacturing execution system
NIST	[US] National Institute of Standards and Technology
PHA	Process hazard analysis
PLC	Programmable logic controller

RTU	Remote terminal unit
SCADA	Supervisory control and data acquisition
SIS	Safety instrumented system
SUC	System under consideration
SL	Security level
SL-A	Achieved SL
SL-C	Capability SL
SL-T	Target SL
SP	[US NIST] Special Publication
USB	Universal serial bus
ZCR	Zone and conduit requirement

3.3 Conventions

This document uses flowcharts to illustrate the workflow between requirements. These flowcharts are informative. Alternate workflows may be used.

4 Zone, conduit and risk assessment requirements

4.1 Overview

Clause 4 describes the requirements for partitioning an SUC into zones and conduits as well as the requirements for assessing the cyber security risk and determining the SL-T for each defined zone and conduit. The requirements introduced in this clause are referred to as zone and conduit requirements (ZCR). This clause also provides rationale and supplemental guidance on each of the requirements. Figure 2 is a workflow diagram outlining the primary steps required to establish zones and conduits, as well as to assess risk. The steps are numbered to indicate their relationship to the ZCRs.

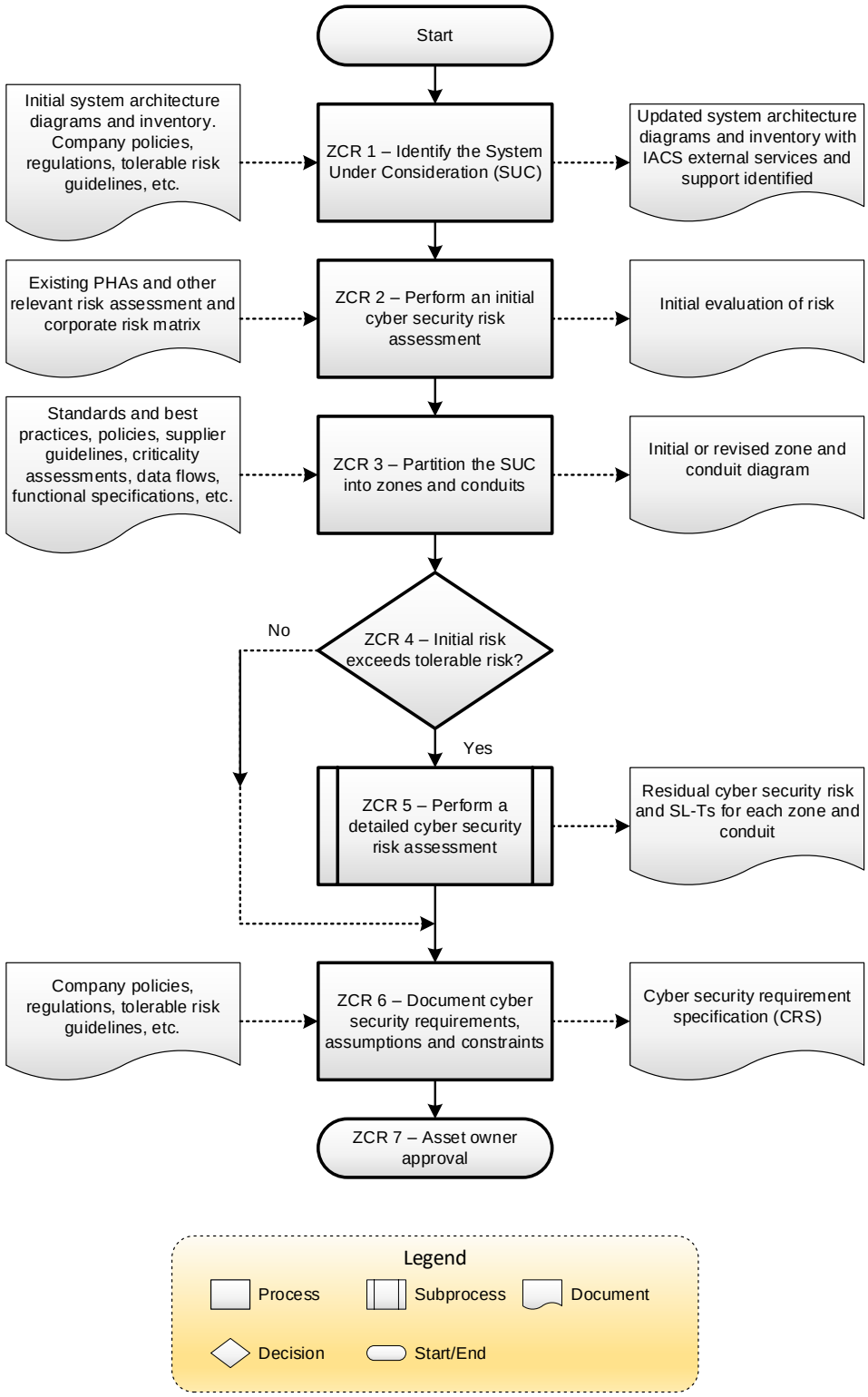

Figure 2 – Workflow diagram outlining the primary steps required to establish zones and conduits, as well as to assess risk

4.2 ZCR 1: Identify the SUC

4.2.1 ZCR 1.1: Identify the SUC perimeter and access points

4.2.1.1 Requirement

The organization shall clearly identify the SUC, including clear demarcation of the security perimeter and identification of all access points to the SUC.

4.2.1.2 Rationale and supplemental guidance

Organizations typically own and operate multiple control systems, especially larger organizations with multiple industrial facilities. Any of these control systems may be defined as a SUC. For example, there is generally at least one control system at an industrial facility, but oftentimes there are several systems that control various functions within the facility.

This requirement specifies that SUCs are identified for the purpose of performing cyber security analysis. The definition of a SUC is intended to include all IACS assets that are needed to provide a complete automation solution.

System inventory, architecture diagrams, network diagrams and dataflows can be used to determine and illustrate the IACS assets that are included in the SUC description.

NOTE The SUC can include multiple subsystems such as basic process control systems (BPCSs), distributed control systems (DCSs), safety instrumented systems (SISs), supervisory control and data acquisition (SCADA) and IACS product supplier's packages. This could also include emerging technologies such as the industrial Internet of Things (IIoT) or cloud-based solutions.

4.3 ZCR 2: Initial cyber security risk assessment

4.3.1 ZCR 2.1: Perform initial cyber security risk assessment

4.3.1.1 Requirement

The organization shall perform a cyber security risk assessment of the SUC or confirm a previous initial cyber security risk assessment is still applicable in order to identify the worst case unmitigated cyber security risk that could result from the interference with, breach or disruption of, or disablement of mission critical IACS operations.

4.3.1.2 Rationale and supplemental guidance

The purpose of the initial cyber security risk assessment is to gain an initial understanding of the worst-case risk the SUC presents to the organization should it be compromised. This is typically evaluated in terms of impacts to health, safety, environmental, business interruption, production loss, product quality, financial, legal, regulatory, reputation, etc. This assessment assists with the prioritization of detailed risk assessments and facilitates the grouping of assets into zones and conduits within the SUC.

For potentially hazardous processes, the results of the process hazard analysis (PHA) and functional safety assessments as defined in IEC 61511-1 [11] should be referenced as part of the initial cyber security risk assessment to identify worst-case impacts. Organizations should also take into consideration threat intelligence from governments, sector specific Information Sharing and Analysis Centers (ISACs) and other relevant sources.

Assessment of initial risk is often accomplished using a risk matrix that establishes the relationship between likelihood, impact and risk (such as, a corporate risk matrix). Examples of risk matrices can be found in Annex B.

4.4 ZCR 3: Partition the SUC into zones and conduits

4.4.1 Overview

Subclauses 4.4.2 through 4.8.1 describe the ZCRs for partitioning the SUC into zones and conduits and provides rationale and supplemental guidance for each requirement. Subclause 4.4.2,

ZCR 3.1: Establish zones and conduits, is the base requirement for establishing zones and conduits within the SUC. Subclauses 4.4.3 through 4.4.7, ZCR 3.2: Separate business and IACS assets through ZCR 3.6: Separate devices connected via external networks, are intended to provide guidance on assignment of assets to zones based upon industry best practices. This is not intended to be an exhaustive list.

4.4.2 ZCR 3.1: Establish zones and conduits

4.4.2.1 Requirement

The organization shall group IACS and related assets into zones or conduits as determined by risk. Grouping shall be based upon the results of the initial cyber security risk assessment or other criteria, such as criticality of assets, operational function, physical or logical location, required access (for example, least privilege principles) or responsible organization.

4.4.2.2 Rationale and supplemental guidance

The intention of grouping assets into zones and conduits is to identify those assets which share common security requirements and to permit the identification of common security measures required to mitigate risk. The assignment of IACS assets to zones and conduits may be adjusted based upon the results of the detailed risk assessment. This is a general requirement, but special attention should be given to the safety related systems including safety instrumented systems, wireless systems, systems directly connected to Internet endpoints, systems that interface to the IACS but are managed by other entities (including external systems) and mobile devices.

For example, a facility might first be divided into operational areas, such as materials storage, processing, finishing, etc. Operational areas can often be further divided into functional layers, such as manufacturing execution systems (MESs), supervisory systems (for example, human machine interfaces [HMIs]), primary control systems (for example, BPCS, DCS, remote terminal units [RTUs] and programmable logic controllers [PLCs]) and safety systems. Models such as the Purdue reference model as defined in ISA-95.00.01 [12] are often used as a basis for this division. IACS product supplier reference architectures can also be helpful.

4.4.3 ZCR 3.2: Separate business and IACS assets

4.4.3.1 Requirement

IACS assets shall be grouped into zones that are logically or physically separated from business or enterprise system assets.

4.4.3.2 Rationale and supplemental guidance

Business and IACS are two different types of systems that need to be divided into separate zones as their functionality, responsible organization, results of initial risk assessment and location are often fundamentally different. It is important to understand the basic difference between business and IACS, and the ability of IACS to impact health, safety and environment (HSE).

4.4.4 ZCR 3.3: Separate safety related assets

4.4.4.1 Requirement

Safety related IACS assets shall be grouped into zones that are logically or physically separated from zones with non-safety related IACS assets. However, if they cannot be separated, the entire zone shall be identified as a safety related zone.

4.4.4.2 Rationale and supplemental guidance

Safety related IACS assets usually have different security requirements than basic control system components or systems, and components interfaced to the control system components. Safety related zones typically require a higher-level of security protection due to the higher potential for health, safety and environmental consequences if the zone is compromised.

4.4.5 ZCR 3.4: Separate temporarily connected devices

4.4.5.1 Recommendation

Devices that are permitted to make temporary connections to the SUC should be grouped into a separate zone or zones from assets that are intended to be permanently connected to the IACS.

4.4.5.2 Rationale and supplemental guidance

Devices that are temporarily connected to the SUC (for example, maintenance portable computers, portable processing equipment, portable security appliances and universal serial bus [USB] devices) are more likely exposed to a different and wider variety of threats than devices that are permanently part of the zone. Therefore, these devices should be modelled in a separate zone or zones. The primary concern with these devices is that, because of the temporary nature of the connection, they may also be able to connect to other networks outside the zone. However, there are exceptions. For example, a hand-held device that is only used within a single zone and never leaves the physical boundary of the zone may be acceptable to include in the zone.

4.4.6 ZCR 3.5: Separate wireless devices

4.4.6.1 Recommendation

Wireless devices should be in one or more zones that are separated from wired devices.

4.4.6.2 Rationale and supplemental guidance

Wireless signals are not controlled by fences or cabinets and are therefore more accessible than normal wired networks. Because of this increased access potential, they are more likely exposed to a different and wider variety of threats than devices that are wired.

Typically, a wireless access point is modelled as the conduit between a wireless zone and a wired zone. Depending upon the capabilities of the wireless access point additional security controls (for example, firewall) may be required to provide appropriate level of separation.

4.4.7 ZCR 3.6: Separate devices connected via external networks

4.4.7.1 Recommendation

Devices that are permitted to make connections to the SUC via networks external to the SUC should be grouped into a separate zone or zones.

4.4.7.2 Rationale and supplemental guidance

It is not uncommon for organizations to grant remote access to personnel such as employees, suppliers and other business partners for maintenance, optimization and reporting purposes. Because remote access is outside the physical boundary of the SUC, it should be modelled as a separate zone or zones with its own security requirements.

4.5 ZCR 4: Risk comparison

4.5.1 Overview

Subclause 4.5.2 includes one ZCR to compare initial risk to tolerable risk.

4.5.2 ZCR 4.1: Compare initial risk to tolerable risk

4.5.2.1 Requirement

The initial risk determined in subclause 4.3, ZCR 2: Initial cyber security risk assessment, shall be compared to the organization’s tolerable risk. If the initial risk exceeds the tolerable risk, the organization shall perform a detailed cyber security risk assessment as defined in subclause 4.6, ZCR 5: Perform a detailed cyber security risk assessment.

4.5.2.2 Rationale and supplemental guidance

The purpose of this step is to determine if the initial risk is tolerable or requires further mitigation.

4.6 ZCR 5: Perform a detailed cyber security risk assessment

4.6.1 Overview

This ZCR discusses the detailed risk assessment requirements for an IACS and provides rationale and supplemental guidance on each requirement. The requirements in this ZCR apply to every zone and conduit. If zones or conduits share similar threat(s), consequences and/or similar assets, it is allowable to analyze groups of zones or conduits together if such grouping enables optimized analysis. It is permissible to use existing results if the zone is standardized (for example, replication of multiple instances of a reference design). The flowchart shown in Figure 3 illustrates the cyber security risk assessment workflow.

Any detailed risk assessment methodology (such as, ISO 31000 [16], NIST SP 800-39 [18], and ISO/IEC 27005 [14]) may be followed provided the risk assessment requirements are satisfied by the methodology selected. The initial and detailed risk assessment methodologies should be derived from the same framework, standard or source and has to use a consistent risk ranking scale in order to produce consistent and coherent results.

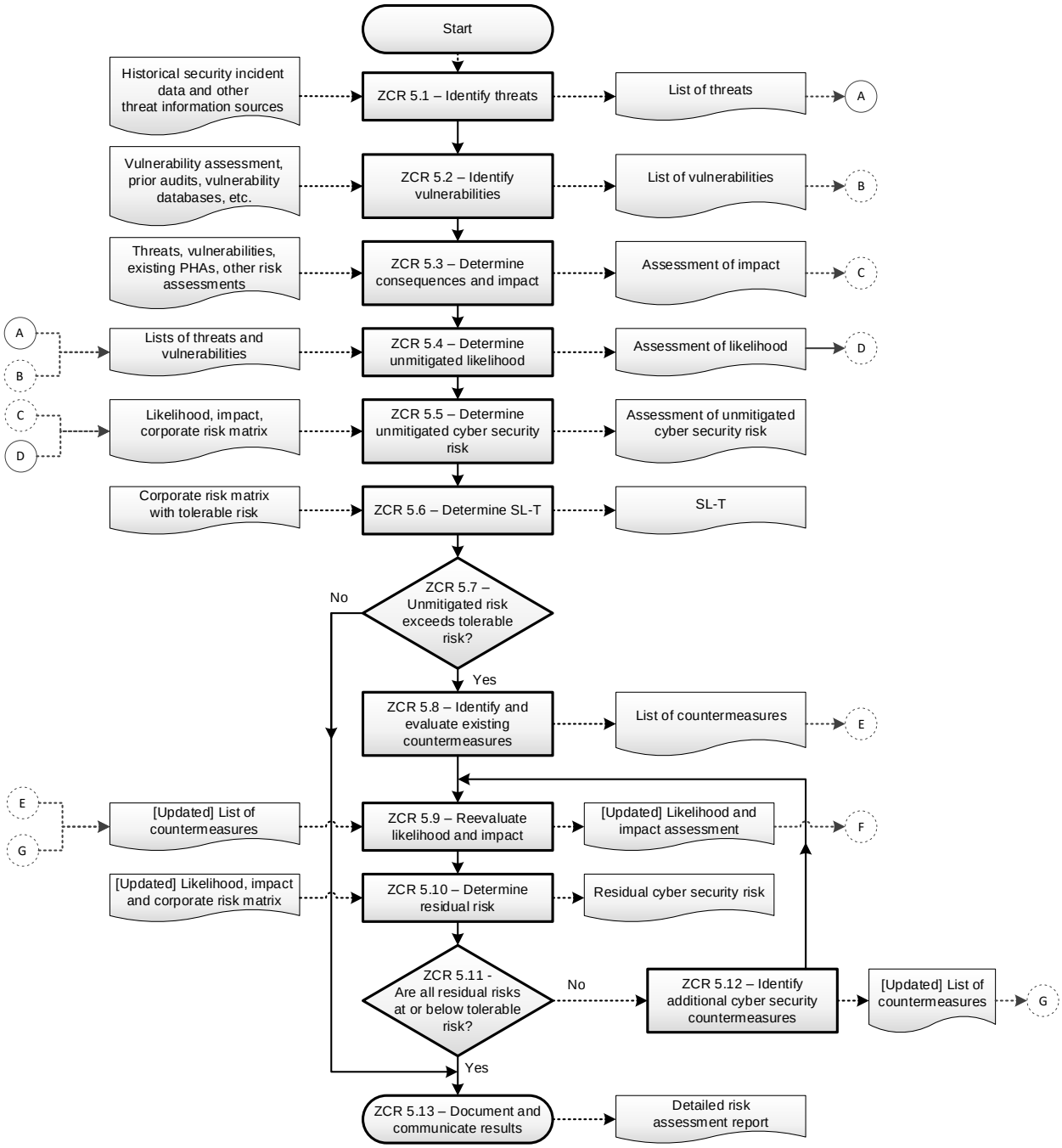

Figure 3 – Detailed cyber security risk assessment workflow per zone or conduit

4.6.2 ZCR 5.1: Identify threats

4.6.2.1 Requirement

A list of the threats that could affect the assets contained within the zone or conduit shall be developed.

4.6.2.2 Rationale and supplemental guidance

It is important to prepare a comprehensive and realistic list of threats in order to perform a security risk assessment. A threat description should include but is not limited to the following:

a) a description of the threat source;

b) a description of the capability or skill-level of the threat source;

c) a description of possible threat vectors;

d) an identification of the potentially affected asset(s).

Some examples of threat descriptions are:

- A non-malicious employee physically accesses the process control zone and plugs a USB memory stick into one of the computers;
- An authorized support person logically accesses the process control zone using an infected laptop; and
- A non-malicious employee opens a phishing email compromising their access credentials.

Given the potential for a large number of possible threats, it is acceptable to summarize by grouping sources, assets, entry points, etc. into classes.

4.6.3 ZCR 5.2: Identify vulnerabilities

4.6.3.1 Requirement

The zone or conduit shall be analyzed in order to identify and document the known vulnerabilities associated with the assets contained within the zone or conduit including the access points.

4.6.3.2 Rationale and supplemental guidance

In order for a threat to be successful, it is necessary to exploit one or more vulnerabilities in an asset. Therefore, it is necessary to identify known vulnerabilities associated with the assets to better understand threat vectors.

A generally accepted approach to identifying vulnerabilities in an IACS is to perform a vulnerability assessment. Refer to ISA-TR84.00.09 [17] for additional information on IACS cyber security vulnerability assessments.

Additionally, there are numerous sources of information regarding known and common vulnerabilities in IACS, such as the industrial control system computer emergency response team (ICS-CERT), IACS product suppliers, etc.

4.6.4 ZCR 5.3: Determine consequence and impact

4.6.4.1 Requirement

Each threat scenario shall be evaluated to determine the consequence and the impact should the threat be realized. Consequences should be documented in terms of the worst-case impact on risk areas such as personnel safety, financial loss, business interruption and environment.

4.6.4.2 Rationale and supplemental guidance

Estimating the worst-case impact of a cyber threat is an important input in performing the cost/benefit analysis of security controls. If the worst-case impact is low, the risk assessment team may decide to proceed to the next threat.

Existing PHA and other related risk assessments (such as, information technology, functional safety, business and physical security) should be reviewed to assist in determining consequences and impact.

The measure of impact may be qualitative or quantitative. One method is to use a consequence scale that is defined by the organization as part of their risk management system (refer to Annex B for examples).

4.6.5 ZCR 5.4: Determine unmitigated likelihood

4.6.5.1 Requirement

Each threat shall be evaluated to determine the unmitigated likelihood. This is the likelihood that the threat will materialize.

4.6.5.2 Rationale and supplemental guidance

In risk management terminology, the word “likelihood” is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as, a probability or a frequency over a given time period). A common method of estimating likelihood is to use a semi-quantitative likelihood scale that is defined by the organization as part of their risk management system (refer to Annex B for examples). Either qualitative or quantitative methods are allowed by this standard.

A number of factors are considered when estimating unmitigated likelihood such as the motivation and capability of the threat source, the history of similar threats, known vulnerabilities, the attractiveness of the target, etc.

Existing cyber security countermeasures for the zone or conduit being evaluated should not be considered when determining unmitigated likelihood; they should be hypothetically eliminated. However, the likelihood determination recognizes countermeasures that are inherent to IACS components and any non-cyber independent protection layers (IPLs) such as physical security, mechanical safeguards (such as, pressure safety valves) or emergency procedures that are in place to reduce the likelihood.

Likelihood is evaluated twice during the detailed risk assessment process. It is initially determined without consideration for any existing countermeasures in order to establish the unmitigated risk. It will be re-evaluated in subclause 4.6.10, ZCR 5.9: Reevaluate likelihood and impact, taking into account existing countermeasures and their effectiveness in order to determine residual risk.

Consequence-only risk assessment methodologies may be used to meet the requirements of this standard. These methodologies typically do not factor likelihood into the determination of unmitigated cyber risk and implicitly assume that likelihood is constant (such as, assuming the likelihood is ever present or quantitatively a ‘1’).

4.6.6 ZCR 5.5: Determine unmitigated cyber security risk

4.6.6.1 Requirement

The unmitigated cyber security risk for each threat shall be determined by combining the impact measure determined in subclause 4.6.4, ZCR 5.3: Determine consequence and impact, and the unmitigated likelihood measure determined in subclause 4.6.5, ZCR 5.4: Determine unmitigated likelihood.

4.6.6.2 Rationale and supplemental guidance

Determination of unmitigated cyber security risk is often accomplished using a risk matrix that establishes the relationship between likelihood, impact and risk, such as a corporate risk matrix (refer to Annex B for examples).

4.6.7 ZCR 5.6: Determine SL-T

4.6.7.1 Requirement

A SL-T shall be established for each security zone or conduit.

4.6.7.2 Rationale and supplemental guidance

SL-T is the desired level of security for a particular IACS, zone or conduit. It is established to clearly communicate this information to those responsible for designing, implementing, operating and maintaining cyber security.

SL-T may be expressed as a single value or a vector. Refer to ISA-62443-3-3:2013, Annex A for a discussion of the SL vector approach.

There is no prescribed method for establishing SL-T. Some organizations choose to establish SL-T based upon the difference between the unmitigated cyber security risk and tolerable risk. Whereas others elect to establish SL-T based on the SL definitions provided in Annex A of this document and ISA-62443-3-3. Another approach, if a risk matrix is used (see Annex B for examples), is to qualitatively establish the SL. Starting from a reasonable estimate of SL (can also be none) the cyber security risk is evaluated by the risk matrix taking into account the countermeasures implied by the SL. If the risk is not acceptable, then the SL is raised (this means additional countermeasures are added) until the cyber security risk is acceptable. The SL derived from this analysis becomes SL-T.

4.6.8 ZCR 5.7: Compare unmitigated risk with tolerable risk

4.6.8.1 Requirement

The unmitigated risk determined for each threat identified in subclause 4.6.6, ZCR 5.5: Determine unmitigated cyber security risk, shall be compared to the organization's tolerable risk. If the unmitigated risk exceeds the tolerable risk, the organization shall determine whether to accept, transfer or mitigate the risk. To mitigate the risk, continue to evaluate the threat by completing subclauses 4.6.9 through 4.6.13, ZCR 5.8: Identify and evaluate existing countermeasures through ZCR 5.12: Identify additional cyber security countermeasures. Otherwise, the organization may document the results in subclause 4.6.14, ZCR 5.13: Document and communicate results, and proceed to the next threat.

4.6.8.2 Rationale and supplemental guidance

The purpose of this step is to determine if the unmitigated risk is tolerable or requires further evaluation.

4.6.9 ZCR 5.8: Identify and evaluate existing countermeasures

4.6.9.1 Requirement

Existing countermeasures in the SUC shall be identified and evaluated to determine the effectiveness of the countermeasures to reduce the likelihood or impact.

4.6.9.2 Rationale and supplemental guidance

In order to determine residual risk, the likelihood and impact should be evaluated taking into account the presence and effectiveness of existing countermeasures. This step in the process focuses on identifying and evaluating existing countermeasures.

ISA-62443-3-3 provides guidance on types of countermeasures and their effectiveness by assigning a capability SL (SL-C) to each system requirement.

4.6.10 ZCR 5.9: Reevaluate likelihood and impact

4.6.10.1 Requirement

The likelihood and impact shall be re-evaluated considering the countermeasures and their effectiveness.

4.6.10.2 Rationale and supplemental guidance

The unmitigated likelihood determined in subclause 4.6.5, ZCR 5.4: Determine unmitigated likelihood, did not account for existing countermeasures. In this step, countermeasures such as technical, administrative or procedural controls are considered and used to determine mitigated likelihood. Likewise, the consequences and impact determined in subclause 4.6.4, ZCR 5.3: Determine consequence and impact, should also be re-evaluated considering the identified countermeasures.

4.6.11 ZCR 5.10: Determine residual risk

4.6.11.1 Requirement

The residual risk for each threat identified in subclause 4.6.2, ZCR 5.1: Identify threats, shall be determined by combining the mitigated likelihood measure and mitigated impact values determined in subclause 4.6.10, ZCR 5.9: Reevaluate likelihood and impact.

4.6.11.2 Rationale and supplemental guidance

Determining residual risk provides a measure of the current level of risk as well as a measure of the effectiveness of existing countermeasures. It is an essential step in determining whether the current level of risk exceeds tolerable risk guidelines.

4.6.12 ZCR 5.11: Compare residual risk with tolerable risk

4.6.12.1 Requirement

The residual risk determined for each threat identified in subclause 4.6.2, ZCR 5.1: Identify threats, shall be compared to the organization’s tolerable risk. If the residual risk exceeds the tolerable risk, the organization shall determine if the residual risk will be accepted, transferred or mitigated based upon the organization’s policy.

4.6.12.2 Rationale and supplemental guidance

The purpose of this step is to determine if the residual risk is tolerable or requires further mitigation. Many organizations define tolerable risk in their risk management policies.

4.6.13 ZCR 5.12: Identify additional cyber security countermeasures

4.6.13.1 Requirement

Additional cyber security countermeasures such as technical, administrative or procedural controls shall be identified to mitigate the risks where the residual risk exceeds the organization’s tolerable risk unless the organization has elected to tolerate or transfer the risk.

4.6.13.2 Rationale and supplemental guidance

When residual risk exceeds an organization's risk tolerance, steps need to be taken to reduce the risk to tolerable levels.

Countermeasures are applied to reduce risk. Cyber security countermeasures may be a combination of technical and non-technical (such as, policies and procedures). Another means of reducing risk is to reallocate an IACS asset from a lower security to a higher security zone or conduit in order to take advantage of the security countermeasures of the higher security zone or conduit.

ISA-62443-3-3 can be used as a guide to select appropriate technical countermeasures. The countermeasures identified in ISA-62443-3-3 have been assigned a SL-C rating which is beneficial in evaluating the effectiveness of the countermeasure.

Users may also want to evaluate the cost and complexity of countermeasures as part of the design process.

4.6.14 ZCR 5.13: Document and communicate results

4.6.14.1 Requirement

The results of the detailed cyber risk assessment shall be documented, reported and made available to the appropriate stakeholders in the organization. Appropriate information security classification shall be assigned to protect the confidentiality of the documentation. Documentation shall include the date each session was conducted as well as the names and titles of the participants. Documentation that was instrumental in performing the cyber risk assessment (such as, system architecture diagrams, PHAs, vulnerability assessments, gap assessments and sources of threat information) shall be recorded and archived along with the cyber risk assessment.

4.6.14.2 Rationale and supplemental guidance

Cyber security risk assessments need to be documented and made available to the appropriate personnel in the organization. Cyber security risk assessments are living documents that may be used for multiple purposes including testing, auditing and future risk assessments. However, it is also important to properly protect this information as it often contains sensitive details about the systems, known vulnerabilities and existing safeguards.

4.7 ZCR 6: Document cyber security requirements, assumptions and constraints

4.7.1 Overview

Subclauses 4.7.2 through 4.7.10 describe the requirements for documenting cyber security requirements, assumptions and constraints within the SUC as needed to achieve the SL-T and provides rationale and supplemental guidance for each requirement.

4.7.2 ZCR 6.1: Cyber security requirements specification

4.7.2.1 Requirement

A cyber security requirements specification (CRS) shall be created to document mandatory security countermeasures of the SUC based on the outcome of the detailed risk assessment as well as general security requirements based upon company or site-specific policies, standards and relevant regulations.

At a minimum, the CRS shall include the following:

- ZCR 6.2: SUC description (see 4.7.3)
- ZCR 6.3: Zone and conduit drawings (see 4.7.4)
- ZCR 6.4: Zone and conduit characteristics (see 4.7.5)
- ZCR 6.5: Operating environment assumptions (see 4.7.6)
- ZCR 6.6: Threat environment(see 4.7.7)
- ZCR 6.7: Organizational security policies (see 4.7.8)
- ZCR 6.8: Tolerable risk (see 4.7.9)
- ZCR 6.9: Regulatory requirements (see 4.7.10)

4.7.2.2 Rationale and supplemental guidance

Cyber security requirements need to be documented in order to ensure the requirements are clearly communicated to all stakeholders and are properly implemented. The CRS does not need to be a single document. Many organizations create a cyber security requirements section in other IACS documents.

NOTE ISA-TR84.00.09 provides additional guidance on the recommended elements in a CRS.

4.7.3 ZCR 6.2: SUC description

4.7.3.1 Requirement

A high-level description and depiction of the SUC shall be included in the CRS. At a minimum, the CRS shall include the name, a high-level description of the function and the intended usage of the SUC, as well as, a description of the equipment or process under control.

4.7.3.2 Rationale and supplemental guidance

It is important to clearly identify and define the scope of the SUC in the CRS. This requirement ensures a minimum amount of information is provided. An illustration of the SUC and the associated data flows and process flows should be included.

4.7.4 ZCR 6.3: Zone and conduit drawings

4.7.4.1 Requirement

The organization shall:

a) Produce a drawing or a set of drawings that illustrates the zone and conduit partitioning of the entire SUC.

b) Assign each asset in the SUC to a zone or a conduit.

4.7.4.2 Rationale and supplemental guidance

It is important to have an overview drawing of the SUC that illustrates the zone and conduit boundaries and the assets contained within those boundaries in order to effectively communicate how the SUC is partitioned.

4.7.5 ZCR 6.4: Zone and conduit characteristics

4.7.5.1 Requirement

The following items shall be identified and documented for each defined zone and conduit:

a) Name and/or unique identifier;

b) Accountable organization(s);

c) Definition of logical boundary;

d) Definition of physical boundary, if applicable;

e) Safety designation;

f) List of all logical access points;

g) List of all physical access points;

h) List of data flows associated with each access point;

i) Connected zones or conduits;

j) List of assets and their classification, criticality and business value;

k) SL-T;

l) Applicable security requirements;

m) Applicable security policies; and

n) Assumptions and external dependencies.

4.7.5.2 Rationale and supplemental guidance

It is important to characterize and document the attributes of a zone or conduit. Each of the items listed in the above requirements has a specific purpose, as described below:

a) **Name and/or unique identifier –** It is important for design and documentation purposes to be able to uniquely identify each zone or conduit.

b) **Accountable organization(s) –** The accountable organization is the person, group or groups who are responsible and accountable for the security of the zone or conduit.

NOTE The accountable and responsible organizations may be different. If so, they should both be identified.

c) **Logical boundary –** The logical boundary is important because it delineates the boundary between the zone or conduit and the rest of the system. It also helps identify the demarcation point for all communications entering or exiting the zone or conduit.

d) **Physical boundary –** It is important to document the physical boundary if the zone or conduit requires physical security to achieve its SL-T. If physical security could enhance (but is not required) the SL-T it should preferably be documented.

e) **Safety Designation –** It is important to identify if the zone or conduit is safety related or contains safety related assets.

f) **List of logical access points –** Logical access points are any place where electronic information can cross the logical boundary of a zone or conduit. Logical access points need to be identified and documented as they may have vulnerabilities that can be exploited by threats.

g) **List of physical access points –** Physical access points (for example, fences, doors and enclosures) are any place where personnel can gain physical access to zone or conduit assets. Physical access points need to be identified and documented to determine appropriate means of monitoring and preventing unauthorized access.

h) **List of data flows –** In order to detect anomalies, it is important to identify and document the expected flow of data (for example, source, destination and protocol) throughout the system and, in particular, the flow of data in and out of a zone or conduit.

i) **Connected zones or conduits –** It is important to identify the connectivity between zones and conduits in order to identify all of the logical access points into and within the system. Typically, this is illustrated in a zone and conduit diagram.

j) **List of assets and their classification, criticality and business value –** It is important to identify the IACS assets contained within each zone or conduit and their classification, criticality and business value in order to develop an understanding of the consequences should that zone or conduit be compromised. When identifying consequences, it is important to consider the consequences to other zones/conduits as well as the zone/conduit in question.

k) **SL-T –** The SL-T communicates the level of protection required for a zone or conduit based upon the results of the risk assessment. Refer to subclause 4.6.7, ZCR 5.6: Determine SL-T, for further information.

l) **Applicable security requirements –** For each zone and conduit it is necessary to identify the applicable security requirements needed to achieve the SL-T. Some requirements may be common to all zones or conduits in the SUC while others may be specific.

NOTE Security requirements specification cannot be finalized until after completion of the detailed risk assessment (refer to subclause 4.6, ZCR 5: Perform a detailed cyber security risk assessment).

m) **Applicable security policies –** For each zone and conduit, it is necessary to identify the applicable organizational security policies needed to achieve the SL-T. Some policies may be common to all zones or conduits in the SUC while others may be specific.

n) **Assumptions and external dependencies –** Oftentimes, the security of a zone or conduit is dependent upon factors outside of the zone or conduit, such as clean power and additional layers of physical and network security. These assumptions and interdependencies should be documented.

4.7.6 ZCR 6.5: Operating environment assumptions

4.7.6.1 Requirement

The CRS shall identify and document the physical and logical environment in which the SUC is located or planned to be located.

4.7.6.2 Rationale and supplemental guidance

The physical environment for the SUC needs to be documented in order to ensure the IACS assets are properly protected. Examples of documentation that can be used to communicate the physical environment would be site maps, floor plans, wiring schematics, connector configurations and site security plans. Existing security vulnerability assessments should also be referenced.

The logical environment for the SUC also needs to be documented to provide a clear understanding of the networks, information technology, protocols and IACS systems that may interface with the SUC. Examples of relevant documentation would be network architecture diagrams, system architecture diagrams, electrical one-lines, heating, ventilation and air-conditioning (HVAC) hook-ups, fire and gas detection and suppression, and other relevant design documents.

4.7.7 ZCR 6.6: Threat environment

4.7.7.1 Requirement

The CRS shall include a description of the threat environment that impacts the SUC. The description shall include the source(s) of threat intelligence and include both current and emerging threats.

4.7.7.2 Rationale and supplemental guidance

There are a number of factors that may affect the threat environment of a SUC, including the geo-political climate, the physical environment and the sensitivity of the system. Examples of appropriate authoritative sources may include:

- Computer emergency response teams (CERTs);
- ICS-CERT;
- Public-private partnerships such as ISACs;
- IACS product suppliers;
- Industry advisory groups;
- Government agencies such as an information security agency;
- Threat intelligence services;

4.7.8 ZCR 6.7: Organizational security policies

4.7.8.1 Requirement

Security countermeasures and features that implement the organizational security policies shall be included in the CRS.

4.7.8.2 Rationale and supplemental guidance

It is important that all systems incorporate the baseline security policies established by the organization.

4.7.9 ZCR 6.8: Tolerable risk

4.7.9.1 Requirement

The organization’s tolerable risk for the SUC shall be included in the CRS.

4.7.9.2 Rationale and supplemental guidance

It is important that stakeholders are aware of the organization's established tolerable risk level in order to ensure that the SUC risk level is in alignment.

4.7.10 ZCR 6.9: Regulatory requirements

4.7.10.1 Requirement

Any relevant cyber security regulatory requirements that apply to the SUC shall be included in the CRS.

4.7.10.2 Rationale and supplemental guidance

This is important to ensure regulatory compliance.

4.8 ZCR 7: Asset owner approval

4.8.1 Overview

Subclause 4.8.2 includes one ZCR to attain asset owner approval.

4.8.2 ZCR 7.1: Attain asset owner approval

4.8.2.1 Requirement

Asset owner management who are accountable for the safety, integrity and reliability of the process controlled by the SUC shall review and approve the results of the risk assessment.

4.8.2.2 Rationale and supplemental guidance

Risk assessments are often facilitated by third parties with participation by various subject matter experts who have intimate knowledge of the operation of the industrial process and the functionality of the IACS and related IT systems. While these personnel have the knowledge and skills to perform the risk assessment, they typically do not have the authority to make decisions to accept risk. Therefore, the results of the assessment have to be presented to the appropriate management with the authority to make such decisions.

Annex A
(informative)

Security levels

ISA-62443-4-2 [10] defines SLs in terms of four different levels (1, 2, 3 and 4), each with an increasing level of security. SL 0 is implicitly defined as no security requirements or security protection necessary.

- **SL 1:** Protection against casual or coincidental violation
- **SL 2:** Protection against intentional violation using simple means with low resources, generic skills and low motivation
- **SL 3:** Protection against intentional violation using sophisticated means with moderate resources, IACS specific skills and moderate motivation
- **SL 4:** Protection against intentional violation using sophisticated means with extended resources, IACS specific skills and high motivation

For SL-T, this means that the asset owner or system integrator has determined through a risk assessment that they need to protect this particular zone, system or component against this level of threat.

SLs have been categorized by ISA-62443-3-3 into three different types: target, achieved and capability. These types, while they all are related, involve different aspects of the security lifecycle.

- SL-Ts are the desired level of security for a particular IACS, zone or conduit. This is usually determined by performing a risk assessment on a system and determining that it needs a particular level of security to ensure its correct operation.
- Achieved SLs (SL-As) are the actual level of security for a particular system. These are measured after a system design is available or when a system is in place. They are used to establish that a security system is meeting the goals that were originally set out in the SL-Ts.
- SL-Cs are the SLs that components or systems can provide when properly configured. These levels state that a particular component or system is capable of meeting the SL-Ts natively without additional compensating countermeasures when properly configured and integrated.

Each of these SLs is intended to be used in different phases of the security life cycle according to the ISA-62443 series. Starting with a target for a particular system, an organization would need to build a design that included the capabilities to achieve the desired result. In other words, the design team would first develop the SL-T necessary for a particular system. They would then design the system to meet those SL-Ts, usually in an iterative process where after each iteration the SL-As of the proposed design are measured and compared to the SL-Ts. As part of that design process, the designers would select components and systems with the necessary SL-Cs to meet the SL-T requirements, or where such systems and components are not available, complement the available ones with compensating countermeasures. After the system went into operation, the actual SL would be measured as the SL-As and compared to the SL-Ts.

This page intentionally left blank.

Annex B
(informative)

Risk matrices

A risk matrix is a tool used in risk management to qualitatively determine the level of risk by assessing the likelihood of an incident occurring and the severity of the consequence should the incident occur.

A risk matrix presents likelihood on one axis and severity on the second axis. The intersections between likelihood and severity establish the risk rank. The intersection between the lowest likelihood and lowest severity yields the lowest risk rank. Whereas the intersection between the highest likelihood and highest severity yields the highest risk rank. The intersections are typically color-coded to indicate increasing risk rank with green typically being the lowest and red typically being the highest.

While always 2-dimensional, risk matrices vary in size (for example, 3 x 3, 4 x 4, 3 x 5, 5 x 5) depending on the number of categories in the likelihood and severity scales.

Table B.1 is an example of a 3 x 5 risk matrix.

Table B.1 – Example of a 3 x 5 risk matrix

		Severity		
		A	B	C
Likelihood	5	High	High	Med-high
	4	High	Med-high	Medium
	3	Med-high	Medium	Med-low
	2	Medium	Med-low	Low
	1	Med-low	Low	Low

A likelihood scale partitions the entire range of likelihood values into discrete categories or bins. Table B.2 is an example of a likelihood scale with 5 categories. This example demonstrates how some likelihood scales provide multiple ways of partitioning the data into categories. In this example a guideword, a likelihood description and a frequency scale are all provided.

Table B.2 – Example of likelihood scale

Likelihood scale	Guideword	Likelihood description	Frequency-based guidance
1	Certain	Almost certain	$>10^{-1}$ per year (High demand)
2	Likely	Likely to occur	10^{-1} to 10^{-3} per year (Low demand)
3	Possible	Quite possible or not unusual to occur	10^{-3} to 10^{-4} per year
4	Unlikely	Conceivably possible, but very unlikely to occur	10^{-4} to 10^{-5} per year
5	Remote	So unlikely that it can be assumed it will not occur	$<10^{-5}$ per year

Similarly, a consequence or severity scale partitions the entire range of severity values into discrete categories or bins. Table B.3 is an example of a consequence scale with 3 categories. This example demonstrates how some likelihood scales provide multiple ways of partitioning the data into categories. In this example a guideword, a likelihood description and a frequency scale are all provided.

Table B.3 – Example of consequence or severity scale

	Operational			Financial			HSE		
Category	Outage at one site	Outage at multiple sites	National infrastructure and services	Cost (Million USD)	Legal	Public confidence	People onsite	People offsite	Environment
A (High)	>7 days	>1 day	Impacts multiple sectors or disrupts community services in a major way	>500	Felony criminal offense	Loss of brand image	Fatality	Fatality or major community incident	Citation by regional agency or long-term significant damage over large area
B (Medium)	<2 days	>1 hour	Potential to impact sector at a level beyond the company	>5	Misdemeanor criminal offense	Loss of customer confidence	Loss of work day or major injury	Complaints or local community impact	Citation by local agency
C (Low)	<1 day	<1 hour	Little to no impact to sectors beyond the individual company. Little to no impact on community.	<5	None	None	First aid or recordable injury	No complaints	Small, contained release below reportable limits

Although some standard risk matrices exist in different contexts individual projects and organizations typically create their own or tailor an existing risk matrix. This annex provides several additional risk matrix examples (shown in Table B.4 through Table B.6) to emphasize to the reader that risk matrices can vary in dimensions, scale categories, color coding, risk ranking, etc. It is critical that the entity facilitating the risk assessment obtain the correct risk matrix that has been approved by the asset owner for the facility that is being assessed.

Table B.4 – Example of a simple 3 x 3 risk matrix

Likelihood	Negligible	Moderate impact	Severe
Highly likely	Medium	High	High
Possible	Low	Medium	High
Unlikely	Low	Low	Medium

Table B.5 – Example of a 5 x 5 risk matrix

		Consequence				
		Minor problem (Easily handled by normal day-to-day processes)	Some disruption possible (Damage between $500k and $1MM)	Significant time and resources required (Damage between $1MM and $10MM)	Operations severely damaged (Damage between $10MM and $25MM)	Business survival at risk (Damage >$25MM)
Likelihood	Almost certain (>90%)	High	High	Extreme	Extreme	Extreme
	Likely (50% to 90%)	Moderate	High	High	Extreme	Extreme
	Moderate (10% to 50%)	Low	Moderate	High	Extreme	Extreme
	Unlikely (3% to 10%)	Low	Low	Moderate	High	Extreme
	Rare (<3%)	Low	Low	Moderate	High	High

Table B.6 – Example of a 3 x 4 matrix

		Severity			
		Acceptable (Little or no effect on event)	Tolerable (Effects are felt, but not critical to outcome)	Undesirable (Serious impact or critical to outcome)	Intolerable (Could result in disaster)
Likelihood	Improbable (Risk is unlikely to occur)	Low - 1 -	Medium - 4 -	Medium - 6 -	High - 10 -
	Possible (Risk will likely occur)	Low - 2 -	Medium - 5 -	High - 8 -	Extreme - 11 -
	Probable (Risk will occur)	Medium - 3 -	High - 7 -	High - 9 -	Extreme - 12 -

BIBLIOGRAPHY

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

[1] ISA-62443-1-2, *Security for industrial automation and control systems, Part 1-2: Master glossary of terms and abbreviations* (in development)

[2] ISA-62443-1-3, *Security for industrial automation and control systems, Part 1-3: Security system conformance metrics* (in development)

[3] ISA-TR62443-1-4, *Security for industrial automation and control systems, Part 1-4: IACS security lifecycle and use cases* (in development)

[4] ISA-62443-2-2, *Security for industrial automation and control systems, Part 2-2: IACS protection ratings* (in development)

[5] ISA-TR62443-2-3:2015, *Security for industrial automation and control systems, Part 2-3: Patch management in the IACS environment*

[6] ISA-62443-2-4:2018, *Security for industrial automation and control systems, Part 2-4: Security program requirements for IACS service providers*

[7] ISA-TR62443-2-5, *Security for industrial automation and control systems, Part 2-5: Implementation guidance for IACS asset owners* (in development)

[8] ISA-TR99.00.01-2007, *Security technologies for industrial automation and control systems*

[9] ISA-62443-4-1:2018, *Security for industrial automation and control systems, Part 4-1: Product security development lifecycle requirements*

[10] ISA-62443-4-2:2018, *Security for industrial automation and control systems, Part 4-2: Technical security requirements for IACS components*

Other standards references:

[11] IEC 61511-1:2018, *Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and software requirements*

[12] ISA-95.00.01-2010 (IEC 62264-1 Modified), *Enterprise-control system integration – Part 1: Models and terminology*

[13] ISO/IEC 18028-4:2005, *Information technology – Security techniques – IT network security – Part 4: Securing remote access*

[14] ISO/IEC 27005:2018, *Information technology – Security techniques – Information security risk management*

[15] ISO Guide 73:2009, *Risk management – Vocabulary*

[16] ISO 31000:2018, *Risk management –Guidelines*

[17] ISA-TR84.00.09, *Cybersecurity Related to the Functional Safety Lifecycle*

[18] NIST Special Publication (SP) 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*

This page intentionally left blank.

Developing and promulgating sound consensus standards, recommended practices, and technical reports 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 T.W. Alexander Drive
P.O. Box 12277
Research Triangle Park, NC 27709

ISBN: 978-1-64331-116-6