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.

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

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*

SOMMAIRE

AVANT-PROPOS 34
INTRODUCTION 36
1 Domaine d'application 37
2 Références normatives 37
3 Termes, définitions, abréviations, acronymes et conventions 37
3.1 Termes et définitions 37
3.2 Abréviations et acronymes 41
3.3 Conventions 42
4 Exigences en matière d'évaluation des zones, des conduits et des risques 42
4.1 Vue d'ensemble 42
4.2 ZCR 1: Identifier le SUC 44
4.2.1 ZCR 1.1: Identifier le périmètre SUC et les points d'accès 44
4.3 ZCR 2: Appréciation initiale du risque de cybersécurité 44
4.3.1 ZCR 2.1: Réalisation d'une appréciation initiale du risque de cybersécurité 44
4.4 ZCR 3: Division du SUC en zones et conduits 45
4.4.1 Vue d'ensemble 45
4.4.2 ZCR 3.1: Établissement de zones et conduits 45
4.4.3 ZCR 3.2: Séparation des actifs des systèmes métiers et des IACS 45
4.4.4 ZCR 3.3: Séparation des actifs liés à la sécurité 46
4.4.5 ZCR 3.4: Séparation temporaire des appareils connectés 46
4.4.6 ZCR 3.5: Séparation des appareils sans fil 46
4.4.7 ZCR 3.6: Séparation des appareils connectés au moyen des réseaux externes 47
4.5 ZCR 4: Comparaison des risques 47
4.5.1 Vue d'ensemble 47
4.5.2 ZCR 4.1: Comparaison du risque initial avec le risque tolérable 47
4.6 ZCR 5: Réalisation d'une appréciation détaillée du risque de cybersécurité 47
4.6.1 Vue d'ensemble 47
4.6.2 ZCR 5.1: Identification des menaces 48
4.6.3 ZCR 5.2: Identification des vulnérabilités 49
4.6.4 ZCR 5.3: Détermination des conséquences et de l'impact 49
4.6.5 ZCR 5.4: Détermination de la vraisemblance non atténuée 50
4.6.6 ZCR 5.5: Détermination du risque de cybersécurité non atténué 50
4.6.7 ZCR 5.6: Détermination du SL-T 51
4.6.8 ZCR 5.7: Comparaison du risque non atténué avec le risque tolérable 51
4.6.9 ZCR 5.8: Identification et évaluation des contremesures existantes 51
4.6.10 ZCR 5.9: Réévaluation de la vraisemblance et de l'impact 52
4.6.11 ZCR 5.10: Détermination du risque résiduel 52
4.6.12 ZCR 5.11: Comparaison du risque résiduel avec le risque tolérable 52
4.6.13 ZCR 5.12: Identification des contremesures de cybersécurité supplémentaires 52
4.6.14 ZCR 5.13: Documentation et communication des résultats 53
4.7 ZCR 6: Documentation des exigences, hypothèses et contraintes liées à la cybersécurité 53
4.7.1 Vue d'ensemble 53
4.7.2 ZCR 6.1: Spécification des exigences de cybersécurité 53

4.7.3 ZCR 6.2: Description du SUC 54
4.7.4 ZCR 6.3: Schémas des zones et des conduits 54
4.7.5 ZCR 6.4: Caractéristiques des zones et des conduits 55
4.7.6 ZCR 6.5: Hypothèses liées à l'environnement d'exploitation 56
4.7.7 ZCR 6.6: Environnement de la menace 57
4.7.8 ZCR 6.7: Politiques en matière de sécurité organisationnelle 57
4.7.9 ZCR 6.8: Risque tolérable 57
4.7.10 ZCR 6.9: Exigences réglementaires 57
4.8 ZCR 7: Approbation du propriétaire de l'actif 58
4.8.1 Vue d'ensemble 58
4.8.2 ZCR 7.1: Obtention de l'approbation du propriétaire de l'actif 58
Annexe A (informative) Niveaux de sécurité 59
Annexe B (informative) Matrices de risques 60
Bibliographie 63

Figure 1 – Diagramme de flux de travail décrivant les principales étapes exigées pour établir des zones et des conduits et évaluer les risques 43
Figure 2 – Flux de travail d'appréciation détaillée du risque de cybersécurité par zone ou conduit 48

Tableau B.1 – Exemple d'une matrice de risques 3 x 5 60
Tableau B.2 – Exemple d'échelle de vraisemblances 60
Tableau B.3 – Exemple d'échelle de conséquences ou de gravités 61
Tableau B.4 – Exemple d'une matrice de risques simple 3 x 3 61
Tableau B.5 – Exemple d'une matrice de risques 5 x 5 62
Tableau B.6 – Exemple d'une matrice de risques 3 x 4 62

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.

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.

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.

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*