IEC 62443-3-2

Edition 1.0 2020-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

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)

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 It also gives information on projects, replaced and withdrawn publications.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

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.

CONTENTS

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.

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.

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.

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.

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).

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)

[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

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.

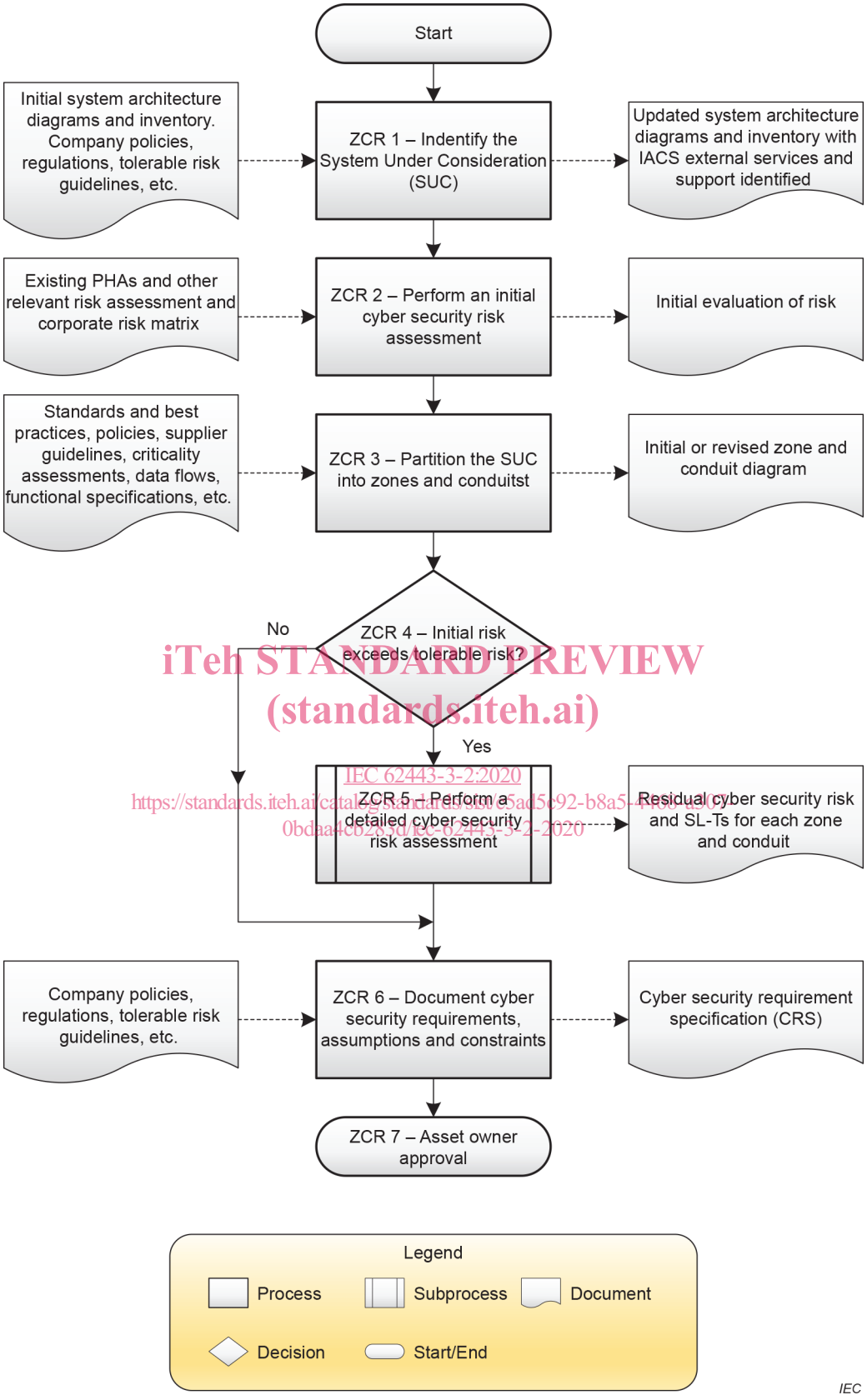

Figure 1 – Workflow diagram outlining the primary steps required to establish zones and conduits, as well as to assess risk

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.