IEC 62443-4-1

Edition 1.0 2018-01

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements

Sécurité des automatismes industriels et des systèmes de commande – Partie 4-1: Exigences relatives au cycle de développement de produit sécurisé

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

ICS 25.040.40; 35.030

ISBN 978-2-8322-8693-7

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 6
INTRODUCTION 8
1 Scope 11
2 Normative references 11
3 Terms, definitions, abbreviated terms, acronyms and conventions 11
3.1 Terms and definitions 11
3.2 Abbreviated terms and acronyms 16
3.3 Conventions 17
4 General principles 17
4.1 Concepts 17
4.2 Maturity model 19
5 Practice 1 – Security management 20
5.1 Purpose 20
5.2 SM-1: Development process 21
5.2.1 Requirement 21
5.3 Rationale and supplemental guidance 21
5.4 SM-2: Identification of responsibilities 21
5.4.1 Requirement 21
5.4.2 Rationale and supplemental guidance 21
5.5 SM-3: Identification of applicability 21
5.5.1 Requirement 21
5.5.2 Rationale and supplemental guidance 22
5.6 SM-4: Security expertise 22
5.6.1 Requirement 22
5.6.2 Rationale and supplemental guidance 22
5.7 SM-5: Process scoping 22
5.7.1 Requirement 22
5.7.2 Rationale and supplemental guidance 23
5.8 SM-6: File integrity 23
5.8.1 Requirement 23
5.8.2 Rationale and supplemental guidance 23
5.9 SM-7: Development environment security 23
5.9.1 Requirement 23
5.9.2 Rationale and supplemental guidance 23
5.10 SM-8: Controls for private keys 23
5.10.1 Requirement 23
5.10.2 Rationale and supplemental guidance 24
5.11 SM-9: Security requirements for externally provided components 24
5.11.1 Requirement 24
5.11.2 Rationale and supplemental guidance 24
5.12 SM-10: Custom developed components from third-party suppliers 24
5.12.1 Requirement 24
5.12.2 Rationale and supplemental guidance 25
5.13 SM-11: Assessing and addressing security-related issues 25
5.13.1 Requirement 25
5.13.2 Rationale and supplemental guidance 25

5.14 SM-12: Process verification 25
5.14.1 Requirement 25
5.14.2 Rationale and supplemental guidance 25
5.15 SM-13: Continuous improvement 25
5.15.1 Requirement 25
5.15.2 Rationale and supplemental guidance 26
6 Practice 2 – Specification of security requirements 26
6.1 Purpose 26
6.2 SR-1: Product security context 27
6.2.1 Requirement 27
6.2.2 Rationale and supplemental guidance 27
6.3 SR-2: Threat model 27
6.3.1 Requirement 27
6.3.2 Rationale and supplemental guidance 28
6.4 SR-3: Product security requirements 28
6.4.1 Requirement 28
6.4.2 Rationale and supplemental guidance 28
6.5 SR-4: Product security requirements content 29
6.5.1 Requirement 29
6.5.2 Rationale and supplemental guidance 29
6.6 SR-5: Security requirements review 29
6.6.1 Requirement 29
6.6.2 Rationale and supplemental guidance 29
7 Practice 3 – Secure by design 30
7.1 Purpose 30
7.2 SD-1: Secure design principles 30
7.2.1 Requirement 30
7.2.2 Rationale and supplemental guidance 30
7.3 SD-2: Defense in depth design 31
7.3.1 Requirement 31
7.3.2 Rationale and supplemental guidance 32
7.4 SD-3: Security design review 32
7.4.1 Requirement 32
7.4.2 Rationale and supplemental guidance 32
7.5 SD-4: Secure design best practices 32
7.5.1 Requirement 32
7.5.2 Rationale and supplemental guidance 33
8 Practice 4 – Secure implementation 33
8.1 Purpose 33
8.2 Applicability 33
8.3 SI-1: Security implementation review 33
8.3.1 Requirement 33
8.3.2 Rationale and supplemental guidance 34
8.4 SI-2: Secure coding standards 34
8.4.1 Requirement 34
8.4.2 Rationale and supplemental guidance 34
9 Practice 5 – Security verification and validation testing 34
9.1 Purpose 34

9.2 SVV-1: Security requirements testing 35
9.2.1 Requirement 35
9.2.2 Rationale and supplemental guidance 35
9.3 SVV-2: Threat mitigation testing 35
9.3.1 Requirement 35
9.3.2 Rationale and supplemental guidance 35
9.4 SVV-3: Vulnerability testing 36
9.4.1 Requirement 36
9.4.2 Rationale and supplemental guidance 36
9.5 SVV-4: Penetration testing 36
9.5.1 Requirement 36
9.5.2 Rationale and supplemental guidance 36
9.6 SVV-5: Independence of testers 37
9.6.1 Requirement 37
9.6.2 Rationale and supplemental guidance 37
10 Practice 6 – Management of security-related issues 38
10.1 Purpose 38
10.2 DM-1: Receiving notifications of security-related issues 38
10.2.1 Requirement 38
10.2.2 Rationale and supplemental guidance 38
10.3 DM-2: Reviewing security-related issues 38
10.3.1 Requirement 38
10.3.2 Rationale and supplemental guidance 39
10.4 DM-3: Assessing security-related issues 39
10.4.1 Requirement 39
10.4.2 Rationale and supplemental guidance 39
10.5 DM-4: Addressing security-related issues 40
10.5.1 Requirement 40
10.5.2 Rationale and supplemental guidance 40
10.6 DM-5: Disclosing security-related issues 41
10.6.1 Requirement 41
10.6.2 Rationale and supplemental guidance 41
10.7 DM-6: Periodic review of security defect management practice 42
10.7.1 Requirement 42
10.7.2 Rationale and supplemental guidance 42
11 Practice 7 – Security update management 42
11.1 Purpose 42
11.2 SUM-1: Security update qualification 42
11.2.1 Requirement 42
11.2.2 Rationale and supplemental guidance 42
11.3 SUM-2: Security update documentation 42
11.3.1 Requirement 42
11.3.2 Rationale and supplemental guidance 43
11.4 SUM-3: Dependent component or operating system security update documentation 43
11.4.1 Requirement 43
11.4.2 Rationale and supplemental guidance 43
11.5 SUM-4: Security update delivery 43
11.5.1 Requirement 43

11.5.2 Rationale and supplemental guidance....43
11.6 SUM-5: Timely delivery of security patches....44
11.6.1 Requirement....44
11.6.2 Rationale and supplemental guidance....44
12 Practice 8 – Security guidelines....44
12.1 Purpose....44
12.2 SG-1: Product defense in depth....44
12.2.1 Requirement....44
12.2.2 Rationale and supplemental guidance....45
12.3 SG-2: Defense in depth measures expected in the environment....45
12.3.1 Requirement....45
12.3.2 Rationale and supplemental guidance....45
12.4 SG-3: Security hardening guidelines....45
12.4.1 Requirement....45
12.4.2 Rationale and supplemental guidance....46
12.5 SG-4: Secure disposal guidelines....46
12.5.1 Requirement....46
12.5.2 Rationale and supplemental guidance....46
12.6 SG-5: Secure operation guidelines....46
12.6.1 Requirement....46
12.6.2 Rationale and supplemental guidance....47
12.7 SG-6: Account management guidelines....47
12.7.1 Requirement....47
12.7.2 Rationale and supplemental guidance....47
12.8 SG-7: Documentation review....47
12.8.1 Requirement....47
12.8.2 Rationale and supplemental guidance....47
Annex A (informative) Possible metrics....48
Annex B (informative) Table of requirements....50
Bibliography....52

Figure 1 – Parts of the IEC 62443 series....9
Figure 2 – Example scope of product life-cycle....10
Figure 3 – Defence in depth strategy is a key philosophy of the secure product life-cycle....18

Table 1 – Maturity levels....20
Table 2 – Example SDL continuous improvement activities....26
Table 3 – Required level of independence of testers from developers....37
Table B.1 – Summary of all requirements....50

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –

Part 4-1: Secure product development lifecycle requirements

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 62443-4-1 has been prepared by IEC technical committee 65: Industrial-process measurement, control and automation.

The text of this International Standard is based on the following documents:

FDIS	Report on voting
65/685/FDIS	65/688/RVD

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

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

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

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

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

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

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

This document is part of a series of standards that addresses the issue of security for industrial automation and control systems (IACS). This document describes product development life-cycle requirements related to cyber security for products intended for use in the industrial automation and control systems environment and provides guidance on how to meet the requirements described for each element.

This document has been developed in large part from the Secure Development Life-cycle Assessment (SDLA) Certification Requirements [26] [1] from the ISA Security Compliance Institute (ISCI). Note that the SDLA procedure was based on the following sources:

– ISO/IEC 15408-3 (Common Criteria) [18];

– Open Web Application Security Project (OWASP) Comprehensive, Lightweight Application Security Process (CLASP) [36];

– The Security Development Life-cycle by Michael Howard and Steve Lipner [43];

– IEC 61508 Functional safety of electrical/electronic/ programmable electronic safety-related systems [24], and

– RCTA DO-178B Software Considerations in Airborne Systems and Equipment Certification [28].

Therefore, all these sources can be considered contributing sources to this document.

This document is the part of the IEC 62443 series that contains security requirements for developers of any automation and control products where security is a concern.

Figure 1 illustrates the relationship of the different parts of IEC 62443 that were in existence or planned as of the date of circulation of this document. Those that are normatively referenced are included in the list of normative references in Clause 2, and those that are referenced for informational purposes or that are in development are listed in the Bibliography.

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

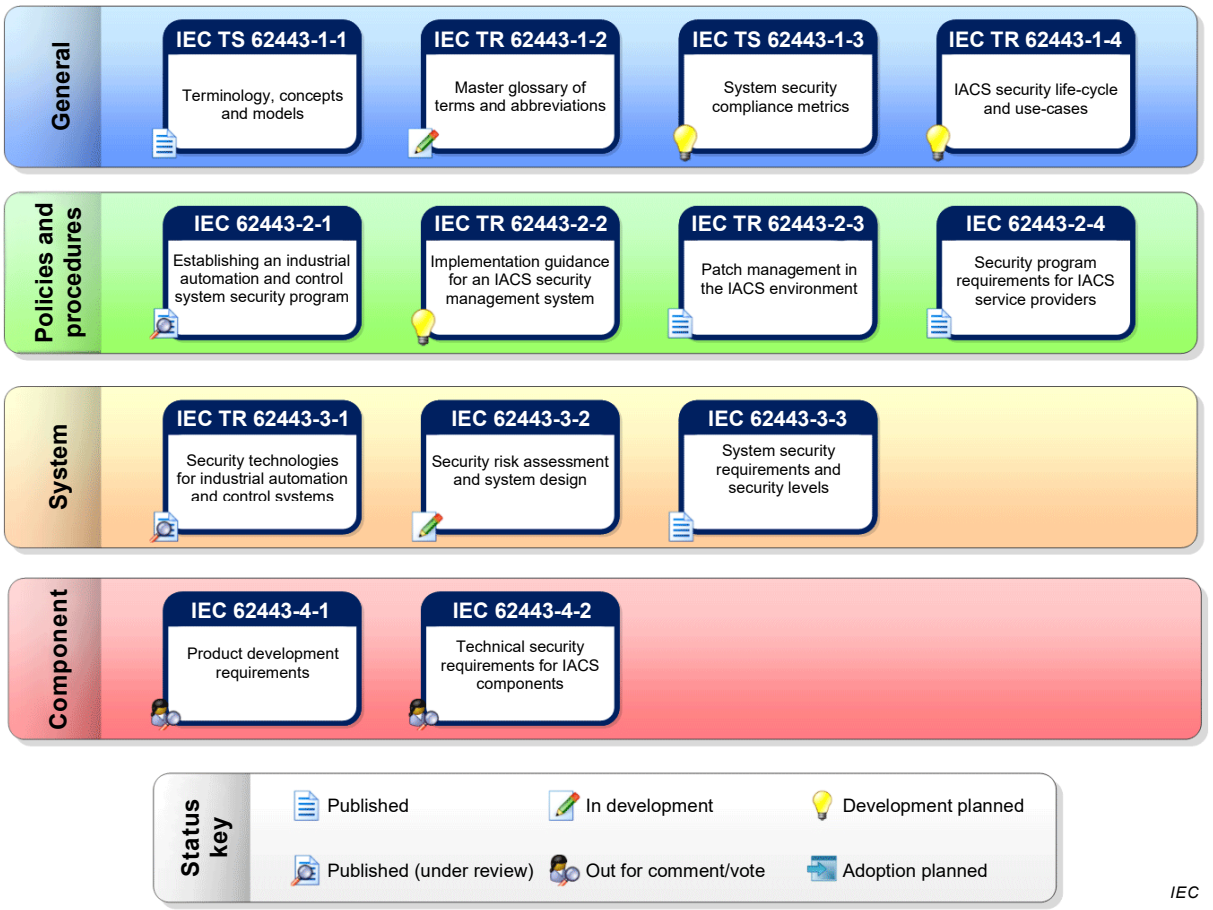


Figure 1 – Parts of the IEC 62443 series

Figure 2 illustrates how the developed product relates to maintenance and integration capabilities defined in IEC 62443-2-4 and to its operation by the asset owner. The product supplier develops products using a process compliant with this document. Those products may be a single component, such as an embedded controller, or a group of components working together as a system or subsystem. The products are then integrated together, usually by a system integrator, into an Automation Solution using a process compliant with IEC 62443-2-4. The Automation Solution is then installed at a particular site and becomes part of the industrial automation and control system (IACS). Some of these capabilities reference security measures defined in IEC 62443-3-3 [10] that the service provider ensures are supported in the Automation Solution (either as product features or compensating mechanisms). This document only addresses the process used for the development of the product; it does not address design, installation or operation of the Automation Solution or IACS.

In Figure 2, the Automation Solution is illustrated to contain one or more subsystems and optional supporting components such as advanced control. The dashed boxes indicate that these components are “optional”.

NOTE 1 Automation Solutions typically have a single product, but they are not restricted to do so. In some industries, there may be a hierarchical product structure. In general, the Automation Solution is the set of hardware and software, independent of product packaging, that is used to control a physical process (for example, continuous or manufacturing) as defined by the asset owner.

NOTE 2 If a service provider provides products used in the Automation Solution, then the service provider is fulfilling the role of product supplier in this diagram.

NOTE 3 If a service provider provides products used in the Automation Solution, then the service provider is fulfilling the role of product supplier in this diagram.

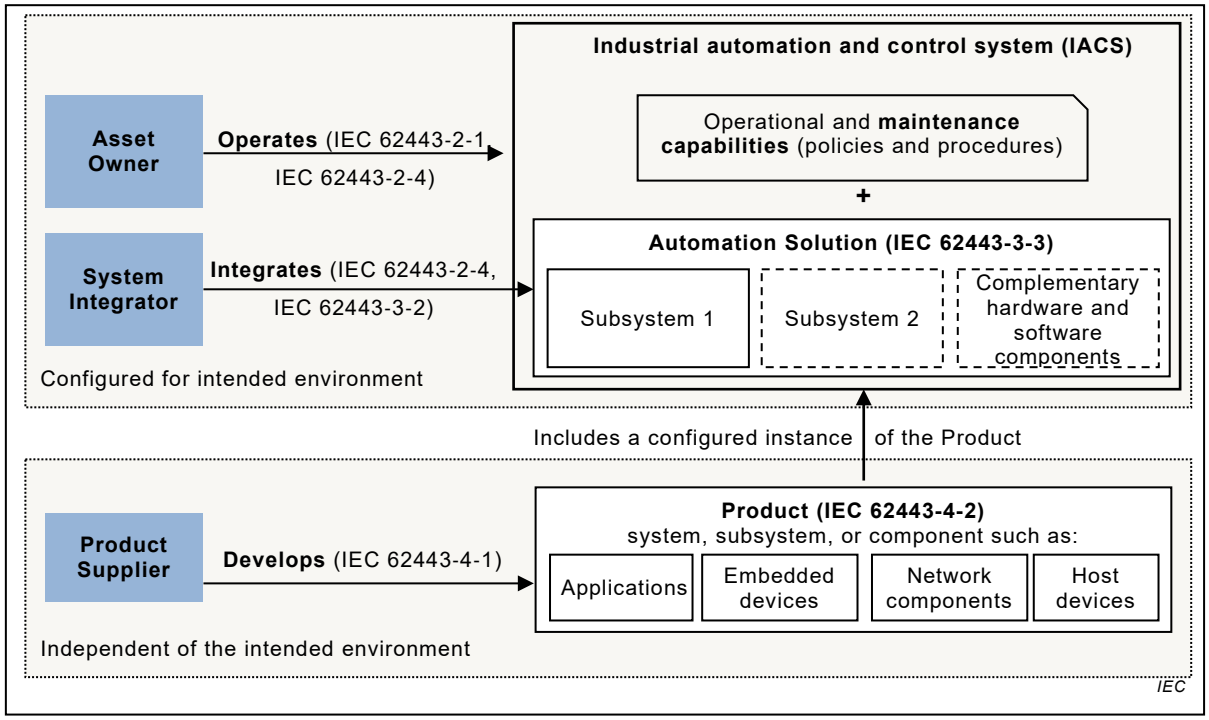


Figure 2 – Example scope of product life-cycle

SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –

Part 4-1: Secure product development lifecycle requirements

1 Scope

This part of IEC 62443 specifies process requirements for the secure development of products used in industrial automation and control systems. It defines a secure development life-cycle (SDL) for the purpose of developing and maintaining secure products. This life-cycle includes security requirements definition, secure design, secure implementation (including coding guidelines), verification and validation, defect management, patch management and product end-of-life. These requirements can be applied to new or existing processes for developing, maintaining and retiring hardware, software or firmware for new or existing products. These requirements apply to the developer and maintainer of the product, but not to the integrator or user of the product. A summary list of the requirements in this document can be found in Annex B.

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

SOMMAIRE

AVANT-PROPOS 60
INTRODUCTION 62
1 Domaine d'application 65
2 Références normatives 65
3 Termes, définitions, abréviations, acronymes et conventions 65
3.1 Termes et définitions 65
3.2 Abréviations et acronymes 71
3.3 Conventions 72
4 Principes généraux 72
4.1 Concepts 72
4.2 Modèle de maturité 73
5 Pratique 1 – Gestion de la sécurité 75
5.1 Objet 75
5.2 SM-1: Processus de développement 76
5.2.1 Exigence 76
5.3 Justification et recommandations supplémentaires 76
5.4 SM-2: Identification des responsabilités 76
5.4.1 Exigence 76
5.4.2 Justification et recommandations supplémentaires 76
5.5 SM-3: Identification de l'applicabilité 76
5.5.1 Exigence 76
5.5.2 Justification et recommandations supplémentaires 77
5.6 SM-4: Expertise en sécurité 77
5.6.1 Exigence 77
5.6.2 Justification et recommandations supplémentaires 77
5.7 SM-5: Définition du processus 78
5.7.1 Exigence 78
5.7.2 Justification et recommandations supplémentaires 78
5.8 SM-6: Intégrité de fichier 78
5.8.1 Exigence 78
5.8.2 Justification et recommandations supplémentaires 78
5.9 SM-7: Sécurité de l'environnement de développement 78
5.9.1 Exigence 78
5.9.2 Justification et recommandations supplémentaires 78
5.10 SM-8: Commandes pour les clés privées 79
5.10.1 Exigence 79
5.10.2 Justification et recommandations supplémentaires 79
5.11 SM-9: Exigences de sécurité pour les composants fournis par des prestataires externes 79
5.11.1 Exigence 79
5.11.2 Justification et recommandations supplémentaires 79
5.12 SM-10: Composants développés à la demande par des fournisseurs tiers 80
5.12.1 Exigence 80
5.12.2 Justification et recommandations supplémentaires 80
5.13 SM-11: Évaluation et traitement des questions liées à la sécurité 80
5.13.1 Exigence 80
5.13.2 Justification et recommandations supplémentaires 80

5.14 SM-12: Vérification du processus 81
5.14.1 Exigence 81
5.14.2 Justification et recommandations supplémentaires 81
5.15 SM-13: Amélioration continue 81
5.15.1 Exigence 81
5.15.2 Justification et recommandations supplémentaires 81
6 Pratique 2 – Spécification des exigences de sécurité 82
6.1 Objet 82
6.2 SR-1: Contexte de sécurité du produit 82
6.2.1 Exigence 82
6.2.2 Justification et recommandations supplémentaires 83
6.3 SR-2: Modèle des menaces 83
6.3.1 Exigence 83
6.3.2 Justification et recommandations supplémentaires 84
6.4 SR-3: Exigences de sécurité du produit 84
6.4.1 Exigence 84
6.4.2 Justification et recommandations supplémentaires 84
6.5 SR-4: Contenu des exigences de sécurité du produit 85
6.5.1 Exigence 85
6.5.2 Justification et recommandations supplémentaires 85
6.6 SR-5: Examen des exigences de sécurité 85
6.6.1 Exigence 85
6.6.2 Justification et recommandations supplémentaires 85
7 Pratique 3 – Sécurité par la conception 86
7.1 Objet 86
7.2 SD-1: Principes de conception sécurisée 86
7.2.1 Exigence 86
7.2.2 Justification et recommandations supplémentaires 86
7.3 SD-2: Conception de la défense en profondeur 88
7.3.1 Exigence 88
7.3.2 Justification et recommandations supplémentaires 88
7.4 SD-3: Examen de la conception de sécurité 88
7.4.1 Exigence 88
7.4.2 Justification et recommandations supplémentaires 88
7.5 SD-4: Meilleures pratiques de conception sécurisée 89
7.5.1 Exigence 89
7.5.2 Justification et recommandations supplémentaires 89
8 Pratique 4 – Mise en œuvre sécurisée 89
8.1 Objet 89
8.2 Applicabilité 89
8.3 SI-1: Examen de la mise en œuvre de sécurité 89
8.3.1 Exigence 89
8.3.2 Justification et recommandations supplémentaires 90
8.4 SI-2: Normes de codage sécurisé 90
8.4.1 Exigence 90
8.4.2 Justification et recommandations supplémentaires 90
9 Pratique 5 – Essai de vérification et de validation de la sécurité 91
9.1 Objet 91

9.2 SVV-1: Essais des exigences de sécurité 91
9.2.1 Exigence 91
9.2.2 Justification et recommandations supplémentaires 91
9.3 SVV-2: Essais d'atténuation des menaces 92
9.3.1 Exigence 92
9.3.2 Justification et recommandations supplémentaires 92
9.4 SVV-3: Essais de vulnérabilité 92
9.4.1 Exigence 92
9.4.2 Justification et recommandations supplémentaires 93
9.5 SVV-4: Essais de pénétration 93
9.5.1 Exigence 93
9.5.2 Justification et recommandations supplémentaires 93
9.6 SVV-5: Indépendance des personnes qui procèdent aux essais 93
9.6.1 Exigence 93
9.6.2 Justification et recommandations supplémentaires 94
10 Pratique 6 – Gestion des questions liées à la sécurité 94
10.1 Objet 94
10.2 DM-1: Réception des notifications de questions liées à la sécurité 95
10.2.1 Exigence 95
10.2.2 Justification et recommandations supplémentaires 95
10.3 DM-2: Examen des questions liées à la sécurité 95
10.3.1 Exigence 95
10.3.2 Justification et recommandations supplémentaires 96
10.4 DM-3: Évaluation des questions liées à la sécurité 96
10.4.1 Exigence 96
10.4.2 Justification et recommandations supplémentaires 96
10.5 DM-4: Traitement des questions liées à la sécurité 97
10.5.1 Exigence 97
10.5.2 Justification et recommandations supplémentaires 98
10.6 DM-5: Divulgation des questions liées à la sécurité 98
10.6.1 Exigence 98
10.6.2 Justification et recommandations supplémentaires 98
10.7 DM-6: Examen périodique de la pratique de gestion des défauts de sécurité 99
10.7.1 Exigence 99
10.7.2 Justification et recommandations supplémentaires 99
11 Pratique 7 – Gestion des mises à jour de sécurité 99
11.1 Objet 99
11.2 SUM-1: Qualification de mise à jour de sécurité 99
11.2.1 Exigence 99
11.2.2 Justification et recommandations supplémentaires 99
11.3 SUM-2: Documentation de mise à jour de sécurité 100
11.3.1 Exigence 100
11.3.2 Justification et recommandations supplémentaires 100
11.4 SUM-3: Documentation de mise à jour de sécurité des systèmes d'exploitation ou de composants dépendants 100
11.4.1 Exigence 100
11.4.2 Justification et recommandations supplémentaires 100
11.5 SUM-4: Livraison de mise à jour de sécurité 101
11.5.1 Exigence 101

11.5.2 Justification et recommandations supplémentaires 101
11.6 SUM-5: Livraison en temps opportun des correctifs de sécurité 101
11.6.1 Exigence 101
11.6.2 Justification et recommandations supplémentaires 101
12 Pratique 8 – Lignes directrices de sécurité 101
12.1 Objet 101
12.2 SG-1: Défense en profondeur du produit 102
12.2.1 Exigence 102
12.2.2 Justification et recommandations supplémentaires 102
12.3 SG-2: Mesures de défense en profondeur prévues dans l'environnement 102
12.3.1 Exigence 102
12.3.2 Justification et recommandations supplémentaires 102
12.4 SG-3: Lignes directrices relatives au renforcement de la sécurité 103
12.4.1 Exigence 103
12.4.2 Justification et recommandations supplémentaires 103
12.5 SG-4: Lignes directrices en matière d'élimination sécurisée 103
12.5.1 Exigence 103
12.5.2 Justification et recommandations supplémentaires 104
12.6 SG-5: Lignes directrices en matière de fonctionnement sécurisé 104
12.6.1 Exigence 104
12.6.2 Justification et recommandations supplémentaires 104
12.7 SG-6: Lignes directrices en matière de gestion de compte 104
12.7.1 Exigence 104
12.7.2 Justification et recommandations supplémentaires 105
12.8 SG-7: Examen de la documentation 105
12.8.1 Exigence 105
12.8.2 Justification et recommandations supplémentaires 105
Annexe A (informative) Mesures possibles 106
Annexe B (informative) Tableau des exigences 108
Bibliographie 110

Figure 1 – Parties de la série IEC 62443 63
Figure 2 – Exemple de domaine d'application du cycle de vie du produit 64
Figure 3 – La stratégie de défense en profondeur est une philosophie du cycle de vie du produit sécurisé 73

Tableau 1 – Niveaux de maturité 75
Tableau 2 – Exemple d'activités d'amélioration continue du SDL 82
Tableau 3 – Niveau exigé d'indépendance par rapport aux développeurs des personnes qui procèdent aux essais 94
Tableau B.1 – Récapitulatif de toutes les exigences 108

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

SÉCURITÉ DES AUTOMATISMES INDUSTRIELS ET DES SYSTÈMES DE COMMANDE –

Partie 4-1: Exigences relatives au cycle de développement de produit sécurisé

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 62443-4-1 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 2018-01.

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 IEC 62443, publiées sous le titre général *Sécurité des automatismes industriels et des systèmes de commande*, peut être consultée sur le site web de l'IEC.

Les futures normes de cette série porteront dorénavant le nouveau titre général cité ci-dessus. Le titre des normes existant déjà dans cette série sera mis à jour lors de la prochaine édition.

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 ce document en utilisant une imprimante couleur.

INTRODUCTION

Le présent document fait partie d'une série de normes qui couvrent les questions de sécurité des automatismes industriels et des systèmes de commande (IACS – *industrial automation and control systems*). Il décrit les exigences relatives au cycle de développement de produit liées à la cybersécurité des produits destinés à être utilisés dans un environnement d'automatismes industriels et de systèmes de commande, et donne les recommandations qui permettent de satisfaire aux exigences décrites pour chaque élément.

L'établissement du présent document s'appuie dans une large mesure sur les exigences de certification SDLA (*Secure Development Life-cycle Assessment*) [26][1] de l'ISCI (*ISA Security Compliance Institute*). Il est à noter que la procédure SDLA repose sur les sources suivantes:

– ISO/IEC 15408-3 (Critères communs) [18];
– Open Web Application Security Project (OWASP) Comprehensive, Lightweight Application Security Process (CLASP) [36];
– The Security Development Life-cycle, par Michael Howard et Steve Lipner [43];
– IEC 61508, Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité [24], et
– RCTA DO-178B Software Considerations in Airborne Systems and Equipment Certification [28].

Par conséquent, toutes ces sources peuvent être considérées comme contribuant au présent document.

Le présent document est la partie de la série IEC 62443 qui contient les exigences de sécurité destinées aux développeurs de tous les produits d'automatisation et de commande pour lesquels la sécurité représente un enjeu.

La Figure 1 représente les relations entre les différentes parties de l'IEC 62443 existantes ou prévues à la date de diffusion du présent document. Celles qui sont citées en référence de manière normative sont incluses dans la liste des références normatives de l'Article 2, et celles qui sont citées en référence à titre d'information ou qui sont en cours d'élaboration sont énumérées dans la Bibliographie.

[1] Les chiffres entre crochets se réfèrent à la Bibliographie.

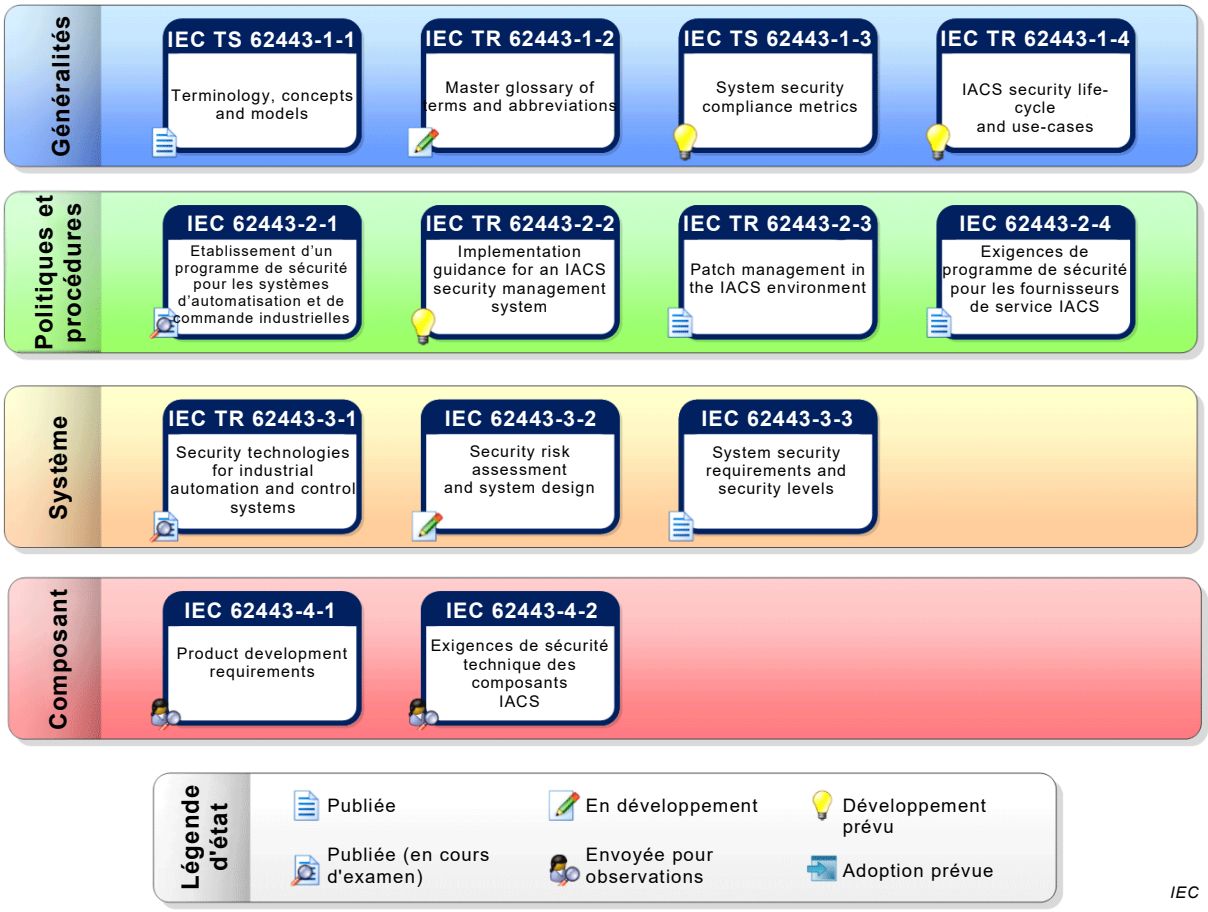


Figure 1 – Parties de la série IEC 62443

La Figure 2 représente la façon dont le produit développé est associé aux capacités de maintenance et d'intégration définies dans l'IEC 62443-2-4 et à son utilisation par le propriétaire d'actif. Le fournisseur de produit développe les produits en utilisant un procédé conforme au présent document. Il peut s'agir d'un seul composant (un contrôleur intégré, par exemple) ou d'un groupe de composants qui fonctionnent ensemble comme un système ou un sous-système. Les produits sont ensuite intégrés ensemble, en général par un intégrateur de système, à une Solution d'Automatisation selon un processus conforme à l'IEC 62443-2-4. La Solution d'Automatisation est ensuite installée sur un site particulier et devient une partie intégrante de l'automatisme industriel et du système de commande (IACS). Certaines de ces capacités font référence aux mesures de sécurité définies dans l'IEC 62443-3-3 [10] dont le fournisseur de service assure qu'elles sont prises en charge dans la Solution d'Automatisation (comme des caractéristiques du produit ou des mécanismes de compensation). Le présent document porte uniquement sur le processus de développement du produit. Il ne concerne pas la conception, l'installation ou le fonctionnement de la Solution d'Automatisation ou de l'IACS.

La Solution d'Automatisation représentée à la Figure 2 contient un ou plusieurs sous-systèmes et composants de prise en charge facultatifs (une commande avancée, par exemple). Les cases en pointillés indiquent que ces composants sont “facultatifs”.

NOTE 1 En règle générale, les Solutions d'automatisation ne comportent qu'un seul produit, mais elles peuvent en comporter plus. Dans certains secteurs industriels, il peut y avoir une structure de produits hiérarchique. En général, la Solution d'Automatisation comprend l'ensemble des matériels et logiciels, indépendants de l'emballage du produit, qui est utilisé pour contrôler un processus physique (continu ou de fabrication, par exemple) tel que défini par le propriétaire d'actif.

NOTE 2 Si un fournisseur de service fournit un produit utilisé dans la Solution d'Automatisation, il joue, dans le diagramme qui suit, le rôle de fournisseur de produit.

NOTE 3 Si un fournisseur de service fournit un produit utilisé dans la Solution d'Automatisation, il joue, dans le diagramme qui suit, le rôle de fournisseur de produit.

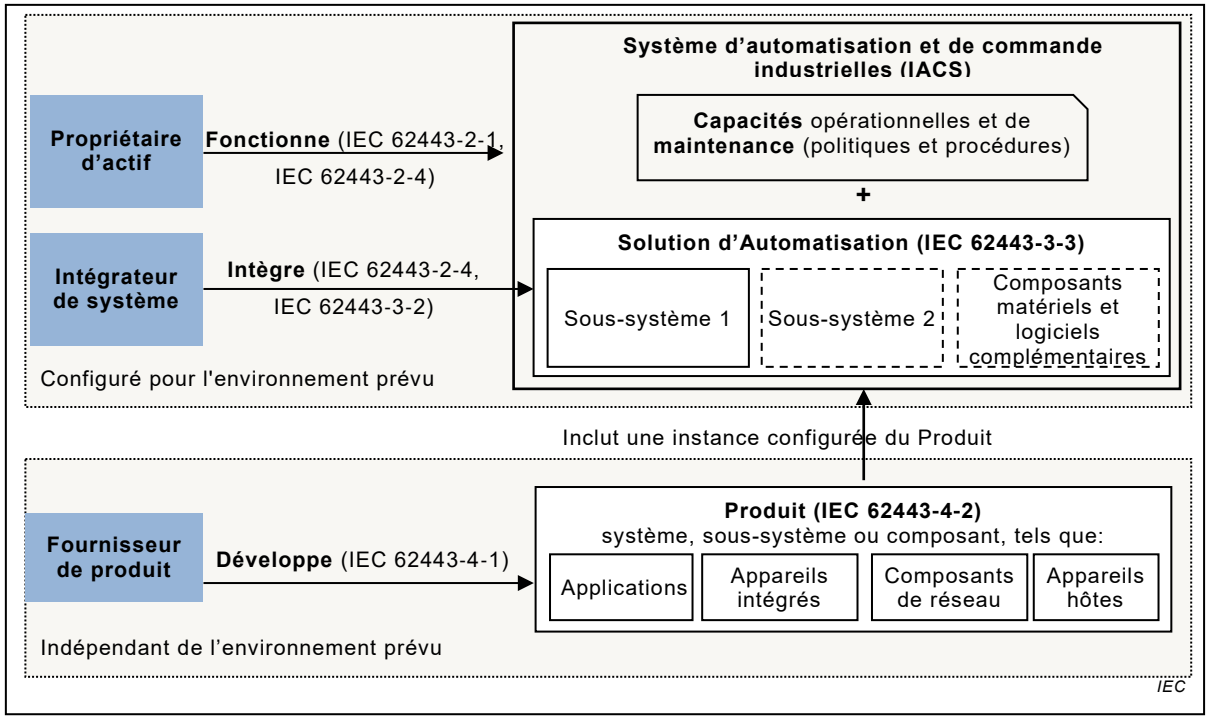


Figure 2 – Exemple de domaine d'application du cycle de vie du produit

SÉCURITÉ DES AUTOMATISMES INDUSTRIELS ET DES SYSTÈMES DE COMMANDE –

Partie 4-1: Exigences relatives au cycle de développement de produit sécurisé

1 Domaine d'application

La présente partie de l'IEC 62443 spécifie les exigences relatives au processus de développement sécurisé des produits utilisés dans des systèmes d'automatisation et de commande industriels. Elle définit un cycle de développement sécurisé (SDL – *secure development life-cycle*) en vue de développer et d'assurer la sécurité des produits. Ce cycle inclut la définition des exigences de sécurité, la conception sécurisée, la mise en œuvre sécurisée (y compris les lignes directrices en matière de codage), la vérification et la validation, la gestion des défauts, la gestion des correctifs et la fin de vie du produit. Ces exigences peuvent être appliquées à des processus nouveaux ou existants pour le développement, la maintenance et le retrait des matériels, logiciels et micrologiciels destinés aux produits nouveaux ou existants. Elles s'appliquent au développeur et au chargé de maintenance du produit, mais pas à l'intégrateur ni à l'utilisateur du produit. Une liste récapitulative des exigences du présent document peut être consultée à l'Annexe B.

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils 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 62443-2-4:2015, *Sécurité des automatismes industriels et des systèmes de commande – Partie 2-4: Exigences de programme de sécurité pour les fournisseurs de service IACS*
IEC 62443-2-4:2015/AMD1:2017