IEC 62443-4-2

Edition 1.0 2019-02

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components

Sécurité des systèmes d'automatisation et de commande industrielles – Partie 4-2: Exigences de sécurité technique des composants IACS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

ICS 25.040.40; 35.030

ISBN 978-2-8322-6597-0

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –

Part 4-2: Technical security requirements for IACS components

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 62443-4-2 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
65/735/FDIS	65/740/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

0.1 Overview

Industrial automation and control system (IACS) organizations increasingly use commercial-off-the-shelf (COTS) networked devices that are inexpensive, efficient and highly automated. Control systems are also increasingly interconnected with non-IACS networks for valid business reasons. These devices, open networking technologies and increased connectivity provide an increased opportunity for cyber-attack against control system hardware and software. That weakness may lead to health, safety and environmental (HSE), financial and/or reputational consequences in deployed control systems.

Organizations choosing to deploy business information technology (IT) cyber security solutions to address IACS security may not fully comprehend the results of their decision. While many business IT applications and security solutions can be applied to IACS, they should be applied in an appropriate way to eliminate inadvertent consequences. For this reason, the approach used to define system requirements is based on a combination of functional requirements and risk assessment, often including an awareness of operational issues as well.

IACS security countermeasures should not have the potential to cause loss of essential services and functions, including emergency procedures (IT security countermeasures, as often deployed, do have this potential). IACS security goals focus on control system availability, plant protection, plant operations (even in a degraded mode) and time-critical system response. IT security goals often do not place the same emphasis on these factors; they may be more concerned with protecting information rather than physical assets. These different goals should be clearly stated as security objectives regardless of the degree of plant integration achieved. A key step in the risk assessment, as required by IEC 62443-2-1[1] [1][2], should be the identification of which services and functions are truly essential for operations (for example, in some facilities engineering support may be determined to be a non-essential service or function). In some cases, it may be acceptable for a security action to cause temporary loss of a non-essential service or function, unlike an essential service or function that should not be adversely affected.

This document provides the cyber security technical requirements for the components that make up an IACS, specifically the embedded devices, network components, host components and software applications. Annex A describes categories of devices commonly used in IACSs. This document derives its requirements from the IACS system security requirements described in IEC 62443-3-3. The intent of this document is to specify security capabilities that enable a component to mitigate threats for a given security level (SL) without the assistance of compensating countermeasures. Annex B provides a table that summarizes the SLs of each of the requirements and requirement enhancements defined in this document.

The primary goal of the IEC 62443 series is to provide a flexible framework that facilitates addressing current and future vulnerabilities in IACS and applying necessary mitigations in a systematic, defensible manner. It is important to understand that the intention of the IEC 62443 series is to build extensions to enterprise security that adapt the requirements for business IT systems and combines them with the unique requirements for strong integrity and availability needed by IACS.

---

1 Many documents in the IEC 62443 series are currently under review or in development.

2 Numbers in square brackets refer to the bibliography.

0.2 Purpose and intended audience

The IACS community audience for this document is intended to be asset owners, system integrators, product suppliers, and, where appropriate, compliance authorities. Compliance authorities include government agencies and regulators with the legal authority to perform audits to verify compliance with governing laws and regulations.

System integrators will use this document to assist them in procuring control system components that make up an IACS solution. The assistance will be in the form of helping system integrators specify the appropriate security capability level of the individual components they require. The primary standards for system integrators are IEC 62443-2-1 [1], IEC 62443-2-4 [3], IEC 62443-3-2 [5][3] and IEC 62443-3-3 that provide organizational and operational requirements for a security management system and guide them through the process of defining security zones for a system and the target security capability levels (SL-T) for those zones. Once the SL-T for each zone has been defined, components that provide the necessary security capabilities can be used to achieve the SL-T for each zone.

Product suppliers will use this document to understand the requirements placed on control system components for specific security capability levels (SL-C) of those components. A component may not provide a required capability itself but may be designed to integrate with a higher-level entity and thus benefit from that entity's capability – for example an embedded device may not be maintaining a user directory itself, but may integrate with a system wide authentication and authorization service and thus still meet the requirements to provide individual user authentication, authorization and management capabilities. This document will guide product suppliers as to which requirements can be allocated and which requirements should be native in the components. As defined in Practice 8 of IEC 62443-4-1, the product supplier will provide documentation on how to properly integrate the component into a system to meet a specific SL-T.

The component requirements (CRs) in this document are derived from the system requirements (SRs) in IEC 62443-3-3. The requirements in IEC 62443-3-3 are referred to as SRs, which are derived from the overall foundational requirements (FRs) defined in IEC 62443-1-1. CRs may also include a set of requirement enhancements (REs). The combination of CRs and REs is what will determine the target security level that a component is capable of.

This document provides component requirements for four types of components: software application, embedded device, host device and network device. Thus, the CRs for each type of component will be designated as follows:

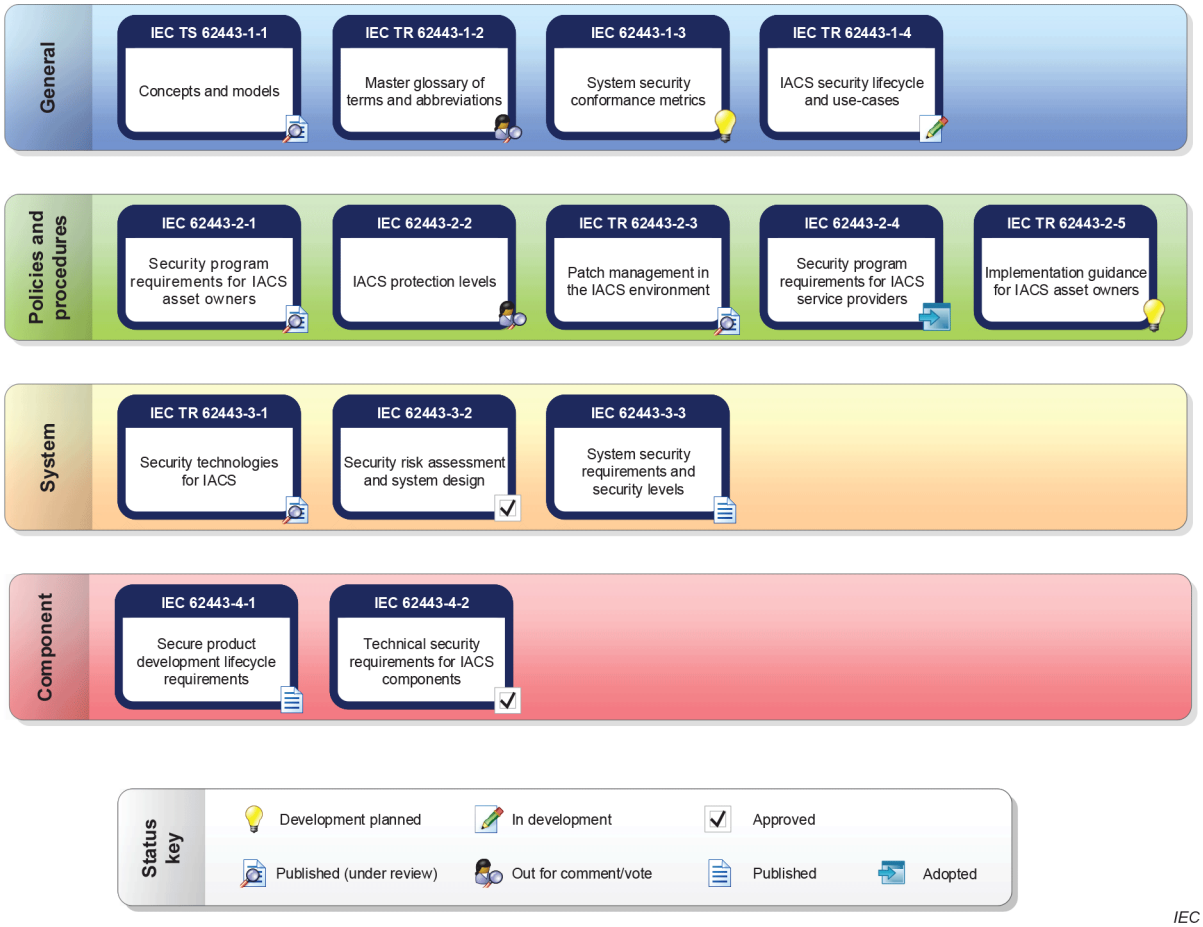
- Software application requirements (SAR);
- Embedded device requirements (EDR);
- Host device requirements (HDR); and
- Network device requirements (NDR).

The majority of the requirements in this document are the same for the four types of components and are thus designated simply as a CR. When there are unique component-specific requirements then the generic requirement will state that the requirements are component-specific and are located in the component-specific requirements clauses of this document.

Figure 1 shows a graphical depiction of the IEC 62443 series when this document was written.

---

3 Under preparation. Stage at the time of publication: IEC PRVC 62443-3-2:2018.



IEC

Figure 1 – Parts of the IEC 62443 series

SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –

Part 4-2: Technical security requirements for IACS components

1 Scope

This part of IEC 62443 provides detailed technical control system component requirements (CRs) associated with the seven foundational requirements (FRs) described in IEC TS 62443-1-1 including defining the requirements for control system capability security levels and their components, SL-C(component).

As defined in IEC TS 62443-1-1 there are a total of seven foundational requirements (FRs):

a) identification and authentication control (IAC),

b) use control (UC),

c) system integrity (SI),

d) data confidentiality (DC),

e) restricted data flow (RDF),

f) timely response to events (TRE), and

g) resource availability (RA).

These seven FRs are the foundation for defining control system security capability levels. Defining security capability levels for the control system component is the goal and objective of this document as opposed to SL-T or achieved SLs (SL-A), which are out of scope.

NOTE 1 Refer to IEC 62443-2-1 [1] for an equivalent set of non-technical, program-related, capability requirements necessary for fully achieving a SL-T(control system).

NOTE 2 The trademarks and trade names mentioned in this document are given for the convenience of users of this document. This information does not constitute an endorsement by IEC of the products named.

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

IEC 62443-3-3:2013, *Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels*

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

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

SÉCURITÉ DES SYSTÈMES D'AUTOMATISATION ET DE COMMANDE INDUSTRIELLES –

Partie 4-2: Exigences de sécurité technique des composants IACS

AVANT-PROPOS

1) La Commission Electrotechnique 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 62443-4-2 a été établie par le comité d'études 65 de l'IEC: Mesure, commande et automation dans les processus industriels.

Le texte de cette Norme internationale est issu des documents suivants:

FDIS	Rapport de vote
65/735/FDIS	65/740/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à l'approbation de cette Norme internationale.

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 systèmes d'automatisation et de commande industrielles*, 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 cette publication en utilisant une imprimante couleur.

INTRODUCTION

0.1 Vue d'ensemble

L'industrie des systèmes d'automatisation et de commande industrielles (IACS) utilise de plus en plus les appareils en réseau sur étagère (COTS), peu onéreux, rentables et hautement automatisés. En outre, les systèmes de commande et les réseaux non IACS sont de plus en plus interconnectés, et ce, pour des raisons commerciales tangibles. Ces appareils, technologies de réseau ouvert et connectivités accrues sont exposés dans une plus large mesure aux cyberattaques contre les matériels et les logiciels de système de commande. Cette faiblesse peut avoir des conséquences sur la santé, la sécurité et l'environnement (HSE), des conséquences financières et/ou des conséquences sur la réputation des systèmes de commande déployés.

Les organisations qui choisissent de déployer des solutions en matière de cybersécurité des technologies de l'information (IT) d'entreprise pour assurer la sécurité du système d'automatisation et de commande industrielles (IACS) peuvent ne pas totalement appréhender les effets de leur décision. Même si de nombreuses applications IT d'entreprise et solutions de sécurité peuvent être appliquées à l'IACS, il convient de le faire de manière appropriée afin d'éliminer toutes les conséquences indésirables. C'est la raison pour laquelle la méthode de définition des exigences du système est fondée sur une combinaison d'exigences fonctionnelles et d'appréciation du risque, ce qui implique souvent d'être également sensible aux enjeux opérationnels.

Il convient que les contre-mesures mises en place en matière de sécurité IACS ne soient pas susceptibles de provoquer des pertes de services et de fonctions essentiels, y compris les procédures d'urgence (les contre-mesures de sécurité IT, souvent déployées, présentent ce risque). La sécurité IACS a pour principaux objectifs la disponibilité du système de commande, la protection de l'usine, le fonctionnement de l'usine (même en mode dégradé) et la réponse du système prioritaire. Souvent, la sécurité informatique ne met pas ces facteurs sur le même plan. La plupart du temps, il peut s'agir de protéger les informations plutôt que les actifs physiques. Il convient de définir clairement ces différents objectifs comme relevant de la sécurité, quel que soit le degré d'intégration atteint. Il convient qu'une étape fondamentale de l'appréciation du risque, telle qu'exigée par l'IEC 62443-2-1[1] [1][2], consiste à identifier les services et fonctions réellement essentiels pour le fonctionnement (dans certaines installations, le support technique peut être déterminé comme étant un service ou une fonction non essentiel(le), par exemple). Dans certains cas, il peut être acceptable, dans le cadre d'une action de sécurité, de provoquer la perte temporaire d'un service ou d'une fonction non essentiel(le), à l'inverse d'un service ou d'une fonction essentiel(le) qu'il convient de ne pas affecter.

Le présent document fournit les exigences techniques en matière de cybersécurité des composants d'un IACS, en particulier des appareils intégrés, des composants de réseau, des composants hôtes et des applications logicielles. L'Annexe A décrit des catégories d'appareils couramment utilisés dans les IACS. Les exigences du présent document sont déduites des exigences de sécurité des systèmes IACS décrites dans l'IEC 62443-3-3. Le présent document a pour objet de spécifier les capacités de sécurité permettant à un composant d'atténuer les menaces pesant sur un système présentant un niveau de sécurité (SL) donné sans l'aide de contre-mesures compensatoires. Un tableau récapitulant les SL de chacune des exigences et améliorations d'exigences définies dans le présent document est donné à l'Annexe B.

---

1 De nombreux documents de la série IEC 62443 sont en cours de révision ou d'élaboration.

2 Les chiffres entre crochets se réfèrent à la bibliographie.

L'objectif principal de la série IEC 62443 est de fournir un cadre souple permettant de résoudre aisément les vulnérabilités actuelles et futures des IACS, et de mettre en œuvre les mesures d'atténuation nécessaires de manière systématique et justifiable. Il est important de bien comprendre que la série IEC 62443 vise à étendre la sécurité d'entreprise afin d'adapter les exigences des systèmes IT d'entreprise et les combine aux exigences uniques de fortes intégrité et disponibilité dont ont besoin les IACS.

0.2 Objet et public visé

Dans la communauté IACS, le présent document s'adresse aux propriétaires d'actifs, aux intégrateurs systèmes, aux fournisseurs de produits et, le cas échéant, aux autorités compétentes. Les autorités compétentes sont les organismes gouvernementaux et les organismes de réglementation ayant autorité légale de procéder à des audits pour vérifier la conformité aux lois et règlements en vigueur.

Les intégrateurs systèmes se fondent sur le présent document pour procurer les composants de système de commande qui constituent la solution IACS. En effet, le présent document leur permet de spécifier le niveau de capacité de sécurité approprié des composants individuels qu'ils exigent. Les principales normes destinées aux intégrateurs systèmes sont l'IEC 62443-2-1 [1], l'IEC 62443-2-4 [3], l'IEC 62443-3-2 [5] [3] et l'IEC 62443-3-3. Ces normes indiquent les exigences organisationnelles et opérationnelles pour les systèmes de gestion de la sécurité et les orientent tout au long du processus de définition des zones de sécurité et des niveaux de capacité de sécurité (SL-T) à atteindre pour ces zones. Lorsque le SL-T de chaque zone a été défini, les composants présentant les capacités nécessaires de sécurité peuvent être utilisés pour atteindre le SL-T pour chaque zone.

Les fournisseurs de produits utilisent le présent document pour bien comprendre les exigences dont font l'objet les composants du système de commande pour leur niveau de capacité de sécurité (SL-C) spécifique. Un composant peut ne pas fournir une capacité exigée lui-même, mais peut être conçu pour être intégré à une entité de niveau supérieur et, par conséquent, bénéficier de ses capacités (par exemple, un appareil intégré peut ne pas maintenir lui-même un répertoire utilisateur, mais peut être intégré à un service d'authentification et d'autorisation au niveau du système, et donc toujours satisfaire aux exigences en matière de capacités d'authentification, d'autorisation et de gestion d'utilisateurs individuels). Le présent document aide les fournisseurs de produits à connaître les exigences pouvant être attribuées et les exigences convenues comme natives dans les composants. Comme cela a été défini dans la Pratique 8 de l'IEC 62443-4-1, le fournisseur de produit met à disposition la documentation relative à l'intégration correcte du composant dans un système afin de satisfaire à un SL-T spécifique.

Dans le présent document, les exigences relatives au composant (CR) sont déduites des exigences relatives au système (SR) indiquées dans l'IEC 62443-3-3. Les exigences de l'IEC 62443-3-3, appelées SR, sont déduites des exigences fondamentales (FR) générales définies dans l'IEC 62443-1-1. Les exigences relatives au composant (CR) peuvent également inclure un ensemble d'améliorations d'exigences (RE). La combinaison des CR et des RE détermine le niveau de sécurité cible qu'un composant est capable d'atteindre.

Le présent document donne les exigences pour quatre types de composants: application logicielle, appareil intégré, appareil hôte et appareil de réseau. Ainsi, les exigences pour chaque type de composant se présentent comme suit:

- Exigences relatives aux applications logicielles (SAR);
- Exigences relatives aux appareils intégrés (EDR);
- Exigences relatives aux appareils hôtes (HDR); et
- Exigences relatives aux appareils de réseaux (NDR);

---

3 En cours d'élaboration. Stade au moment de la publication IEC PRVC 62443-3-2:2018.

La majorité des exigences du présent document sont les mêmes pour les quatre types de composants et sont donc de simples exigences relatives au composant. En présence d'exigences spécifiques à un seul composant, l'exigence générique les signale comme telles et précise qu'elles se trouvent dans les articles du présent document relatifs aux exigences spécifiques au composant.

La Figure 1 est une représentation graphique de la série IEC 62443 lors de la rédaction du présent document.

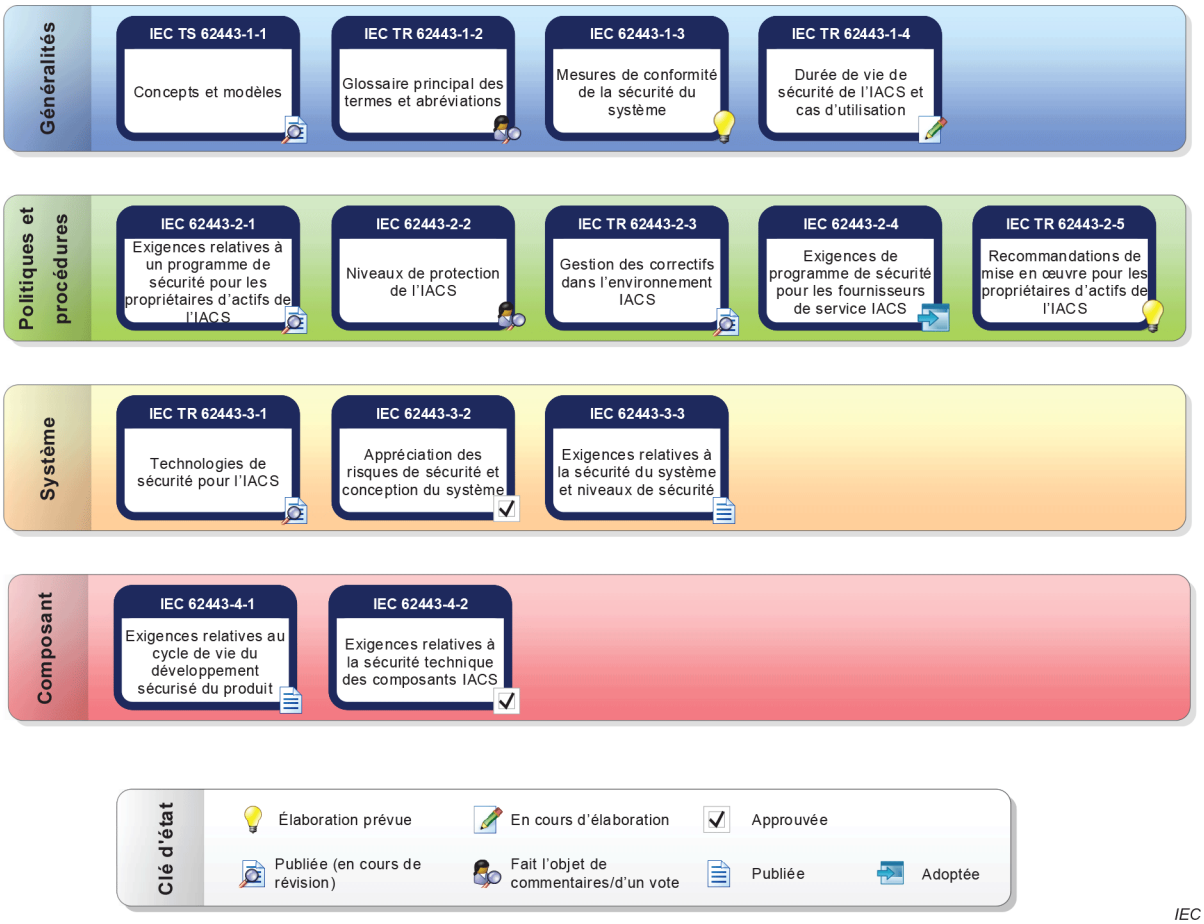


Figure 1 – Parties de la série IEC 62443

SÉCURITÉ DES SYSTÈMES D'AUTOMATISATION ET DE COMMANDE INDUSTRIELLES –

Partie 4-2: Exigences de sécurité technique des composants IACS

1 Domaine d'application

La présente partie de l'IEC 62443 indique les exigences relatives au composant (CR) d'un système de commande technique ainsi que les sept exigences fondamentales (FR) décrites dans l'IEC TS 62443-1-1, y compris la définition des exigences relatives aux niveaux de sécurité de capacité des systèmes de commande et à leurs composants, SL-C(composant).

Comme l'indique l'IEC TS 62443-1-1, il existe en tout sept exigences fondamentales (FR):

a) contrôle d'identification et d'authentification (IAC),
b) contrôle d'utilisation (UC),
c) intégrité du système (SI),
d) confidentialité des données (DC),
e) transfert de données limité (RDF),
f) réponse appropriée aux événements (TRE), et
g) disponibilité des ressources (RA).

Ces sept exigences fondamentales sont à la base de la définition des niveaux de capacité de sécurité des systèmes de commande. Le présent document a pour objet de définir les niveaux de capacité de sécurité du composant du système de commande, par opposition au SL-T ou aux niveaux de sécurité atteints (SL-A), qui n'entrent pas dans le domaine d'application.

NOTE 1 Voir l'IEC 62443-2-1 [1] pour obtenir un ensemble équivalent d'exigences de capacité non techniques liées aux programmes, nécessaires pour atteindre un niveau SL-T(système de commande).

NOTE 2 Les appellations et marques mentionnées dans le présent document sont données à l'intention des utilisateurs du présent document. Cette information ne signifie nullement que l'IEC approuve ou recommande l'emploi exclusif des produits ainsi désignés.

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 TS 62443-1-1, *Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models* (disponible en anglais seulement)

IEC 62443-3-3:2013, *Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels* (disponible en anglais seulement)

IEC 62443-4-1, *Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements* (disponible en anglais seulement)