IEC 62443-3-2

Edition 1.0 2020-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

IECNORM.COM : Click to view the full PDF of IEC 62443-3-2:2020

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

Sécurité des systèmes d'automatisation et de commande industriels – Partie 3-2: Évaluation des risques de sécurité pour la conception des systèmes

IEC 62443-3-2:2020-06(en-fr)

THIS PUBLICATION IS COPYRIGHT PROTECTED
Copyright © 2020 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

IECNORM.COM : Click to view the full PDF of IEC 62443-3-2:2020

About the IEC
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
67 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

A propos de l'IEC
La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications IEC
Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Recherche de publications IEC - webstore.iec.ch/advsearchform
La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études,…). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished
Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et une fois par mois par email.

Service Clients - webstore.iec.ch/csc
Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: sales@iec.ch.

Electropedia - www.electropedia.org
Le premier dictionnaire d'électrotechnologie en ligne au monde, avec plus de 22 000 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 16 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary
67 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et Définitions des publications IEC parues depuis 2002. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

IEC 62443-3-2

Edition 1.0 2020-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

IECNORM.COM : Click to view the full PDF of IEC 62443-3-2:2020

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

Sécurité des systèmes d'automatisation et de commande industriels – Partie 3-2: Évaluation des risques de sécurité pour la conception des systèmes

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

ICS 25.040.40; 35.030

ISBN 978-2-8322-8613-5

Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.

® Registered trademark of the International Electrotechnical Commission
Marque déposée de la Commission Electrotechnique Internationale

CONTENTS

IECNORM.COM : Click to view the full PDF of IEC 62443-3-2:2020

IECNORM.COM : Click to view the full PDF of IEC 62443-3-2:2020

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –

Part 3-2: Security risk assessment for 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 IEC technical committee 65: Industrial-process measurement, control and automation.

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

FDIS	Report on voting
65/799/FDIS	65/804/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.

IECNORM.COM : Click to view the full PDF of IEC 62443-3-2:2020

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.

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.

IECNORM.COM : Click to view the full PDF of IEC 62443-3-2:2020

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 IEC TS 62443-1-1.

This document has been developed in cooperation with the ISA99 liaison. ISA99 is the committee on Industrial Automation and Control Systems Security of the International Society of Automation (ISA).

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

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

IECNORM.COM : Click to view the full PDF of IEC 62443-3-2:2020

SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –

Part 3-2: Security risk assessment for system design

1 Scope

This part of IEC 62443 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

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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 62443-3-3:2013, *Industrial communication networks – Network and system security – 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 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.

IECNORM.COM : Click to view the full PDF of IEC 62443-3-2:2020

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

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 document 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

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.

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.

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).

IECNORM.COM : Click to view the full PDF of IEC 62443-3-2:2020

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 73:2009 [13][1], 3.6.1.1 and ISO/IEC 27005:2018 [12], 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)

IECNORM.COM : Click to view the full PDF of IEC 62443-3-2:2020

[1] Numbers in square brackets refer to the bibliography.

3.1.20
threat source
intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that can 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 [14] and NIST 800-39 [16].

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

The list below 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

IECNORM.COM : Click to view the full PDF of IEC 62443-3-2:2020

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

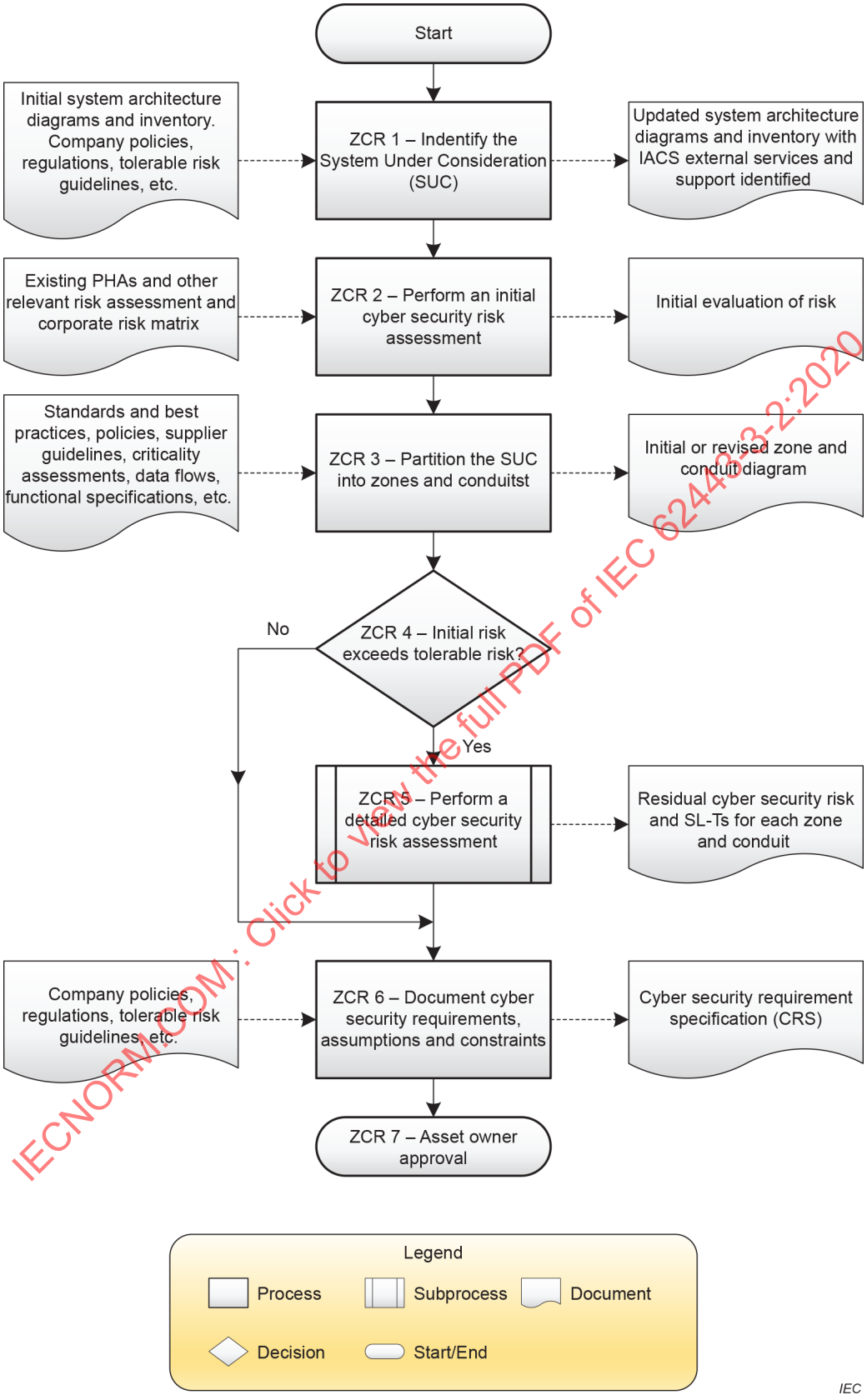
This document uses flowcharts to illustrate the workflow between requirements. These flowcharts are informative. Alternate workflows may be used.

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 Clause 4 are referred to as zone and conduit requirements (ZCR). Clause 4 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, as well as to assess risk. The steps are numbered to indicate their relationship to the ZCRs.

IECNORM.COM : Click to view the full PDF of IEC 62443-3-2:2020



IECNORM.COM : Click to view the full PDF of IEC 62443-3-2:2020

Figure 1 – 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 61511-2 [8] 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.

IECNORM.COM : Click to view the full PDF of IEC 62443-3-2:2020

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 provide rationale and supplemental guidance for each requirement. Subclause 4.4.2, sets out the base requirement for establishing zones and conduits within the SUC. Subclauses 4.4.3 through 4.4.7 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 IEC 62264-1 [9] 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.

IECNORM.COM : Click to view the full PDF of IEC 62443-3-2:2020

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 included 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.

IECNORM.COM : Click to view the full PDF of IEC 62443-3-2:2020

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 4.3 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 4.6.

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 analyse 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 2 illustrates the cybersecurity risk assessment workflow.

Any detailed risk assessment methodology (such as, ISO 31000 [14], NIST SP 800-39 [16], and ISO/IEC 27005 [12]) 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 have to use a consistent risk ranking scale in order to produce consistent and coherent results.

IECNORM.COM : Click to view the full PDF of IEC 62443-3-2:2020

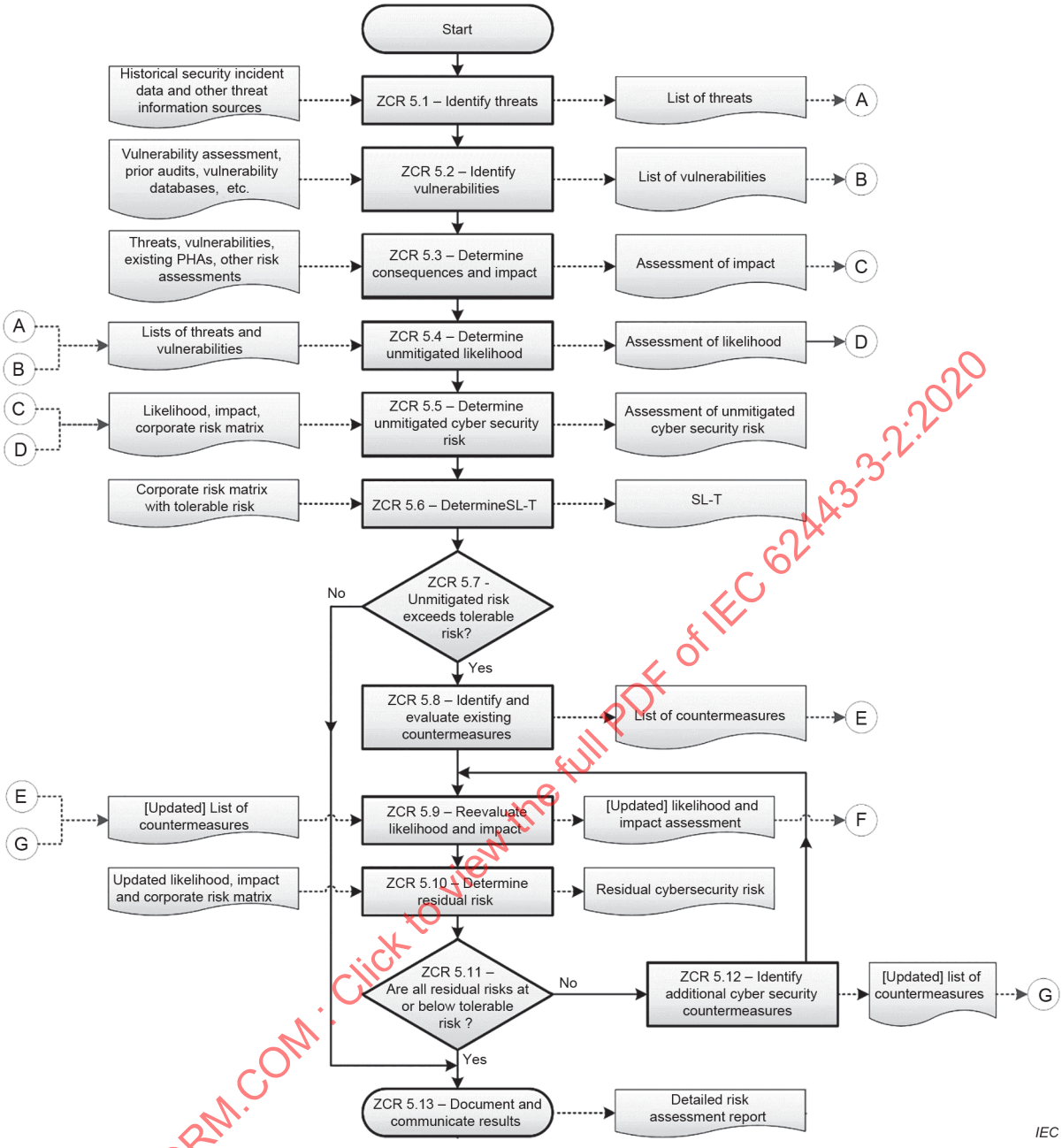


Figure 2 – Detailed cyber security risk assessment workflow per zone or conduit

IECNORM.COM : Click to view the full PDF of IEC 62443-3-2:2020

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 analysed 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. Additional information on IACS cyber security vulnerability assessments is available in ISA-TR84.00.09 [15].

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).

IECNORM.COM : Click to view the full PDF of IEC 62443-3-2:2020

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 document.

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 4.6.10, 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 document. 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 4.6.4, and the unmitigated likelihood measure determined in 4.6.5.

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.

IECNORM.COM : Click to view the full PDF of IEC 62443-3-2:2020

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 IEC 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 chose 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 IEC 62443-3-3:2013. 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 4.6.6, 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 4.6.9 through 4.6.13. Otherwise, the organization may document the results in 4.6.14 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 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.

IECNORM.COM : Click to view the full PDF of IEC 62443-3-2:2020

4.6.10.2 Rationale and supplemental guidance

The unmitigated likelihood determined in 4.6.5 does 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 4.6.4 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 4.6.2, shall be determined by combining the mitigated likelihood measure and mitigated impact values determined in 4.6.10.

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 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.

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.

IECNORM.COM : Click to view the full PDF of IEC 62443-3-2:2020

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 should 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 should 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.

IECNORM.COM : Click to view the full PDF of IEC 62443-3-2:2020

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:

IECNORM.COM : Click to view the full PDF of IEC 62443-3-2:2020

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 can be different. If so, they will 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 4.6.7 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 4.6).

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.

IECNORM.COM : Click to view the full PDF of IEC 62443-3-2:2020

4.7.6.2 Rationale and supplemental guidance

The physical environment for the SUC should 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 should 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 can 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 can 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.

IECNORM.COM : Click to view the full PDF of IEC 62443-3-2:2020

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.

IECNORM.COM : Click to view the full PDF of IEC 62443-3-2:2020

Annex A
(informative)

Security levels

IEC 62443-4-2 [7] 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 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 to IEC 62443 (all parts). 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.

IECNORM.COM : Click to view the full PDF of IEC 62443-3-2:2020

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 colour-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.

IECNORM.COM : Click to view the full PDF of IEC 62443-3-2:2020

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 recorda-ble 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. Annex B 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, colour 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				
	Highly likely	Medium	High	High
	Possible	Low	Medium	High
	Unlikely	Low	Low	Medium
		Negligible	Moderate impact	Severe

IECNORM.COM : Click to view the full PDF of IEC 62443-3-2:2020

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 $ 500 k and $ 1 MM)	Significant time and resources required (Damage between $ 1 MM and $ 10 MM)	Operations severely damaged (Damage between $ 10 MM and $ 25 MM)	Business survival at risk (Damage >$ 25 MM)
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 -

IECNORM.COM : Click to view the full PDF of IEC 62...

Bibliography

References to other parts of the IEC 62443 series:

[1] IEC TS 62443-1-1, *Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models*

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

[3] IEC TR 62443-2-3:2015, *Security for industrial automation and control systems – Part 2-3: Patch management in the IACS environment*

[4] IEC 62443-2-4:2015, *Security for industrial automation and control systems – Part 2-4: Security program requirements for IACS service providers*
IEC 62443-2-4:2015/AMD1:2017

[5] IEC TR 62443-3-1:2009, *Industrial communication networks – Network and system security – Part 3-1: Security technologies for industrial automation and control systems*

[6] IEC 62443-4-1:2018, *Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements*

[7] IEC 62443-4-2:2019, *Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components*

Other standards references:

[8] IEC 61511-2:2016, *Functional safety – Safety instrumented systems for the process industry sector – Part 2: Guidelines for the application of IEC 61511-1: 2016*

[9] IEC 62264-1:2013, *Enterprise-control system integration – Part 1: Models and terminology*

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

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

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

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

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

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

IECNORM.COM : Click to view the full PDF of IEC 62443-3-2:2020

SOMMAIRE

IECNORM.COM : Click to view the full PDF of IEC 62443-3-2:2020

IECNORM.COM : Click to view the full PDF of IEC 62443-3-2:2020

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

SÉCURITÉ DES SYSTÈMES D'AUTOMATISATION ET DE COMMANDE INDUSTRIELS –

Partie 3-2: Évaluation des risques de sécurité pour la conception des systèmes

AVANT-PROPOS

1) La Commission Électrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. À cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

La Norme internationale IEC 62443-3-2 a été établie par le comité d'études 65 de l'IEC: Mesure, commande et automation dans les processus industriels.

La présente version bilingue (2020-07) correspond à la version anglaise monolingue publiée en 2020-06.

La version française de cette norme n'a pas été soumise au vote.

Ce document a été rédigé selon les Directives ISO/IEC, Partie 2.

IECNORM.COM : Click to view the full PDF of IEC 62443-3-2:2020

Une liste de toutes les parties de la série de normes IEC 62443, publiées sous le titre général *Sécurité des systèmes d'automatisation et de commande industriels*, peut être consultée sur le site web de l'IEC.

Le comité a décidé que le contenu de ce document ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous "http://webstore.iec.ch" dans les données relatives au document recherché. À cette date, le document sera

- reconduit,
- supprimé,
- remplacé par une édition révisée, ou
- amendé.

IMPORTANT – Le logo "colour inside" qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer cette publication en utilisant une imprimante couleur.

IECNORM.COM : Click to view the full PDF of IEC 62443-3-2:2020

INTRODUCTION

Il n'existe pas de solution simple pour sécuriser un système d'automatisation et de commande industriel (IACS, *industrial automation and control system*), et la raison en est connue. Cela est dû au fait que la sécurité est une question de management du risque. Chaque IACS présente un risque différent pour l'organisation, selon les menaces auxquelles elle est exposée, de la vraisemblance de ces menaces, des vulnérabilités inhérentes au système et des conséquences dans le cas où le système est compromis. De plus, chaque organisation qui possède et exploite un IACS présente une tolérance au risque qui est différente.

Le présent document s'efforce de définir un ensemble de mesures d'ingénierie pour guider une organisation dans le processus d'appréciation du risque d'un IACS particulier, et d'identification et d'application de contremesures de sécurité afin de réduire ce risque à des niveaux tolérables.

Un concept clé du présent document est l'application de zones de sécurité et conduits de l'IACS. Les zones et les conduits sont présentés dans l'IEC TS 62443-1-1.

Le présent document a été élaboré en coopération avec la liaison ISA99. L'ISA99 est le comité sur la sécurité des systèmes d'automatisation et de commande industriels de l'International Society of Automation (ISA).

Ce document concerne le propriétaire de l'actif, l'intégrateur du système, le fournisseur du produit, le fournisseur de services et l'autorité de conformité.

Le présent document fournit une base pour spécifier les contremesures de sécurité, en alignant les niveaux de sécurité cibles (SL-T) identifiés dans le présent document avec les niveaux de sécurité de capacité exigée (SL-C) spécifiés dans l'IEC 62443-3-3.

IECNORM.COM : Click to view the full PDF of IEC 62443-3-2:2020

SÉCURITÉ DES SYSTÈMES D'AUTOMATISATION ET DE COMMANDE INDUSTRIELS –

Partie 3-2: Évaluation des risques de sécurité pour la conception des systèmes

1 Domaine d'application

La présente partie de l'IEC 62443 établit les exigences concernant:

- la définition d'un système à l'étude (SUC, *system under consideration*) pour un système d'automatisation et de commande industriel (IACS);
- la division du SUC en zones et conduits;
- l'appréciation du risque pour chaque zone et conduit;
- l'établissement d'un niveau de sécurité cible (SL-T) pour chaque zone et conduit; et
- la documentation des exigences de sécurité.

2 Références normatives

Les documents suivants cités dans le texte constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

IEC 62443-3-3:2013, *Réseaux industriels de communication – Sécurité dans les réseaux et les systèmes – Partie 3-3: Exigences de sécurité des systèmes et niveaux de sécurité*

3 Termes, définitions, abréviations, acronymes et conventions

3.1 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

- ISO Online browsing platform: disponible à l'adresse https://www.iso.org/obp
- IEC Electropedia: disponible à l'adresse http://www.electropedia.org/

3.1.1
voie de communication
lien de communication logique ou physique spécifique entre les actifs

Note 1 à l'article: Une voie de communication facilite l'établissement d'une connexion.

3.1.2
autorité de conformité
entité compétente en matière de détermination de l'adéquation d'une évaluation de sécurité ou de l'efficacité de la mise en œuvre spécifiée dans un document de gouvernance

Note 1 à l'article: Les autorités de conformité incluent, par exemple, les agences gouvernementales, les organismes de réglementation et les vérificateurs externes et internes.

IECNORM.COM : Click to view the full PDF of IEC 62443-3-2:2020

3.1.3
conduit
groupement logique de voies de communication partageant des exigences de sécurité communes et connectant deux ou plusieurs zones

3.1.4
confidentialité
préservation des restrictions autorisées sur l'accès aux informations et sur leur divulgation, y compris les moyens mis en œuvre pour protéger la confidentialité et les informations exclusives

3.1.5
conséquence
résultat d'un incident, habituellement décrit en fonction des effets sur la santé et la sécurité, des impacts environnementaux, de la perte de propriété, de la perte d'information (par exemple de propriété intellectuelle) et/ou de coûts d'interruption d'activité découlant d'un incident particulier

3.1.6
contremesure
action, appareil, procédure ou technique qui réduit une menace, une vulnérabilité ou les conséquences d'une attaque, en les éliminant ou en les prévenant, en réduisant le plus possible les dommages pouvant être causés ou en les découvrant et en les signalant afin que des mesures correctives puissent être prises

Note 1 à l'article: Le terme "commande" est également utilisé pour décrire ce concept dans certains contextes. Le terme "contremesure" a été choisi pour ce document afin d'éviter toute confusion avec le mot "commande" dans le contexte de "commande de processus".

3.1.7
cybersécurité
mesures prises pour protéger un ordinateur ou un système informatique contre un accès non autorisé ou une attaque

Note 1 à l'article: Les IACS sont des systèmes informatiques.

3.1.8
flux de données
mouvement des données à travers un système composé de logiciels, de matériels ou d'une combinaison des deux

3.1.9
réseau externe
réseau connecté au SUC qui n'en fait pas partie

3.1.10
impact
mesure de la perte ou du dommage ultime associé à une conséquence

EXEMPLE: La conséquence de l'incident était un déversement. L'impact du déversement était une amende de 100 000 $ et des frais de nettoyage de 25 000 $.

Note 1 à l'article: L'impact peut être exprimé en nombre de blessures et/ou de décès, d'ampleur des dommages environnementaux et/ou d'ampleur des pertes telles que les dommages matériels, les pertes matérielles, les pertes de propriété intellectuelle, les pertes de production, les pertes de part de marché et les coûts de récupération.

IECNORM.COM : Click to view the full PDF of IEC 62443-3-2:2020

3.1.11
vraisemblance
possibilité que quelque chose se produise

Note 1 à l'article: Dans la terminologie du management du risque, le mot "vraisemblance" est utilisé pour indiquer la possibilité que quelque chose se produise, que cette possibilité soit définie, mesurée ou déterminée de façon objective ou subjective, qualitative ou quantitative, et qu'elle soit décrite au moyen de termes généraux ou mathématiques (telles une probabilité ou une fréquence sur une période donnée).

Note 2 à l'article: Lors de l'estimation de la vraisemblance dans le cadre du management du risque lié au système d'information, un certain nombre de facteurs sont pris en considération tels que la motivation et les capacités à l'origine des menaces, l'historique de menaces similaires, les vulnérabilités connues, l'attrait de la cible, etc.

[SOURCE: Guide ISO 73:2009 [13][1], 3.6.1.1 et ISO/IEC 27005:2018 [12], 3.7]

3.1.12
analyse des dangers liés aux processus
ensemble d'évaluations organisées et systématiques des dangers potentiels associés à un processus industriel

3.1.13
risque résiduel
risque qui subsiste après la mise en œuvre des contremesures existantes (comme le risque net ou le risque après application des contremesures)

3.1.14
risque
prévision de perte exprimée par la vraisemblance qu'une menace particulière exploite une vulnérabilité particulière avec une conséquence particulière

3.1.15
niveau de sécurité
SL
mesure de confiance indiquant que le système à l'étude (SUC), la zone de sécurité ou le conduit est exempt de vulnérabilités et fonctionne de la manière prévue

Note 1 à l'article: L'abréviation "SL" est dérivée du terme anglais développé correspondant "security level".

3.1.16
périmètre de sécurité
frontière logique ou physique entourant tous les actifs qui sont contrôlés et protégés par la zone de sécurité

3.1.17
système à l'étude
SUC
collection définie d'actifs de l'IACS nécessaire pour fournir une solution d'automatisation complète, y compris les actifs d'infrastructure réseau pertinents

Note 1 à l'article: Un SUC est constitué d'une ou plusieurs zones et conduits associés. Tous les actifs d'un SUC appartiennent à une zone ou à un conduit.

Note 2 à l'article: L'abréviation "SUC" est dérivée du terme anglais développé correspondant "system under consideration".

IECNORM.COM : Click to view the full PDF of IEC 62443-3-2:2020

[1] Les chiffres entre crochets se réfèrent à la bibliographie

3.1.18
menace
circonstance ou événement de nature à avoir un impact préjudiciable sur les opérations de l'organisation (y compris sa mission, ses fonctions, son image ou sa réputation) et/ou les actifs de l'organisation, y compris l'IACS

Note 1 à l'article: Les circonstances incluent les personnes qui, ne respectant pas la politique de sécurité, empêchent intentionnellement ou involontairement l'accès aux données ou provoquent la destruction, la divulgation ou la modification de données telles que la logique ou les paramètres de contrôle, la logique ou les paramètres de protection ou les diagnostics.

3.1.19
environnement de menace
résumé des informations sur les menaces, incluant les sources de menace, les vecteurs et les tendances de menaces susceptibles d'avoir un impact préjudiciable sur une cible définie (par exemple, une entreprise, une installation ou un SUC)

3.1.20
source de menace
intention et méthode visant l'exploitation intentionnelle d'une vulnérabilité ou d'une situation et d'une méthode pouvant exploiter accidentellement une vulnérabilité

3.1.21
vecteur de menace
chemin d'accès ou moyen par lequel une source de menace peut accéder à un actif

3.1.22
risque tolérable
niveau de risque jugé acceptable pour une organisation

Note 1 à l'article: Il convient que les organisations tiennent compte des exigences légales lorsqu'elles établissent le risque tolérable. Des recommandations supplémentaires relatives à l'établissement des risques tolérables peuvent être consultées dans les normes ISO 31000 [14] et NIST 800-39 [16].

3.1.23
risque de cybersécurité non atténué
niveau de risque de cybersécurité présent dans un système avant application de toute contremesure de cybersécurité

Note 1 à l'article: Ce niveau permet d'identifier l'ampleur de la réduction du risque de cybersécurité fournie par toute contremesure.

3.1.24
vulnérabilité
faille ou faiblesse dans la conception, la mise en œuvre ou l'utilisation et la gestion d'un système, qui peut être exploitée dans le but de violer l'intégrité ou la politique de sécurité du système

3.1.25
zone
regroupement d'actifs logiques ou physiques fondé sur le risque ou sur d'autres critères tels que la criticité des actifs, la fonction opérationnelle, l'emplacement physique ou logique, l'accès exigé (par exemple, les principes du droit d'accès minimal) ou l'organisation responsable

Note 1 à l'article: Ensemble d'actifs logiques ou physiques qui représentent la division d'un système à l'étude, sur la base de leurs exigences communes en matière de sécurité, de leur criticité (par exemple, impact financier élevé, impact sur la santé, la sécurité ou l'environnement), leurs fonctionnalités et leurs relations logiques et physiques (y compris leur emplacement).

IECNORM.COM : Click to view the full PDF of IEC 62443-3-2:2020

3.2 Abréviations et acronymes

La liste ci-dessous définit les abréviations et les acronymes utilisés dans le présent document.

ANSI	American National Standards Institute (Institut national américain de normalisation)
BPCS	Basic process control system (Système de commande de processus de base)
CERT	Computer emergency response team (Équipe de réaction en informatique)
CRS	Cybersecurity requirements specification (Spécification des exigences de cybersécurité)
DCS	Distributed Control System (Système à commande distribuée)
IHM	Interface homme-machine
HSE	Health, safety and environment (Santé, sécurité et environnement)
HVAC	Heating, ventilation and air-conditioning (Chauffage, ventilation et climatisation)
IACS	Industrial automation and control system(s) (Système(s) d'automatisation et de commande industriels)
ICS-CERT	Industrial control system CERT (Système de commande industriel CERT)
IEC	International Electrotechnical Commission (Commission électrotechnique internationale)
IIoT	Industrial Internet of Things (Internet des objets industriel)
IPL	Independent protection layer (Couche de protection indépendante)
ISA	International Society of Automation (Société internationale d'automatisation)
ISAC	Information Sharing and Analysis Centers (Centres d'échange et d'analyse d'informations)
ISO	International Organization for Standardization (Organisation internationale de normalisation)
MES	Manufacturing execution system (Système industriel d'exécution)
NIST	[États-Unis] National Institute of Standards and Technology (Institut national des sciences et de la technologie)
PHA	Process hazard analysis (Analyse des dangers liés aux processus)
PLC	Programmable logic controller (Automate programmable)
RTU	Remote terminal unit (Terminal à distance)
SCADA	Supervisory control and data acquisition (Système de supervision, contrôle et acquisition de données)
SIS	Safety Instrumented Systems (Systèmes de sécurité instrumentés)
SUC	System under consideration (Système à l'étude)
SL	Security level (Niveau de sécurité)
SL-A	Achieved SL (Niveau de sécurité atteint)
SL-C	Capability SL (Niveau de sécurité de capacité)
SL-T	Target SL (Niveau de sécurité cible)
SP	[NIST États-Unis] Special Publication (Publication spéciale)
USB	Universal serial bus (Bus série universel)

IECNORM.COM : Click to view the full PDF of IEC 62443-3-2:2020

ZCR Zone and conduit requirement (Exigence de zone et conduit)

3.3 Conventions

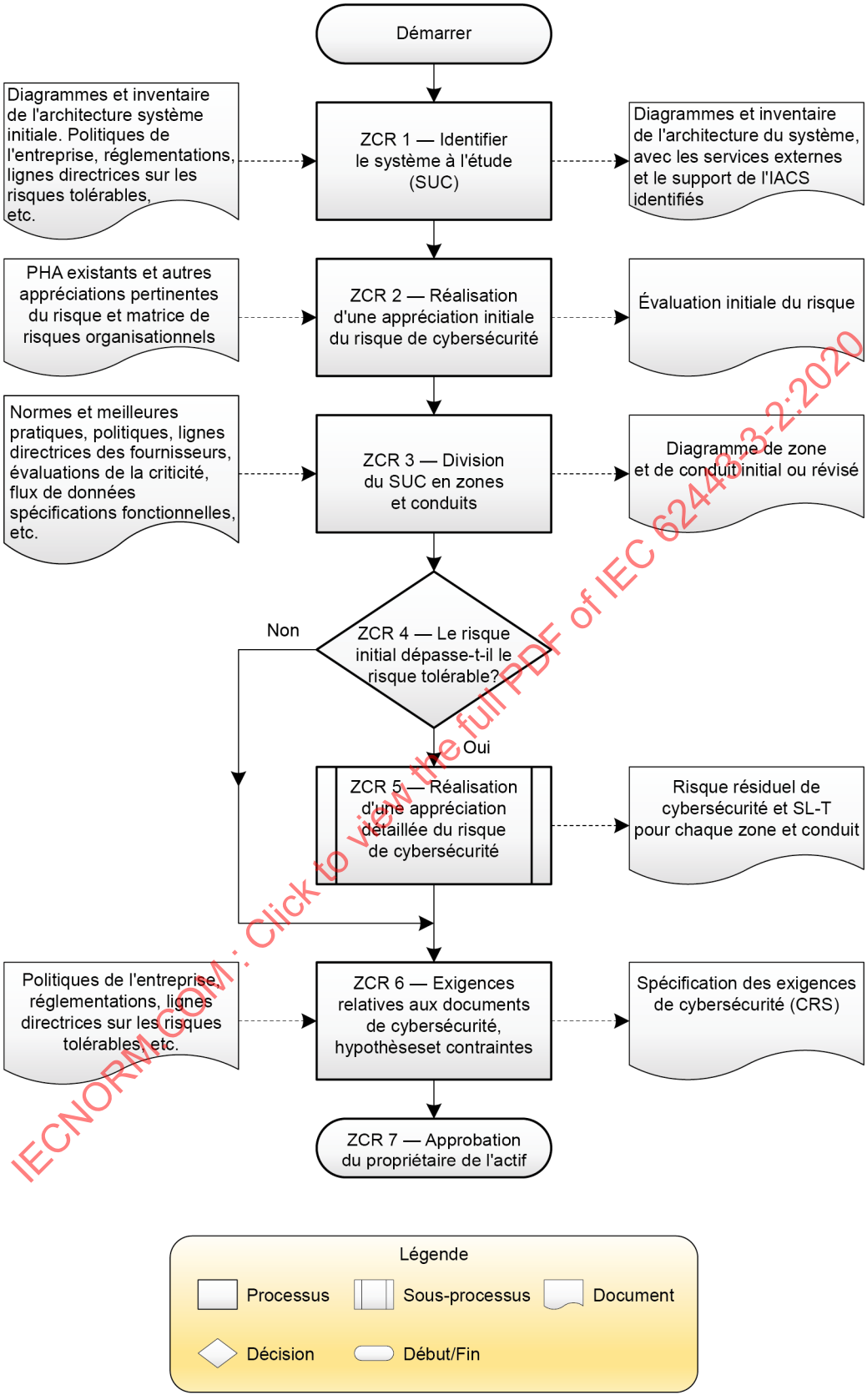
Le présent document utilise des organigrammes pour représenter le flux de travail entre les exigences. Ces organigrammes sont informatifs. D'autres flux de travail peuvent être utilisés.

4 Exigences en matière d'évaluation des zones, des conduits et des risques

4.1 Vue d'ensemble

L'Article 4 décrit les exigences pour la division d'un SUC en zones et conduits, ainsi que les exigences pour évaluer le risque de cybersécurité et déterminer le SL-T pour chaque zone et conduit définis. Les exigences présentées à l'Article 4 sont appelées exigences de zone et de conduit (ZCR). L'Article 4 fournit également une justification et des recommandations supplémentaires relatives à chacune des exigences. La Figure 1 représente un diagramme de flux de travail décrivant les principales étapes exigées pour établir des zones et des conduits et évaluer les risques. Les étapes sont numérotées pour indiquer leur relation avec les ZCR.

IECNORM.COM : Click to view the full PDF of IEC 62443-3-2:2020



IECNORM.COM : Click to view the full PDF of IEC 62443-3-2:2020

Figure 1 – Diagramme de flux de travail décrivant les principales étapes exigées pour établir des zones et des conduits et évaluer les risques

4.2 ZCR 1: Identifier le SUC

4.2.1 ZCR 1.1: Identifier le périmètre SUC et les points d'accès

4.2.1.1 Exigence

L'organisation doit clairement identifier le SUC, délimiter clairement le périmètre de sécurité et identifier tous les points d'accès au SUC.

4.2.1.2 Justification et recommandations supplémentaires

Les organisations possèdent et exploitent généralement plusieurs systèmes de commande, en particulier les grandes organisations possédant plusieurs installations industrielles. Chacun de ces systèmes de commande peut être défini comme un SUC. Par exemple, il y a généralement au moins un système de commande dans une installation industrielle, mais il y a souvent plusieurs systèmes qui commandent différentes fonctions au sein de l'installation.

Cette exigence précise que les SUC sont identifiés dans le but d'effectuer des analyses de cybersécurité. La définition d'un SUC est destinée à inclure tous les actifs de l'IACS nécessaires pour fournir une solution d'automatisation complète.

Les diagrammes d'inventaire et d'architecture du système, les diagrammes de réseau et les flux de données peuvent être utilisés pour déterminer et représenter les actifs de l'IACS inclus dans la description du SUC.

NOTE Le SUC peut inclure plusieurs sous-systèmes tels que les systèmes de commande de processus de base (BPCS), les systèmes à commande distribuée (DCS), les systèmes de sécurité instrumentés (SIS), les systèmes de supervision, contrôle et acquisition de données (SCADA) et les paquetages de fournisseurs de produits IACS. Cela peut également inclure les technologies émergentes telles que l'Internet des objets industriel (IIoT) ou les solutions fondées sur le cloud.

4.3 ZCR 2: Appréciation initiale du risque de cybersécurité

4.3.1 ZCR 2.1: Réalisation d'une appréciation initiale du risque de cybersécurité

4.3.1.1 Exigence

L'organisation doit effectuer une appréciation du risque de cybersécurité du SUC ou confirmer qu'une appréciation initiale précédente du risque de cybersécurité est toujours applicable, afin d'identifier le risque de cybersécurité non atténué le plus défavorable qui peut résulter de l'interférence avec des opérations critiques de l'IACS, d'infractions ou de perturbations de l'IACS ou de sa désactivation.

4.3.1.2 Justification et recommandations supplémentaires

L'objectif de l'appréciation initiale du risque de cybersécurité est d'appréhender initialement le risque le plus défavorable que le SUC représente pour l'organisation s'il est compromis. Elle est généralement évaluée par rapport à l'impact sur la santé, la sécurité, l'environnement, l'interruption des activités, la perte de production, la qualité des produits, les aspects financiers, juridiques, réglementaires, la réputation, etc. Cette appréciation aide à hiérarchiser les appréciations détaillées du risque, et facilite le regroupement des actifs dans les zones et les conduits au sein du SUC.

Pour les processus potentiellement dangereux, il convient que les résultats de l'analyse des dangers liés aux processus (PHA) et les évaluations de sécurité fonctionnelle définies dans l'IEC 61511-2 [8] soient référencés dans le cadre de l'appréciation initiale du risque de cybersécurité, afin d'identifier les impacts les plus défavorables. Il convient, pour les organisations, de prendre également en considération les renseignements sur les menaces émanant des gouvernements, des centres d'échange et d'analyse d'informations (ISAC) sectoriels et d'autres sources pertinentes.

IECNORM.COM : Click to view the full PDF of IEC 62443-3-2:2020

L'appréciation initiale du risque est souvent réalisée à l'aide d'une matrice de risques qui établit la relation entre la vraisemblance, l'impact et le risque (comme une matrice de risques organisationnels). L'Annexe B donne des exemples de matrices de risques.

4.4 ZCR 3: Division du SUC en zones et conduits

4.4.1 Vue d'ensemble

Les paragraphes 4.4.2 à 4.8.1 décrivent les ZCR pour diviser le SUC en zones et conduits, et fournissent une justification et des recommandations supplémentaires pour chaque exigence. Le paragraphe 4.4.2 stipule l'exigence de base pour l'établissement de zones et conduits au sein du SUC. Les paragraphes 4.4.3 à 4.4.7 sont destinés à fournir des recommandations relatives à l'affectation des actifs aux zones, en se fondant sur les meilleures pratiques de l'industrie. Il ne s'agit pas d'une liste exhaustive.

4.4.2 ZCR 3.1: Établissement de zones et conduits

4.4.2.1 Exigence

L'organisation doit regrouper l'IACS et les actifs associés en zones ou en conduits selon le risque déterminé. Le regroupement doit être fondé sur les résultats de l'appréciation initiale du risque de cybersécurité ou sur d'autres critères tels que la criticité des actifs, la fonction opérationnelle, l'emplacement physique ou logique, l'accès exigé (par exemple, les principes de droit d'accès minimal) ou l'organisation responsable.

4.4.2.2 Justification et recommandations supplémentaires

Le regroupement d'actifs en zones et conduits consiste à identifier les actifs qui partagent des exigences de sécurité communes, et à admettre l'identification des mesures de sécurité communes exigées pour atténuer les risques. L'affectation des actifs de l'IACS aux zones et conduits peut être ajustée selon les résultats de l'appréciation détaillée du risque. Il s'agit d'une exigence générale, mais il convient d'accorder une attention particulière aux systèmes liés à la sécurité, notamment aux systèmes instrumentés de sécurité, aux systèmes sans fil, aux systèmes directement connectés aux terminaux Internet et aux systèmes qui interagissent avec l'IACS, mais sont gérés par d'autres appareils mobiles (y compris des systèmes externes).

Par exemple, une installation peut d'abord être divisée en zones opérationnelles, telles que des zones de stockage du matériel, de traitement, de finition, etc. Les zones opérationnelles peuvent souvent être subdivisées en couches fonctionnelles, telles que des systèmes industriels d'exécution (MES), des systèmes de supervision (par exemple, les interfaces homme-machine [IHM]), des systèmes de commande principaux (par exemple, BCPS, DCS, des terminaux à distance [RTU] et des automates programmables [PLC]), ainsi que des systèmes de sécurité. Des modèles tels que le modèle de référence Purdue, comme cela est défini dans l'IEC 62264-1 [9] sont souvent utilisés comme base pour cette division. Les architectures de référence du fournisseur du produit IACS peuvent également être utiles.

4.4.3 ZCR 3.2: Séparation des actifs des systèmes métiers et des IACS

4.4.3.1 Exigence

Les actifs de l'IACS doivent être regroupés en zones qui sont logiquement ou physiquement séparées des actifs des systèmes métier ou de l'entreprise.

4.4.3.2 Justification et recommandations supplémentaires

Les systèmes métier et les IACS sont deux types de systèmes différents qu'il est nécessaire de diviser en zones distinctes, car leurs fonctionnalités, leur organisation responsable, les résultats de l'appréciation initiale du risque et leur emplacement sont souvent fondamentalement différents. Il est important de comprendre la différence fondamentale entre les systèmes métier et les IACS, et l'impact possible des IACS sur la santé, la sécurité et l'environnement (HSE).

IECNORM.COM : Click to view the full PDF of IEC 62443-3-2:2020

4.4.4 ZCR 3.3: Séparation des actifs liés à la sécurité

4.4.4.1 Exigence

Les actifs de l'IACS liés à la sécurité doivent être regroupés en zones qui sont logiquement ou physiquement séparées des zones comprenant des actifs de l'IACS non liés à la sécurité. Cependant, s'ils ne peuvent pas être séparés, toute la zone doit être identifiée comme zone liée à la sécurité.

4.4.4.2 Justification et recommandations supplémentaires

Les actifs de l'IACS liés à la sécurité ont généralement des exigences de sécurité différentes de celles des composants de systèmes ou des systèmes de commande de base et des composants interfacés aux composants de système de commande. Les zones liées à la sécurité exigent généralement une protection de sécurité plus élevée en raison des risques potentiels élevés pour la santé, la sécurité et l'environnement si la zone est compromise.

4.4.5 ZCR 3.4: Séparation temporaire des appareils connectés

4.4.5.1 Recommandation

Il convient de regrouper les appareils autorisés à établir des connexions temporaires avec le SUC dans une ou des zones distinctes des actifs destinés à être connectés en permanence à l'IACS.

4.4.5.2 Justification et recommandations supplémentaires

Les appareils qui sont temporairement connectés au SUC (par exemple, les ordinateurs portables de maintenance, les équipements de traitement portables, les appareils de sécurité portables et les appareils USB) sont plus susceptibles d'être exposés à des menaces, différentes et plus diverses que les appareils qui font partie intégrante de la zone. Par conséquent, il convient de modéliser ces appareils dans une ou des zones distinctes. La principale préoccupation concernant ces appareils est que, en raison de la nature temporaire de la connexion, ils peuvent également se connecter à d'autres réseaux, en dehors de la zone. Cependant, il existe des exceptions. Par exemple, un appareil portatif qui n'est utilisé que dans une seule zone et ne quitte jamais la frontière physique de la zone peut être inclus dans la zone.

4.4.6 ZCR 3.5: Séparation des appareils sans fil

4.4.6.1 Recommandation

Il convient de placer les appareils sans fil dans une ou plusieurs zones, séparées des appareils câblés.

4.4.6.2 Justification et recommandations supplémentaires

Les signaux sans fil ne sont pas contrôlés par des clôtures ou des armoires et sont donc plus accessibles que les réseaux câblés normaux. Du fait de cette possibilité de plus grande facilité d'accès, ils sont plus susceptibles d'être exposés à des menaces, différentes et plus diverses que les appareils câblés.

Généralement, un point d'accès sans fil est modélisé comme conduit entre une zone sans fil et une zone câblée. Selon les fonctionnalités du point d'accès sans fil, des contrôles de sécurité supplémentaires (par exemple, pare-feu) peuvent être exigés pour assurer un niveau de séparation approprié.

IECNORM.COM : Click to view the full PDF of IEC 62443-3-2:2020

4.4.7 ZCR 3.6: Séparation des appareils connectés au moyen des réseaux externes

4.4.7.1 Recommandation

Il convient de regrouper dans une ou des zones distinctes les appareils autorisés à établir des connexions avec le SUC au moyen des réseaux externes au SUC.

4.4.7.2 Justification et recommandations supplémentaires

Il n'est pas rare que des organisations accordent un accès à distance aux différents acteurs impliqués dans leurs activités, par exemple à leurs employés, aux fournisseurs et autres partenaires commerciaux, à des fins de maintenance, d'optimisation et d'établissement de rapports. L'accès à distance se situant à l'extérieur de la frontière physique du SUC, il convient de le modéliser en tant que zone ou zones distinctes, avec ses propres exigences de sécurité.

4.5 ZCR 4: Comparaison des risques

4.5.1 Vue d'ensemble

Le paragraphe 4.5.2 inclut une ZCR pour comparer le risque initial au risque tolérable.

4.5.2 ZCR 4.1: Comparaison du risque initial avec le risque tolérable

4.5.2.1 Exigence

Le risque initial déterminé au 4.3 doit être comparé au risque tolérable pour l'organisation. Si le risque initial dépasse le risque tolérable, l'organisation doit effectuer une appréciation détaillée du risque de cybersécurité définie au 4.6.

4.5.2.2 Justification et recommandations supplémentaires

L'objectif de cette étape est de déterminer si le risque initial est tolérable ou exige une atténuation supplémentaire.

4.6 ZCR 5: Réalisation d'une appréciation détaillée du risque de cybersécurité

4.6.1 Vue d'ensemble

La présente ZCR traite des exigences d'appréciation détaillée du risque pour un IACS, et fournit des justifications et des recommandations supplémentaires relatives à chaque exigence. Les exigences décrites dans la présente ZCR s'appliquent à chaque zone et conduit. Si des zones ou des conduits partagent une ou des menaces similaires, des conséquences et/ou des actifs similaires, il est admissible d'analyser ensemble des groupes de zones ou de conduits, si ce regroupement permet d'optimiser l'analyse. Il est admissible d'utiliser les résultats existants si la zone est normalisée (par exemple, en cas de réplication d'instances multiples d'une conception de référence). L'organigramme donné à la Figure 2 représente le déroulement des opérations d'appréciation du risque de cybersécurité.

Toute méthodologie d'appréciation détaillée du risque (par exemple, ISO 31000 [14], NIST SP 800-39 [16] et ISO/IEC 27005 [12]) peut être suivie, à condition que la méthodologie choisie satisfasse aux exigences d'appréciation du risque. Il convient d'utiliser les méthodologies d'appréciation initiale et détaillée du risque provenant du même cadre, de la même norme ou de la même source, et ces méthodologies doivent utiliser une échelle de classement des risques cohérente, afin de produire des résultats cohérents.

IECNORM.COM : Click to view the full PDF of IEC 62443-3-2:2020

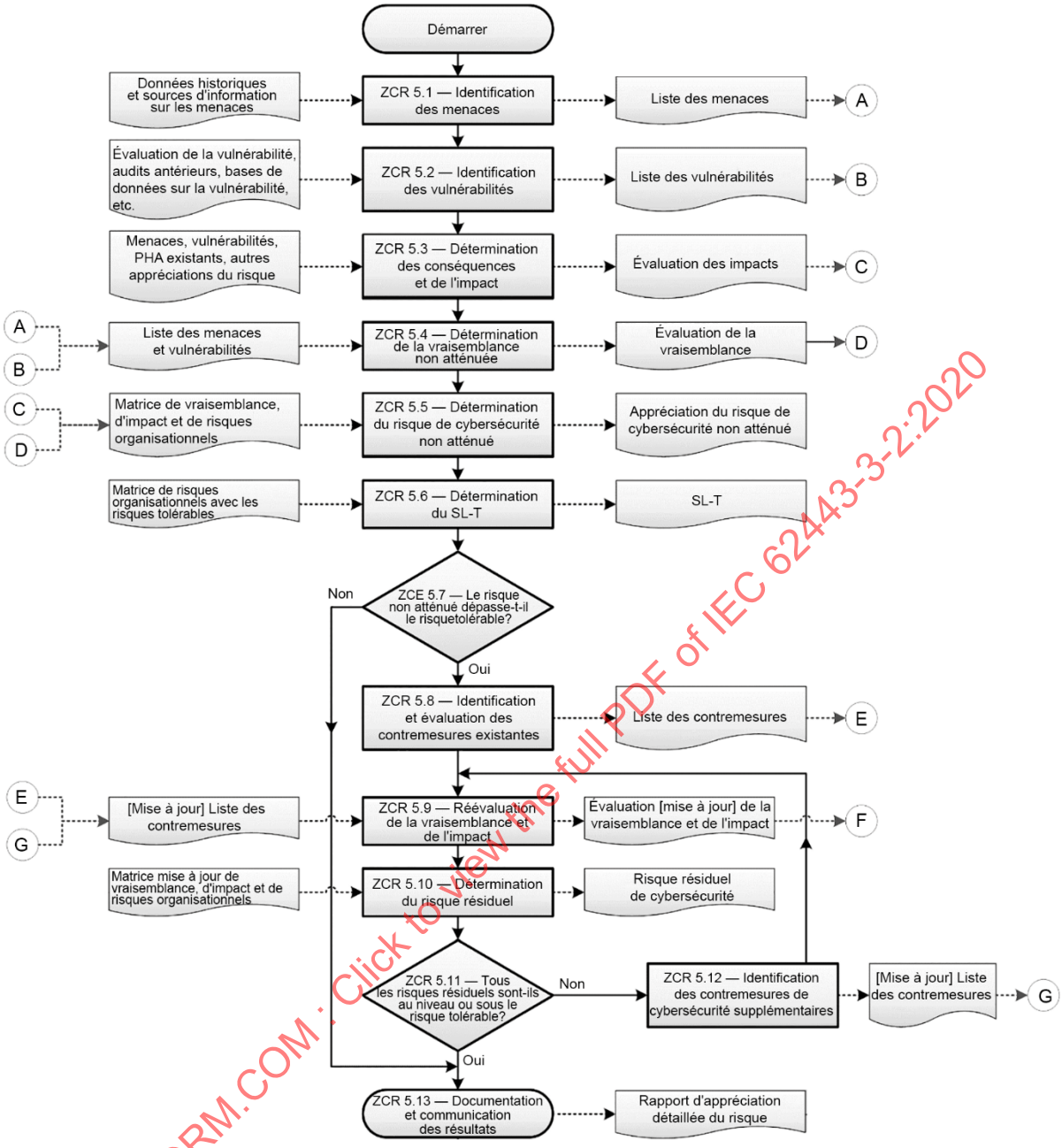


Figure 2 – Flux de travail d'appréciation détaillée du risque de cybersécurité par zone ou conduit

IECNORM.COM : Click to view the full PDF of IEC 62443-3-2:2020

4.6.2 ZCR 5.1: Identification des menaces

4.6.2.1 Exigence

Une liste des menaces susceptibles d'affecter les actifs contenus dans la zone ou le conduit doit être établie.

4.6.2.2 Justification et recommandations supplémentaires

Il est important d'établir une liste complète et réaliste des menaces, afin d'effectuer une appréciation du risque de sécurité. Dans la description d'une menace, il convient d'inclure, entre autres:

a) une description de la source de la menace;

b) une description de la capacité ou du niveau de qualification de la source de la menace;

c) une description des vecteurs de menace possibles;

d) une identification du ou des actifs potentiellement affectés.

Quelques exemples de descriptions de menaces:

- un employé non malveillant accède physiquement à la zone de contrôle du processus et branche une clé USB dans l'un des ordinateurs;
- un employé de support habilité accède logiquement à la zone de contrôle du processus à l'aide d'un ordinateur portable infecté;
- un employé non malveillant ouvre un courriel d'hameçonnage qui compromet ses informations d'accès.

Étant donné le nombre potentiel élevé de menaces possibles, il est acceptable de résumer en regroupant les sources, les actifs, les points d'entrée, etc., en classes.

4.6.3 ZCR 5.2: Identification des vulnérabilités

4.6.3.1 Exigence

La zone ou le conduit doit être analysé afin d'identifier et de documenter les vulnérabilités connues associées aux actifs contenus dans la zone ou le conduit, y compris celles des points d'accès.

4.6.3.2 Justification et recommandations supplémentaires

Pour qu'une menace aboutisse, il est nécessaire d'exploiter une ou plusieurs vulnérabilités dans un actif. Par conséquent, il est nécessaire d'identifier les vulnérabilités connues associées aux actifs pour mieux comprendre les vecteurs de menace.

Une approche généralement acceptée pour identifier les vulnérabilités dans un IACS consiste à effectuer une évaluation de la vulnérabilité. De plus amples informations sur les évaluations de la vulnérabilité de cybersécurité de l'IACS sont disponibles dans l'ISA TR84.00.09 [15].

En outre, il existe de nombreuses sources d'informations sur les vulnérabilités connues et courantes dans les IACS, telles que les équipes de réaction en informatique pour les systèmes de commande industriels (ICS-CERT), les fournisseurs de produits IACS, etc.

4.6.4 ZCR 5.3: Détermination des conséquences et de l'impact

4.6.4.1 Exigence

Chaque scénario de menace doit être évalué pour déterminer les conséquences et l'impact dans le cas d'une menace. Il convient de documenter les conséquences en matière d'impact le plus défavorable sur les zones de risque, notamment sur la sécurité du personnel, les pertes financières, l'interruption des activités et l'environnement.

4.6.4.2 Justification et recommandations supplémentaires

L'estimation de l'impact le plus défavorable d'une menace cybernétique constitue une contribution importante à l'analyse coût/bénéfice des contrôles de sécurité. Si l'impact le plus défavorable est faible, l'équipe d'appréciation du risque peut décider de passer à la menace suivante.

Il convient d'examiner les évaluations PHA et autres appréciations du risque associées (comme les risques liés aux technologies de l'information, à la sécurité fonctionnelle, à la sécurité des entreprises et à la sécurité physique), afin de déterminer les conséquences et l'impact de la menace.

IECNORM.COM : Click to view the full PDF of IEC 62443-3-2:2020

La mesure de l'impact peut être qualitative ou quantitative. Une méthode consiste à utiliser une échelle de conséquences définie par l'organisation dans le cadre de son système de management du risque (voir les exemples donnés dans l'Annexe B).

4.6.5 ZCR 5.4: Détermination de la vraisemblance non atténuée

4.6.5.1 Exigence

Chaque menace doit être évaluée pour déterminer la vraisemblance non atténuée. Il s'agit de la vraisemblance que la menace se réalise.

4.6.5.2 Justification et recommandations supplémentaires

Dans la terminologie du management du risque, le mot "vraisemblance" est utilisé pour indiquer la possibilité que quelque chose se produise, que cette possibilité soit définie, mesurée ou déterminée de façon objective ou subjective, qualitative ou quantitative, et qu'elle soit décrite au moyen de termes généraux ou mathématiques (comme une probabilité ou une fréquence sur une période donnée). Une méthode courante d'estimation de la vraisemblance consiste à utiliser une échelle de vraisemblance semi-quantitative définie par l'organisation dans le cadre de son système de management du risque (voir les exemples donnés dans l'Annexe B). Le présent document admet des méthodes qualitatives ou quantitatives.

Lors de l'estimation de la vraisemblance non atténuée, un certain nombre de facteurs sont pris en considération tels que la motivation et les capacités à l'origine des menaces, l'historique de menaces similaires, les vulnérabilités connues, l'attrait de la cible, etc.

Il convient de ne pas prendre en considération les contremesures de cybersécurité existantes pour la zone ou le conduit évalué lors de la détermination de la vraisemblance non atténuée; il convient de les éliminer de manière hypothétique. Cependant, la détermination de la vraisemblance reconnaît les contremesures inhérentes aux composants IACS et toutes les couches de protection indépendantes (IPL), hors cybersécurité, telles que la sécurité physique, les dispositifs de protection mécaniques (par exemple, les soupapes de sécurité) ou les procédures d'urgence mises en place pour réduire la vraisemblance.

La vraisemblance est évaluée deux fois au cours du processus d'appréciation détaillée du risque. Elle est initialement déterminée sans prendre en considération les contremesures existantes, afin d'établir le risque non atténué. Elle est réévaluée au 4.6.10, en tenant compte des contremesures existantes et de leur efficacité, afin de déterminer le risque résiduel.

Des méthodes d'appréciation du risque axées uniquement sur les conséquences peuvent être utilisées pour satisfaire aux exigences du présent document. Ces méthodes ne tiennent généralement pas compte de la vraisemblance dans la détermination du risque de cybersécurité non atténué et posent implicitement le principe que la vraisemblance est constante (par exemple, selon l'hypothèse que la vraisemblance est déjà présente ou, quantitativement, correspond à un "1").

4.6.6 ZCR 5.5: Détermination du risque de cybersécurité non atténué

4.6.6.1 Exigence

Le risque de cybersécurité non atténué pour chaque menace doit être déterminé en combinant la mesure de l'impact déterminé au 4.6.4 et la mesure de vraisemblance non atténuée déterminée au 4.6.5.

4.6.6.2 Justification et recommandations supplémentaires

Le risque de cybersécurité non atténué est souvent déterminé à l'aide d'une matrice de risques qui établit la relation entre la vraisemblance, l'impact et le risque, comme une matrice de risques organisationnels (voir les exemples donnés dans l'Annexe B).

IECNORM.COM : Click to view the full PDF of IEC 62443-3-2:2020

4.6.7 ZCR 5.6: Détermination du SL-T

4.6.7.1 Exigence

Un SL-T doit être établi pour chaque zone de sécurité ou conduit.

4.6.7.2 Justification et recommandations supplémentaires

Le SL-T est le niveau de sécurité souhaité pour un IACS, une zone ou un conduit particulier. Il est établi pour communiquer clairement cette information aux responsables de la conception, de la mise en œuvre, du fonctionnement et de la maintenance de la cybersécurité.

Le SL-T peut être exprimé sous forme d'une valeur unique ou d'un vecteur. Consulter l'Annexe A de l'IEC 62443-3-3:2013 pour de plus amples informations sur l'approche du vecteur SL.

Aucune méthode n'est exigée pour l'établissement du SL-T. Certaines organisations choisissent d'établir le SL-T selon la différence entre le risque de cybersécurité non atténué et le risque tolérable. D'autres choisissent d'établir le SL-T sur la base des définitions de SL fournies dans l'Annexe A du présent document et dans l'IEC 62443-3-3:2013. Une autre approche, si une matrice de risques est utilisée (voir les exemples à l'Annexe B), consiste à établir qualitativement le SL. En partant d'une estimation raisonnable du SL (qui peut également être nulle), le risque de cybersécurité est évalué par la matrice de risques en tenant compte des contremesures impliquées par le SL. Si le risque n'est pas acceptable, le SL est augmenté (ce qui signifie que des contremesures supplémentaires sont ajoutées) jusqu'à ce que le risque de cybersécurité soit acceptable. Le SL dérivé de cette analyse devient un SL-T.

4.6.8 ZCR 5.7: Comparaison du risque non atténué avec le risque tolérable

4.6.8.1 Exigence

Le risque non atténué déterminé pour chaque menace identifiée au 4.6.6 doit être comparé au risque tolérable pour l'organisation. Si le risque non atténué dépasse le risque tolérable, l'organisation doit déterminer si elle souhaite accepter, transférer ou atténuer le risque. Pour atténuer le risque, il s'agit de poursuivre l'évaluation de la menace en réalisant les dispositions de 4.6.9 à 4.6.13. Sinon, l'organisation peut documenter les résultats obtenus avec 4.6.14 et passer à la menace suivante.

4.6.8.2 Justification et recommandations supplémentaires

L'objectif de cette étape est de déterminer si le risque non atténué est tolérable ou exige une évaluation supplémentaire.

4.6.9 ZCR 5.8: Identification et évaluation des contremesures existantes

4.6.9.1 Exigence

Les contremesures existantes dans le SUC doivent être identifiées et évaluées afin de déterminer leur efficacité pour réduire la vraisemblance ou l'impact de la menace.

4.6.9.2 Justification et recommandations supplémentaires

Afin de déterminer le risque résiduel, il convient d'évaluer la vraisemblance et l'impact en tenant compte de la présence et de l'efficacité des contremesures existantes. Cette étape du processus se concentre sur l'identification et l'évaluation des contremesures existantes.

L'IEC 62443-3-3 fournit des recommandations relatives aux types de contremesures et leur efficacité, en attribuant un SL de capacité (SL-C) à chaque exigence du système.

IECNORM.COM : Click to view the full PDF of IEC 62443-3-2:2020

4.6.10 ZCR 5.9: Réévaluation de la vraisemblance et de l'impact

4.6.10.1 Exigence

La vraisemblance et l'impact doivent être réévalués en tenant compte des contremesures et de leur efficacité.

4.6.10.2 Justification et recommandations supplémentaires

La vraisemblance non atténuée déterminée au 4.6.5 ne prend pas en compte les contremesures existantes. Dans cette étape, les contremesures, comme les contrôles techniques, administratifs ou de procédure, sont prises en considération et utilisées pour déterminer la vraisemblance atténuée. De même, il convient également de réévaluer les conséquences et l'impact déterminés au 4.6.4 en tenant compte des contremesures identifiées.

4.6.11 ZCR 5.10: Détermination du risque résiduel

4.6.11.1 Exigence

Le risque résiduel pour chaque menace identifiée au 4.6.2 doit être déterminé en combinant la mesure de vraisemblance atténuée et les valeurs d'impact atténué, déterminées au 4.6.10.

4.6.11.2 Justification et recommandations supplémentaires

La détermination du risque résiduel fournit une mesure du niveau de risque actuel ainsi qu'une mesure de l'efficacité des contremesures existantes. Il s'agit d'une étape essentielle pour déterminer si le niveau de risque actuel dépasse les lignes directrices en matière de risques tolérables.

4.6.12 ZCR 5.11: Comparaison du risque résiduel avec le risque tolérable

4.6.12.1 Exigence

Le risque résiduel déterminé pour chaque menace identifiée au 4.6.2, ZCR 5.1: Identification des menaces doit être comparé au risque tolérable pour l'organisation. Si le risque résiduel dépasse le risque tolérable, l'organisation doit déterminer si ce risque résiduel sera accepté, transféré ou atténué, selon la politique de l'organisation.

4.6.12.2 Justification et recommandations supplémentaires

L'objectif de cette étape est de déterminer si le risque résiduel est tolérable ou exige une atténuation supplémentaire. De nombreuses organisations définissent le risque tolérable dans leurs politiques de management du risque.

4.6.13 ZCR 5.12: Identification des contremesures de cybersécurité supplémentaires

4.6.13.1 Exigence

Des contremesures de cybersécurité supplémentaires, comme des contrôles techniques, administratifs ou de procédure, doivent être identifiées pour atténuer les risques, lorsque le risque résiduel dépasse le risque tolérable pour l'organisation, à moins que l'organisation ne choisisse de tolérer ou de transférer le risque.

4.6.13.2 Justification et recommandations supplémentaires

Lorsque le risque résiduel dépasse la tolérance au risque d'une organisation, il est nécessaire de prendre des mesures pour réduire le risque à des niveaux tolérables.

IECNORM.COM : Click to view the full PDF of IEC 62443-3-2:2020