



**NSAI**  
Standards

Irish Standard  
I.S. EN IEC 62443-3-2:2020

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

**I.S. EN IEC 62443-3-2:2020**

*Incorporating amendments/corrigenda/National Annexes issued since publication:*

The National Standards Authority of Ireland (NSAI) produces the following categories of formal documents:

I.S. xxx: Irish Standard — national specification based on the consensus of an expert panel and subject to public consultation.

S.R. xxx: Standard Recommendation — recommendation based on the consensus of an expert panel and subject to public consultation.

SWiFT xxx: A rapidly developed recommendatory document based on the consensus of the participants of an NSAI workshop.

*This document replaces/revises/consolidates the NSAI adoption of the document(s) indicated on the CEN/CENELEC cover/Foreword and the following National document(s):*

*NOTE: The date of any NSAI previous adoption may not match the date of its original CEN/CENELEC document.*

*This document is based on:*

EN IEC 62443-3-2:2020

*Published:*

2020-08-28

*This document was published  
under the authority of the NSAI  
and comes into effect on:*

2020-09-14

ICS number:

NOTE: If blank see CEN/CENELEC cover page

NSAI  
1 Swift Square,  
Northwood, Santry  
Dublin 9

T +353 1 807 3800  
F +353 1 807 3838  
E standards@nsai.ie  
W NSAI.ie

Sales:  
T +353 1 857 6730  
F +353 1 857 6729  
W standards.ie

Údarás um Chaighdeáin Náisiúnta na hÉireann

## National Foreword

I.S. EN IEC 62443-3-2:2020 is the adopted Irish version of the European Document EN IEC 62443-3-2:2020, Security for industrial automation and control systems - Part 3-2: Security risk assessment for system design

This document does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

For relationships with other publications refer to the NSAI web store.

**Compliance with this document does not of itself confer immunity from legal obligations.**

*In line with international standards practice the decimal point is shown as a comma (,) throughout this document.*

This page is intentionally left blank

EUROPEAN STANDARD  
NORME EUROPÉENNE  
EUROPÄISCHE NORM

**EN IEC 62443-3-2**

August 2020

ICS 25.040.40; 35.030

English Version

**Security for industrial automation and control systems - Part 3-2:  
Security risk assessment for system design  
(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  
(IEC 62443-3-2:2020)

IT-Sicherheit für industrielle Automatisierungssysteme - Teil  
3-2: Sicherheitsrisikobeurteilung und Systemgestaltung  
(IEC 62443-3-2:2020)

This European Standard was approved by CENELEC on 2020-07-29. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.



European Committee for Electrotechnical Standardization  
Comité Européen de Normalisation Electrotechnique  
Europäisches Komitee für Elektrotechnische Normung

**CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels**

**EN IEC 62443-3-2:2020 (E)****European foreword**

The text of document 65/799/FDIS, future edition 1 of IEC 62443-3-2, prepared by IEC/TC 65 "Industrial-process measurement, control and automation" was submitted to the IEC-CENELEC parallel vote and approved by CENELEC as EN IEC 62443-3-2:2020.

The following dates are fixed:

- latest date by which the document has to be implemented at national level by publication of an identical national standard or by endorsement (dop) 2021-04-29
- latest date by which the national standards conflicting with the document have to be withdrawn (dow) 2023-07-29

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC shall not be held responsible for identifying any or all such patent rights.

**Endorsement notice**

The text of the International Standard IEC 62443-3-2:2020 was approved by CENELEC as a European Standard without any modification.

In the official version, for Bibliography, the following notes have to be added for the standards indicated:

IEC 62443-2-1	NOTE	Harmonized as EN IEC 62443-2-1 <sup>1</sup>
IEC 62443-2-4:2015	NOTE	Harmonized as EN IEC 62443-2-4:2019 (not modified)
IEC 62443-4-1:2018	NOTE	Harmonized as EN IEC 62443-4-1:2018 (not modified)
IEC 62443-4-2:2019	NOTE	Harmonized as EN IEC 62443-4-2:2019 (not modified)
IEC 61511-2:2016	NOTE	Harmonized as EN 61511-2:2017 (not modified)
IEC 62264-1:2013	NOTE	Harmonized as EN 62264-1:2013 (not modified)

---

<sup>1</sup> To be published. Stage at the time of publication: prEN IEC 62443-2-1:2019.

## **Annex ZA**

(normative)

### **Normative references to international publications with their corresponding European publications**

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.

NOTE 1 Where an International Publication has been modified by common modifications, indicated by (mod), the relevant EN/HD applies.

NOTE 2 Up-to-date information on the latest versions of the European Standards listed in this annex is available here: [www.cenelec.eu](http://www.cenelec.eu).

<u>Publication</u>	<u>Year</u>	<u>Title</u>	<u>EN/HD</u>	<u>Year</u>
IEC 62443-3-3	2013	Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels	EN IEC 62443-3-3	2019

This page is intentionally left blank





**IEC 62443-3-2**

Edition 1.0 2020-06

# **INTERNATIONAL STANDARD**



---

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



**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.

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

Tel.: +41 22 919 02 11  
[info@iec.ch](mailto:info@iec.ch)  
[www.iec.ch](http://www.iec.ch)

**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](http://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](http://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](http://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](mailto:sales@iec.ch).

**Electropedia - [www.electropedia.org](http://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](http://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.



**IEC 62443-3-2**

Edition 1.0 2020-06

# INTERNATIONAL STANDARD



---

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

INTERNATIONAL  
ELECTROTECHNICAL  
COMMISSION

ICS 25.040.40; 35.030

ISBN 978-2-8322-8501-5

**Warning! Make sure that you obtained this publication from an authorized distributor.**

## CONTENTS

FOREWORD.....	4
INTRODUCTION.....	6
1 Scope.....	7
2 Normative references .....	7
3 Terms, definitions, abbreviated terms, acronyms and conventions.....	7
3.1 Terms and definitions.....	7
3.2 Abbreviated terms and acronyms .....	10
3.3 Conventions.....	11
4 Zone, conduit and risk assessment requirements.....	11
4.1 Overview.....	11
4.2 ZCR 1: Identify the SUC.....	13
4.2.1 ZCR 1.1: Identify the SUC perimeter and access points.....	13
4.3 ZCR 2: Initial cyber security risk assessment .....	13
4.3.1 ZCR 2.1: Perform initial cyber security risk assessment.....	13
4.4 ZCR 3: Partition the SUC into zones and conduits .....	14
4.4.1 Overview .....	14
4.4.2 ZCR 3.1: Establish zones and conduits.....	14
4.4.3 ZCR 3.2: Separate business and IACS assets .....	14
4.4.4 ZCR 3.3: Separate safety related assets.....	14
4.4.5 ZCR 3.4: Separate temporarily connected devices.....	15
4.4.6 ZCR 3.5: Separate wireless devices .....	15
4.4.7 ZCR 3.6: Separate devices connected via external networks .....	15
4.5 ZCR 4: Risk comparison .....	16
4.5.1 Overview .....	16
4.5.2 ZCR 4.1: Compare initial risk to tolerable risk .....	16
4.6 ZCR 5: Perform a detailed cyber security risk assessment.....	16
4.6.1 Overview .....	16
4.6.2 ZCR 5.1: Identify threats.....	17
4.6.3 ZCR 5.2: Identify vulnerabilities .....	18
4.6.4 ZCR 5.3: Determine consequence and impact .....	18
4.6.5 ZCR 5.4: Determine unmitigated likelihood .....	19
4.6.6 ZCR 5.5: Determine unmitigated cyber security risk.....	19
4.6.7 ZCR 5.6: Determine SL-T .....	19
4.6.8 ZCR 5.7: Compare unmitigated risk with tolerable risk .....	20
4.6.9 ZCR 5.8: Identify and evaluate existing countermeasures .....	20
4.6.10 ZCR 5.9: Reevaluate likelihood and impact.....	20
4.6.11 ZCR 5.10: Determine residual risk .....	21
4.6.12 ZCR 5.11: Compare residual risk with tolerable risk.....	21
4.6.13 ZCR 5.12: Identify additional cyber security countermeasures .....	21
4.6.14 ZCR 5.13: Document and communicate results.....	22
4.7 ZCR 6: Document cyber security requirements, assumptions and constraints .....	22
4.7.1 Overview .....	22
4.7.2 ZCR 6.1: Cyber security requirements specification .....	22
4.7.3 ZCR 6.2: SUC description.....	23
4.7.4 ZCR 6.3: Zone and conduit drawings .....	23
4.7.5 ZCR 6.4: Zone and conduit characteristics.....	23
4.7.6 ZCR 6.5: Operating environment assumptions .....	24

4.7.7	ZCR 6.6: Threat environment.....	25
4.7.8	ZCR 6.7: Organizational security policies .....	25
4.7.9	ZCR 6.8: Tolerable risk.....	25
4.7.10	ZCR 6.9: Regulatory requirements.....	26
4.8	ZCR 7: Asset owner approval.....	26
4.8.1	Overview .....	26
4.8.2	ZCR 7.1: Attain asset owner approval.....	26
Annex A (informative)	Security levels.....	27
Annex B (informative)	Risk matrices .....	28
Bibliography.....		31
Figure 1 – Workflow diagram outlining the primary steps required to establish zones and conduits, as well as to assess risk .....		12
Figure 2 – Detailed cyber security risk assessment workflow per zone or conduit .....		17
Table B.1 – Example of a 3 x 5 risk matrix .....		28
Table B.2 – Example of likelihood scale .....		28
Table B.3 – Example of consequence or severity scale .....		29
Table B.4 – Example of a simple 3 x 3 risk matrix .....		29
Table B.5 – Example of a 5 x 5 risk matrix .....		30
Table B.6 – Example of a 3 x 4 matrix.....		30

## 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.

This is a free preview. Purchase the entire publication at the link below:

[Product Page](#)

- 
- Looking for additional Standards? Visit Intertek Inform Infostore
  - Learn about LexConnect, All Jurisdictions, Standards referenced in Australian legislation
-