Draft for Public Comment

Form 36

DPC: 18/30267404 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000
Fax: +44 (0)20 8996 7400
www.bsigroup.com

Date: 19 March 2018
Origin: European

Latest date for receipt of comments: 01 May 2018

Project No. 2012/02014

Responsible committee: GEL/65 Measurement and control

Interested committees:

Title: Draft BS EN 62443-3-2 Security for industrial automation and control systems. Part 3-2: Security risk assessment and system design.

Please notify the secretary if you are aware of any keywords that might assist in classifying or identifying the standard or if the content of this standard

i) has any issues related to 3rd party IPR, patent or copyright
ii) affects other national standard(s)
iii) requires additional national guidance or information

WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD. THIS DRAFT IS NOT CURRENT BEYOND 01 May 2018

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

Further copies of this draft may be purchased from BSI Shop http://shop.bsigroup.com or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from https://standardsdevelopment.bsigroup.com/.

Responsible Committee Secretary: Mrs Hazel Cochrane (BSI)
Direct tel: 0208 996 7465
E-mail: hazel.cochrane@bsigroup.com

Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at **https://standardsdevelopment.bsigroup.com/**. You will need to register in order to comment.

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx

1	2	(3)	4	5	(6)	7
MB	Clause No./ Subclause No./Annex **(e.g. 3.1)**	Paragraph/Figure/ Table/Note	**Type of comment**	**Commend (justification for change) by the MB**	**Proposed change by the MB**	**Secretariat observations on each comment submitted**
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	

65/690/CDV

COMMITTEE DRAFT FOR VOTE (CDV)

PROJECT NUMBER: **IEC 62443-3-2 ED1**	
DATE OF CIRCULATION: **2018-03-09**	CLOSING DATE FOR VOTING: **2018-06-01**
SUPERSEDES DOCUMENTS: **65/611/NP,65/641A/RVN**	

IEC TC 65 : INDUSTRIAL-PROCESS MEASUREMENT, CONTROL AND AUTOMATION	
SECRETARIAT: France	SECRETARY: Mr Rudy BELLIARDI
OF INTEREST TO THE FOLLOWING COMMITTEES: TC 44,SC 45A,TC 57,SC 62A,ISO/IEC JTC 1/SC 41	PROPOSED HORIZONTAL STANDARD: ☐ Other TC/SCs are requested to indicate their interest, if any, in this CDV to the secretary.
FUNCTIONS CONCERNED: ☐ EMC ☐ ENVIRONMENT ☐ QUALITY ASSURANCE ☐ SAFETY	
☒ SUBMITTED FOR CENELEC PARALLEL VOTING **Attention IEC-CENELEC parallel voting** The attention of IEC National Committees, members of CENELEC, is drawn to the fact that this Committee Draft for Vote (CDV) is submitted for parallel voting. The CENELEC members are invited to vote through the CENELEC online voting system.	☐ NOT SUBMITTED FOR CENELEC PARALLEL VOTING

This document is still under study and subject to change. It should not be used for reference purposes.

Recipients of this document are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

TITLE:

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

PROPOSED STABILITY DATE: 2021

NOTE FROM TC/SC OFFICERS:

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

____

Security for industrial automation and control systems –

Part 3-2: Security risk assessment and system design

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

International Standard IEC 62443-3-2 has been prepared by TC65: Industrial-process measurement, control and automation, in cooperation with the ISA99 liaison.

The text of this standard is based on the following documents:

FDIS	Report on voting
65/XX/FDIS	65/XX/RVD

Full information on the voting for the approval of this International Standard can be found in the report on voting indicated in the above table.

This document has been drafted in accordance with the ISO/IEC Directives, Part 2.

A list of all parts in the IEC 62443 series, published under the general title *Security for industrial automation and control systems*, can be found on the IEC website.

Future standards in this series will carry the new general title as cited above. Titles of existing standards in this series will be updated at the time of the next edition.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under "http://webstore.iec.ch" in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

The National Committees are requested to note that for this document the stability date is 2022. THIS TEXT IS INCLUDED FOR THE INFORMATION OF THE NATIONAL COMMITTEES AND WILL BE DELETED AT THE PUBLICATION STAGE.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

NOTE: The format of this document follows the ISO/IEC requirements discussed in ISO/IEC Directives, Part 2 [14]. This document specifies the format of the document as well as the use of terms like “shall”, “should”, and “may”. The requirements specified in normative clauses use the conventions discussed in Appendix H of the Directives document.

Overview

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 standard 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 IEC 62443-1-1 [1]. Readers are encouraged to familiarize themselves with these concepts prior to reading this document.

Purpose and intended audience

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

Usage within other parts of the IEC 62443 series

This standard provides a basis for specifying security countermeasures by aligning the target security level (SL-T) identified in this standard with the required security level capabilities (SL-C) specified in IEC 62443-3-3 [10].

Security for industrial automation and control systems –

Part 3-2: Security risk assessment and system design

1 Scope

This standard 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 security level target (SL-T) for each zone and conduit; and
- documenting the security requirements.

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.

IEC 62443-1-1 – *Security for industrial automation and control systems –, Part 1-1: Concepts and models* [1]

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

IEC 62443-3-3 – *Security for industrial automation and control systems –, Part 3-3: System security requirements and security levels* [10]

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 IEC/TR 62443-1-2 and the following apply.

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

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

3.1.1
channel
specific logical or physical communication link between assets

Note 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 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

3.1.4
confidentiality
preserving 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 (e.g. intellectual property), and/or business interruption costs, that occurs from a particular incident

3.1.6
countermeasure
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

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

Note to entry: IACS are computer systems

3.1.8

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

3.1.9

external network
Any 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 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

[SOURCE: ISO Guide 73:2009 and ISO/IEC 27005:2011]

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.

3.1.12
impact
measure of the ultimate loss or harm associated with a consequence

Note 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.

3.1.13
process hazard analysis
set of organized and systematic assessments of the potential hazards associated with an industrial process

3.1.14
residual risk
The risk that remains after existing countermeasures are taken into account (i.e. the net risk or risk after countermeasures are applied).

3.1.15
risk
expectation of loss expressed as the likelihood that a particular threat will exploit a particular vulnerability with a particular consequence

3.1.16
security level
measure of confidence that the System-Under-Consideration, Security Zone or Conduit is free from vulnerabilities and functions in the intended manner

3.1.17
security perimeter
logical or physical boundary surrounding all the assets that are controlled and protected by the Security Zone.

3.1.18
system under consideration
defined collection of IACS assets that are needed to provide a complete automation solution. including any relevant network infrastructure assets

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

3.1.19
threat
any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image or reputation) and/or organizational assets including IACS.

Note 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

3.1.20
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)

3.1.21
threat source
intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally exploit a vulnerability

3.1.22
threat vector
path or means by which a threat source can gain access to an asset

3.1.23
tolerable risk
level of risk deemed tolerable to an organization

Note to entry: Additional guidance on establishing tolerable risk can be found in ISO 31000 and NIST 800-39.

3.1.24
unmitigated cybersecurity risk
level of cybersecurity risk that is present in a system before any cybersecurity countermeasures are considered

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

3.1.25
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.

3.1.26
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 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 (e.g. high financial, health, safety, or environmental impact), functionality, logical and physical (including location) relationship

3.2 Abbreviated terms and acronyms

The following abbreviated terms and acronyms are used in this document.

ANSI	American National Standards Institute
CRS	Cybersecurity requirements specification
DCS	Distributed control system
IACS	Industrial automation and control system(s)
IEC	International Electrotechnical Commission
ISA	International Society of Automation
ISAC	Information Sharing and Analysis Centers
ISO	International Organization for Standardization
NIST	[US] National Institute of Standards and Technology
PHA	Process hazard analysis
SIS	Safety instrumented system
SUC	System under consideration
SL	Security level
SL-T	Target security level
SP	[US NIST] Special Publication
USB	Universal serial bus
ZCR	Zone and conduit requirement

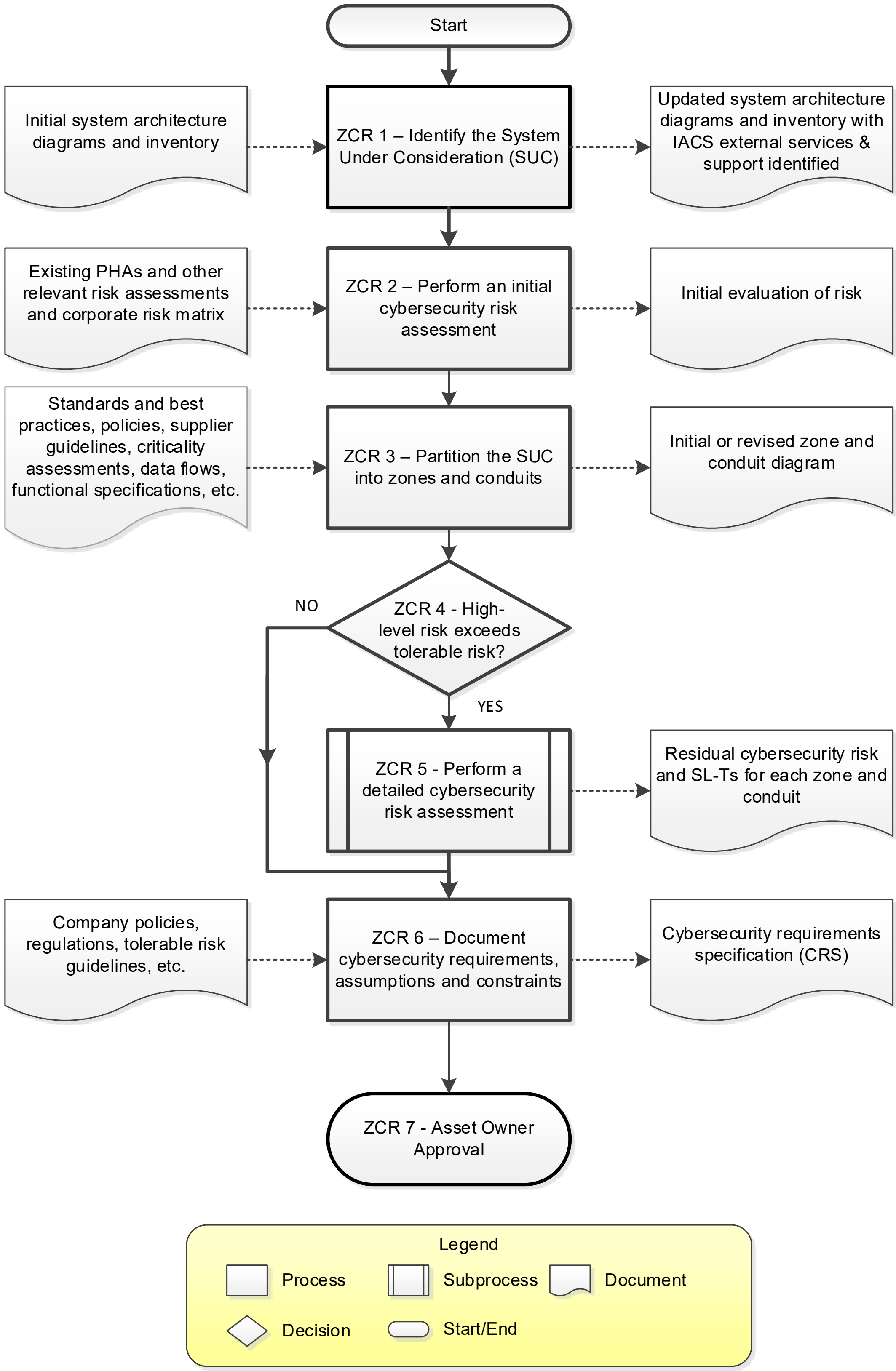
3.3 Conventions

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 a SUC into zones and conduits as well as the requirements for assessing the cybersecurity 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). The clause also provides rationale and supplemental guidance on each of the requirements. Figure 1 is a workflow diagram outlining the primary steps required to establish zones and conduits and assess risk. The steps are numbered to indicate their relationship to the ZCRs.



340

341 **Figure 1 – Workflow to establish zones and conduits and assess risk**

4.2 ZCR-1: Identify the System-under-consideration

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 delineation of the security perimeter and identification of all access points to the SUC.

4.2.1.2 Rationale and supplemental guidance

For the purpose of performing cybersecurity analysis, a SUC is intended to include all IACS assets that are needed to provide a complete automation solution.

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

Note: the SUC may include multiple subsystems such as DCS, SIS, SCADA and vendor packages.

4.3 ZCR-2: Initial cybersecurity risk assessment

4.3.1 ZCR-2.1: Perform initial cybersecurity risk assessment

4.3.1.1 Requirement

The organization shall perform a cybersecurity 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 cybersecurity risk that could result from the interference with, disruption of, or disablement of mission critical IACS operations.

4.3.1.2 Rationale and supplemental guidance

The purpose of the initial cybersecurity risk assessment is to gain a high-level understanding of the worst-case risk the SUC presents to the organization should it be compromised. 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 [18] should be referenced as part of the high-level cybersecurity 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 high-level 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 Informative Annex B.

4.4 ZCR-3: Partition the SUC into zones and conduits

4.4.1 Overview

The following sections describe the ZCR-for partitioning the SUC into zones and conduits and provides rationale and supplemental guidance for each requirement. ZCR-3.1 is the base requirement for establishing zones and conduits within the SUC. ZCRs 3.2 through 3.6 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 establish zones and conduits by grouping IACS and related assets as necessary as determined by risk. Grouping shall be based upon the results of the initial cybersecurity 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 intent 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 (MES), supervisory systems (for example, human machine interfaces [HMIs]), primary control systems (for example, distributed control systems [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 [19] are often used as a basis for this division. Vendor reference architectures can also be helpful.

4.4.3 ZCR-3.2: Separate business and control system 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 high level 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 assets shall be grouped into zones that are logically or physically separated from zones with non-safety related 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 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 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 modeled 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 they are more likely exposed to a different and wider variety of threats than devices that are wired.

Typically, a wireless access point is modeled as the conduit between a wireless zone and a wired zone. Depending upon the capabilities of the wireless access point additional security controls (e.g. 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 modeled as a separate zone or zones with its own security requirements.

4.5 ZCR-4: Risk comparison

4.5.1 ZCR-4.1: Compare high-level risk to tolerable risk

4.5.1.1 Requirement

The high-level risk determined in ZCR-2 shall be compared to the organization's tolerable risk. If the high-level risk exceeds the tolerable risk, the organization shall perform a detailed cyber security risk assessment as defined in ZCR-5.

4.5.1.2 Rationale and supplemental guidance

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

4.6 ZCR-5: Perform a detailed cybersecurity risk assessment

4.6.1 Overview

ZCR-5 discusses the detailed risk assessment requirements for an IACS and provides rationale and supplemental guidance on each requirement. The requirements in ZCR-5 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 if such grouping enables optimized analysis. It is permissible to use existing results if the zone is standardized (e.g. replication of multiple instances of a reference design). The flowchart shown in Figure 2 illustrates the workflow.

Any detailed risk assessment methodology (such as, ISO 31000 [17], NIST SP800-39 [20] and ISO/IEC 27005 [16]) may be followed provided the requirements are satisfied by the methodology selected. The high-level and detailed risk assessment methodologies should be derived from the same framework, standard or source and must use a consistent risk ranking scale in order to produce consistent and coherent results.

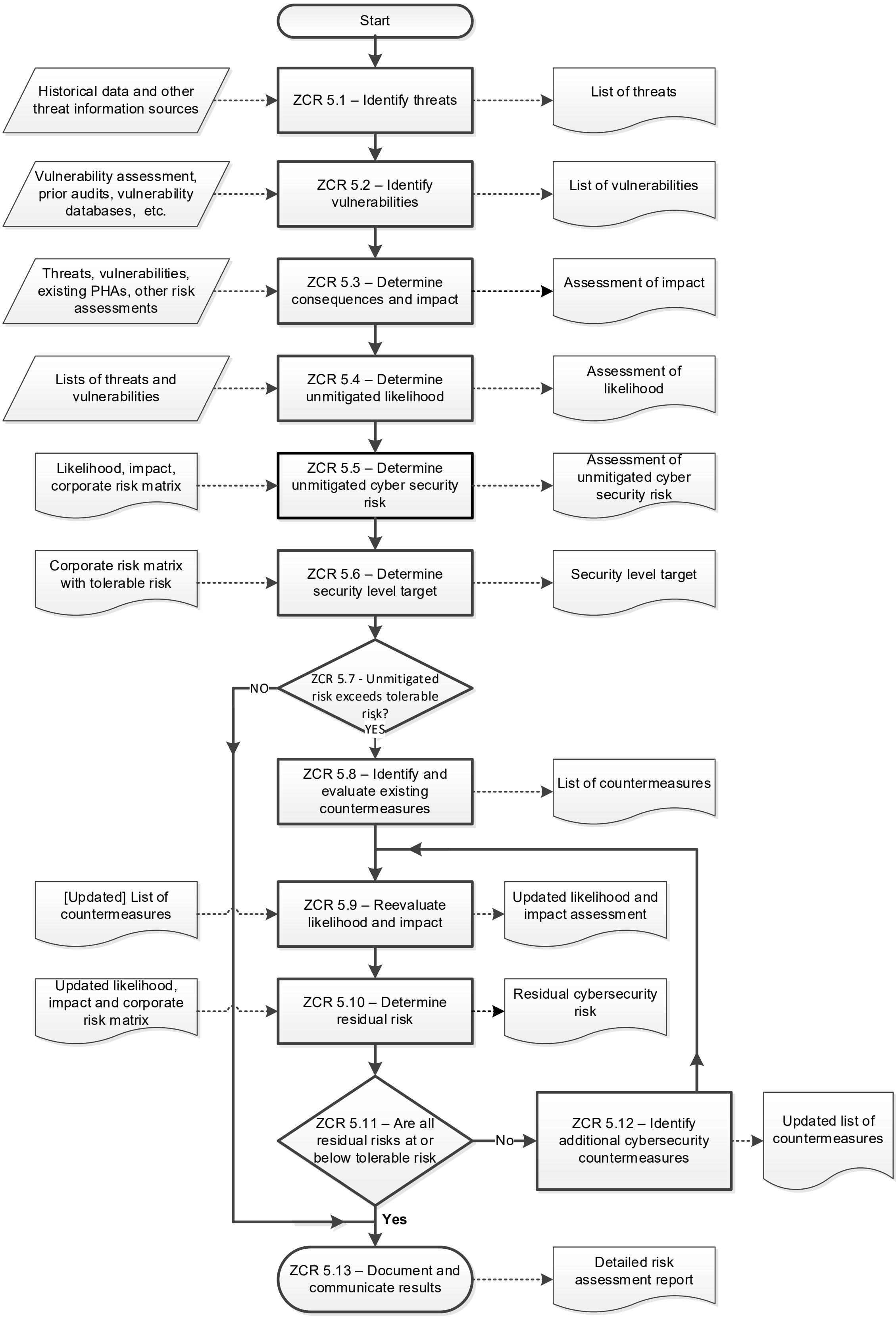


Figure 2 – Detailed cybersecurity risk assessment workflow per zone or conduit

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 personnel logically accesses the process control zone using an infected laptop; and
- A non-malicious employee opens a phishing email compromising his 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 in 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 in 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 for additional information on IACS cybersecurity vulnerability assessments.

Additionally, there are numerous sources of information regarding known and common vulnerabilities in IACS, such as ICS-CERT, IACS vendors, 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 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 advance to the next threat.

Existing PHA and other related risk assessments (such as, information technology, 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 Informative Annex B for examples).

4.6.5 ZCR-5.4: Determine unmitigated likelihood

4.6.5.1 Recommendation

Each threat should 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 Informative Annex B for examples).

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 cybersecurity countermeasures for the zone or conduit being evaluated should not be considered when determining unmitigated likelihood. However, the likelihood determination recognizes countermeasures that are inherent to IACS components and any non-cyber independent protection layers (IPLs) such as physical security or mechanical safeguards (such as, pressure safety valves) 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 ZCR-5.9 taking into account existing countermeasures and their effectiveness in order to determine residual risk.

4.6.6 ZCR-5.5: Determine unmitigated cybersecurity risk

4.6.6.1 Requirement

The unmitigated cybersecurity risk for each threat shall be determined by combining the impact measure determined in ZCR-5.3 and the unmitigated likelihood measure determined in ZCR-5.4.

4.6.6.2 Rationale and supplemental guidance

Determination of unmitigated cybersecurity 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 Informative Annex B for examples).

4.6.7 ZCR-5.6: Determine security level target (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 cybersecurity.

SL-T may be expressed as a single value or a vector. Refer to IEC 62443-3-3 Annex A [10] for a discussion of the SL vector approach.

There is no prescribed method for establishing SL-T. Some organizations chose to establish SL-T based upon the difference between the unmitigated cybersecurity risk and tolerable risk. Whereas others elect to establish SL-T based on the SL definitions provided in Informative Annex A and IEC 62443-3-3 [10].

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 ZCR-5.5 shall be compared to the organization's tolerable risk. If the unmitigated risk exceeds the tolerable risk, the organization shall continue to evaluate the threat by completing ZCR-5.8 through ZCR-5.12. Otherwise, the organization may document the results in ZCR-5.13 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.

IEC 62443-3-3 [10] provides guidance on types of countermeasures and their effectiveness by assigning a security level capability (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 reevaluated considering the countermeasures and their effectiveness.

4.6.10.2 Rationale and supplemental guidance

The unmitigated likelihood determined in ZCR-5.4 did not account for existing countermeasures. In this step, countermeasures are considered and used to determine mitigated likelihood. Likewise, the consequences and impact determined in ZCR-5.3 should also be reevaluated 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 ZCR-5.1 shall be determined by combining the mitigated likelihood measure and mitigated impact values determined in ZCR-5.9.

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 ZCR-5.1 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.

4.6.13 ZCR-5.12: Identify additional cybersecurity countermeasures

4.6.13.1 Requirement

Additional cybersecurity countermeasures 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. Cybersecurity countermeasures may be both technical and non-technical (such as, policies and procedures).

IEC 62443-3-3 can be used as a guide to select appropriate technical countermeasures. The countermeasures identified in IEC 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

Cybersecurity risk assessments need to be documented and made available to the appropriate personnel in the organization. Cybersecurity 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 cybersecurity requirements, assumptions and constraints

4.7.1 Overview

The following sections describe the requirements for documenting cybersecurity requirements, assumptions and constraints within the SUC as needed to achieve the security level target (SL-T) and provides rationale and supplemental guidance for each requirement.

4.7.2 ZCR-6.1: Cybersecurity requirements specification

4.7.2.1 Requirement

A cybersecurity 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:

- SUC description (see 4.7.3)
- Zone and conduit drawings (see 4.7.4)
- Zone and conduit characteristics (see 4.7.5)

- Operating environment assumptions (see 4.7.6)
- Threat environment (see 4.7.7)
- Organizational security policies (see 4.7.8)
- Tolerable risk (see 4.7.9)
- Regulatory requirements (see 4.7.10)

4.7.2.2 Rationale and supplemental guidance

Cybersecurity 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 cybersecurity requirements section in other requirements and relevant IACS documents.

Note: ISA TR84.00.09 provides additional guidance on the recommended elements ***in a C****RS.*

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:

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

f) 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:

g) Name and/or unique identifier;

h) Accountable organization(s);

i) Definition of logical boundary;

j) Definition of physical boundary, if applicable;

k) Safety designation;

l) List of all logical access points;

m) List of all physical access points;

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

o) Connected zones or conduits;

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

q) SL-T;

r) Applicable security requirements;

s) Applicable security policies; and

t) 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:

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

v) **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.

w) **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.

x) **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.

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

z) **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.

aa) **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.

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

cc) **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.

dd) **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.

ee) **Target Security Level (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 ZCR-5.6 for further information.

ff) **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 ZCR-5)

gg) **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.

hh) **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, 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 readiness teams (CERTs);
- Industrial Control Systems Cyber Emergency Response Team (ICS-CERT);
- Public-Private partnerships such as Information Sharing and Analysis Centers (ISACs);
- IACS vendors;
- 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 risk level of the SUC is in alignment.

4.7.10 ZCR-6.9: Regulatory requirements

4.7.10.1 Requirement

Any relevant cybersecurity 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 ZCR-7.1: Attain asset owner approval

4.8.1.1 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.

4.8.1.2 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 must be presented to the appropriate management with the authority to make such decisions.

Annex A
(informative)

Security Levels

IEC 62443-3-3 [10] defines security levels (SLs) in terms of five different levels (0, 1, 2, 3 and 4), each with an increasing level of security.

- SL 0: No specific 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.

Security levels have been categorized by IEC 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 the IEC 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.

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 (e.g. 3 x 3, 4 x 4, 3 x 5, 5 x 5) depending on the number of categories in the likelihood and severity scales.

Figure 3 is an example of a 3 x 5 risk matrix.

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

Figure 3 – Example of a 3 x 5 risk matrix

A likelihood scale partitions entire range of likelihood values into discrete categories or bins. Table 1 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 1 – 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 no 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, it can be assumed it will not occur	<10-5 per year

Similarly, a consequence or severity scale partitions entire range of severity values into discrete categories or bins. Table 1 is an example of a category 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.

	Operational			Financial				HSE		
Category	Outage at One Site	Outage at Multiple Sites	National Infrastructure and Services	Cost (Million USD)	Legal	Regulatory	Public Confidence	People, On Site	People, Off Site	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 of Major Community Incident	Citation by Regional Agency or Long-Term Significant Damage over Large Area
B (Medium)	< 2 Days	> 1 Hour	Potential to Impact a Sector at a Level Beyond the Company	> 5	Mis-demeanor 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

Figure 4 – Example of consequence or severity scale

Although some standard risk matrices exist in different contexts individual projects and organizations typically create their own or tailor an existing risk matrix. This informative annex provides several additional risk matrix examples 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.

Likelihood \ Impact	Negligible	Moderate	Severe
Highly Likely	MED	HIGH	HIGH
Possible	LOW	MED	HIGH
Unlikely	LOW	LOW	MED

Figure 5 – Example of a simple 3 x 3 risk matrix

		Consequence				
		Minor Problem easily handled by normal day to day processes	Some Disruption Possible (e.g., damage between $500K and $1 Million)	Significant Time & Resources Required (e.g., damage between $1 Million and $10 Million)	Operations Severely Damaged (e.g., between $10 Million and $25 Million)	Business Survival is at Risk (e.g., damage > $25 Million
Likelihood	**Almost Certain** (e.g., Greater than 90%)	High	High	Extreme	Extreme	Extreme
	Likely (e.g., Between 50% and 90%)	Moderate	High	High	Extreme	Extreme
	Moderate (e.g., Between 10% and 50%)	Low	Moderate	High	Extreme	Extreme
	Unlikely (e.g., From 3% to 10%)	Low	Low	Moderate	High	Extreme
	Rare (e.g., < 3% Chance)	Low	Low	Moderate	High	High

Figure 6 – Example of a 5 x 5 risk matrix

		Severity			
		Acceptable Little or No Effect On Event	**Tolerable** Effects are Felt, But Not Critical to Outcome	**Indesirable** Serious Impact to the Course of Sction or 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 -

Figure 7 – Example of a 3 x 4 matrix

BIBLIOGRAPHY

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

References to other parts, both existing and in progress, of the IEC 62443 series:

NOTE 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 IEC-IEC 62443 series.

[1] ANSI/IEC 62443-1-1 (99.01.01) – *Security for industrial automation and control systems – Part 1-1: Models and concepts*[1]

[2] IEC/TR 62443-1-2 – *Security for industrial automation and control systems – Part 1-2: Master glossary of terms and abbreviations*

[3] IEC/TS 62443-1-3 – *Security for industrial automation and control systems – Part 1-3: System security compliance metrics*

[4] IEC/TR 62443-1-4 – *Security for industrial automation and control systems – Part 1-4: Security life cycle and use cases*

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

[6] IEC/TR 62443-2-2 – *Security for industrial automation and control systems – Part 2-2: Implementation guidance for an IACS security management system*

[7] IEC/TR 62443-2-3 – *Security for industrial automation and control systems – Part 2-3: Patch management in the IACS environment*

[8] IEC 62443-2-4 – *Security for industrial automation and control systems – Part 2-4: Requirements for IACS solution suppliers*

[9] IEC/TR 62443-3-1 – *Security for industrial automation and control systems – Part 3-1: Security technologies for IACS*[1]

NOTE This standard is IEC 62443-3-2 – Security for industrial automation and control systems – Part 3-2: Security risk assessment and system design

[10] IEC 62443-3-3 – *Security for industrial automation and control systems – Part 3-3: System security requirements and security levels*

[11] IEC 62443-4-1 – *Security for industrial automation and control systems – Part 4-1: Product development requirements*

[12] IEC 62443-4-2 – *Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components*

[13] ISA-TR84.00.09 – Cybersecurity Related to the Functional Safety Lifecycle

Other standards references:

[14] ISO/IEC Directives, Part 2, *Rules for the structure and drafting of International Standards*

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

---

[1] Currently under revision.

[16] ISO/IEC 27005 – *Information technology – Security techniques – Information security risk management*

[17] ISO 31000:2009 – *Risk management – Principles and guidelines*

[18] IEC 61511-1:2003 – *Functional safety – Safety instrumented systems for the process industry sector – Part 1: Framework, definitions, system, hardware and software requirements*

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

[20] NIST Special Publication (SP) 800-39 – *Guide for Applying the Risk Management Framework*