COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

RÉSEAUX INDUSTRIELS DE COMMUNICATION – SÉCURITÉ DANS LES RÉSEAUX ET LES SYSTÈMES –

Partie 3-3: Exigences de sécurité des systèmes et niveaux de sécurité

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 62443-3-3 a été établie par le comité d'études 65 de l'IEC: Mesure, commande et automation dans les processus industriels.

La présente version bilingue (2019-01) correspond à la version anglaise monolingue publiée en 2013-08.

Le texte anglais de cette norme est issu des documents 65/531/FDIS et 65/540/RVD.

Le rapport de vote 65/540/RVD donne toute information sur le vote ayant abouti à l'approbation de cette norme.

La version française de cette norme n'a pas été soumise au vote.

Cette publication a été rédigée selon les Directives ISO/IEC, Partie 2.

Une liste de toutes les parties de la série IEC 62443, publiées sous le titre général *Réseaux industriels de communication – Sécurité dans les réseaux et les systèmes*, peut être consultée sur le site web de l'IEC.

Le comité a décidé que le contenu de cette publication 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 à la publication recherchée. À cette date, la publication sera

- reconduite,
- supprimée,
- remplacée par une édition révisée, ou
- amendée.

Le contenu du corrigendum d'avril 2014 est inclus dans la présente copie.

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.

0 Introduction

0.1 Vue d'ensemble

NOTE 1 La présente norme fait partie d'une série de normes traitant de la sécurité des systèmes d'automatisation et de commande industrielles (IACS). Elle a été élaborée par le groupe de travail 4, sous-groupe de travail 2 du comité 99 de l'IEC, en coopération avec le GT 10 du CE 65 de l'IEC. Le présent document spécifie les exigences de sécurité des systèmes de commande associées aux sept exigences fondamentales définies dans l'IEC 62443-1-1, et assigne des niveaux de sécurité (SL - *security level*) de système aux systèmes à l'étude (SuC - *system under consideration*).

NOTE 2 Le format de la présente norme suit les exigences de l'ISO/IEC traitées dans les directives ISO/IEC, Partie 2 [11].[1] Ces directives spécifient le format de la norme ainsi que l'utilisation des termes comme «devoir», «il convient» et «pouvoir». Les exigences spécifiées dans les articles normatifs utilisent les conventions traitées dans l'Appendice H des directives de l'ISO/IEC.

Les organismes de système d'automatisation et de commande industrielles (IACS) utilisent de plus en plus de dispositifs de réseau commerciaux (COTS - *commercial-off-the-shelf*) peu coûteux, efficaces et très automatisés. Les systèmes de commande sont également de plus en plus interconnectés avec des réseaux non IACS pour des raisons commerciales valables. Ces dispositifs, les technologies de réseau ouvertes, ainsi que la connectivité croissante augmentent le risque de cyberattaque contre le matériel et le logiciel du système de commande. Cette faiblesse peut avoir des conséquences au niveau de la santé, sécurité et environnement (HSE - *health, safety and environmental*), des conséquences financières et/ou des conséquences au niveau de la réputation dans les systèmes de commande déployés.

Les organismes qui déploient des solutions de cybersécurité pour le traitement de l'information (IT - *information technology*) commerciale pour traiter de la sécurité des équipements IACS peuvent ne pas pleinement concevoir les résultats de ces décisions. Nombre des applications IT commerciales et solutions de sécurité peuvent être appliquées aux équipements IACS, mais elles doivent l'être de façon appropriée afin d'éviter toute conséquence indésirable. Pour cette raison, l'approche utilisée pour définir les exigences système doit se baser sur une combinaison d'exigences fonctionnelles et d'appréciation du risque, comprenant également le plus souvent une connaissance des problèmes fonctionnels.

Il convient que les mesures de sécurité des IACS n'aient pas la capacité de causer la perte des services et fonctions essentiels, procédures d'urgence incluses. (Ce qui est le cas des mesures de sécurité IT le plus souvent déployées.) Les objectifs de la sécurité IACS se concentrent sur la disponibilité du système de commande, sur la protection des installations et sur leur fonctionnement (même en mode dégradé), et sur la réponse système limitée dans le temps. Les objectifs de la sécurité IT n'accordent généralement pas la même importance à ces aspects. Ils peuvent être plus tournés vers la protection des informations que vers les actifs physiques. Ces objectifs différents doivent être clairement établis en tant que qu'objectifs de sécurité, sans tenir compte du degré d'intégration des installations. Il convient que l'identification des services et fonctions essentiels au fonctionnement, telle qu'exigée par l'IEC 62443-2-1[2], soit une étape clé de l'appréciation du risque. (Par exemple, dans certaines installations, le soutien technique peut être défini comme étant une fonction ou un service non essentiel.) Dans certains cas, il peut être acceptable qu'une action de sécurité cause une perte temporaire d'une fonction ou d'un service non essentiel, contrairement à une fonction ou un service essentiel qu'il convient de ne pas compromettre.

La présente norme part du principe qu'un programme de sécurité a été établi et qu'il est fonctionnel conformément à l'IEC 62443-2-1. En outre, la gestion des correctifs est par principe mise en œuvre conformément aux recommandations détaillées dans l'IEC/TR 62443-2-3 [5], en utilisant les exigences de système de commande appropriées et les améliorations d'exigences, comme décrit dans la présente norme. De plus, l'IEC 62443-3-2 [8] décrit la façon dont un projet définit les niveaux de sécurité (SL) basés

---

1 Les chiffres entre crochets se réfèrent à la Bibliographie.

2 De nombreux documents de la série IEC 62443 sont actuellement à l'étude ou en cours d'élaboration.

sur le risque. Ces derniers sont ensuite utilisés pour sélectionner des produits avec les capacités de sécurité techniques appropriées, comme cela est détaillé dans la présente norme. L'apport majeur de la présente norme inclut l'ISO/IEC 27002 [15] et le NIST SP800-53, rév. 3 [24] (voir l'Article 2 et la Bibliographie pour une liste plus complète des sources documentaires).

La série IEC 62443 a principalement pour objet de fournir un cadre flexible qui facilite le traitement des vulnérabilités actuelles et futures dans l'IACS et l'application des atténuations nécessaires de manière systématique et défendable. Il est important de comprendre que l'intention de la série IEC 62443 est de construire des extensions à la sécurité des entreprises qui adaptent les exigences pour les systèmes IT commerciaux et les combinent avec les exigences uniques pour la disponibilité forte dont l'IACS a besoin.

0.2 Objectif et public visé

Le public de la communauté IACS visé par la présente norme est constitué des propriétaires d'actif, des intégrateurs de système, des fournisseurs de produit, des fournisseurs de service et, lorsque cela est approprié, des autorités de conformité. Les autorités de conformité comprennent les agences et régulateurs gouvernementaux ayant l'autorité légale à réaliser des audits permettant de vérifier la conformité aux lois et régulations en vigueur.

Les intégrateurs de système, fournisseurs de produit et fournisseurs de service utilisent la présente norme pour évaluer la capacité de fourniture de sécurité fonctionnelle de leurs produits et services afin de satisfaire aux exigences de niveau de sécurité cible (SL-T - *target security level*) du propriétaire d'actif. Comme pour l'évaluation des SL-T, l'applicabilité des exigences de système de commande individuelles (SR - *system requirement*) et des améliorations d'exigences (RE - *requirement enhancement*) doivent se baser sur les politiques de sécurité, procédures et appréciation du risque du propriétaire d'actif dans le contexte de leur site spécifique. Il est à noter que certaines SR contiennent des conditions spécifiques pour les exceptions admissibles, comme lorsque la conformité aux SR enfreint les exigences fondamentales de fonctionnement d'un système de commande (ce qui peut entraîner des contre-mesures compensatoires).

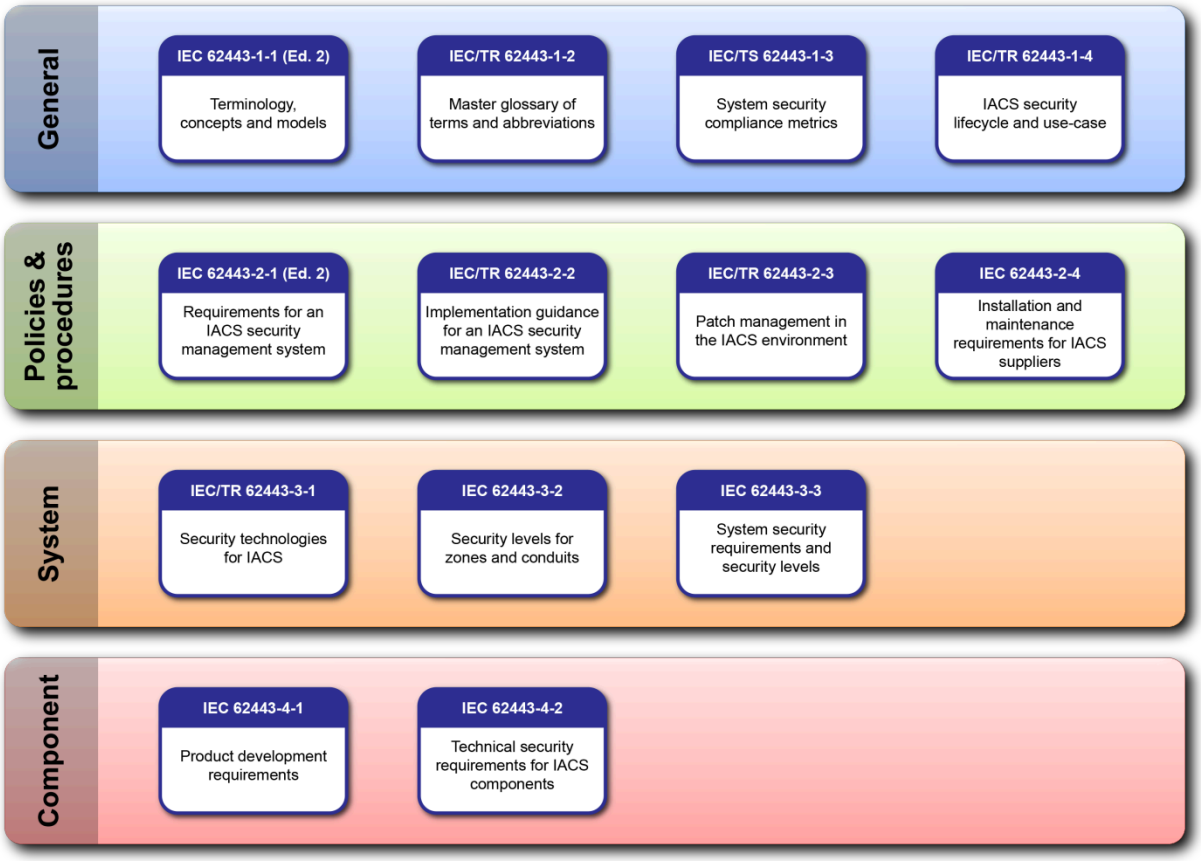
Lors de la conception d'un système de commande conformément à l'ensemble des SR associées aux SL-T spécifiques, il n'est pas nécessaire que chaque composant du système de commande proposé prenne en charge chaque exigence système au niveau imposé dans la présente norme. Des contre-mesures compensatoires peuvent être employées afin de fournir les fonctionnalités nécessaires à d'autres sous-systèmes, de façon à ce que les exigences générales SL-T soient satisfaites au niveau du système de commande. Il convient que l'inclusion des contre-mesures compensatoires lors de la phase de conception soit accompagnée par une documentation complète de façon à ce que le SL et le SL-A (système de commande) du système de commande atteint reflètent pleinement les capacités de sécurité prévues inhérentes à la conception. De même, lors de l'essai de certification et/ou des audits post-installation, des contre-mesures compensatoires peuvent être utilisées et documentées afin de satisfaire au SL général du système de commande.

La présente norme n'est pas assez détaillée pour concevoir et construire une architecture de sécurité intégrée. Cela exige une analyse supplémentaire au niveau du système et l'élaboration d'exigences dérivées qui sont le sujet d'autres normes de la série IEC 62443 (voir 0). Il est à noter que la présente norme n'a pas pour objet de fournir des spécifications assez détaillées pour construire une architecture de sécurité. L'objectif est de définir un ensemble d'exigences minimales et communes pour atteindre progressivement des niveaux de sécurité plus élevés. La conception effective d'une architecture qui satisfait à ces exigences relève des intégrateurs de système et des fournisseurs de produit. Ces derniers disposent d'une liberté de choix individuels, ce qui renforce la compétition et l'innovation. Ainsi, la présente norme adhère strictement aux exigences fonctionnelles spécifiques, et ne traite pas de la manière dont il convient de satisfaire à ces exigences.

0.3 Utilisation dans d'autres parties de la série IEC 62443

La Figure 1 donne une représentation graphique de la série IEC 62443 lors de la rédaction de la présente norme.

L'IEC 62443-3-2 utilise les SR et RE comme liste de vérification. Après que le système à l'étude (SuC) a été décrit en matière de zones et conduits, et qu'un SL cible individuel a été assigné à ces zones et conduits, les SR et RE dans la présente norme, ainsi que leur mapping aux SL de capacité (SL-C), sont utilisés pour dresser une liste d'exigences auxquelles la conception du système de commande doit satisfaire. L'intégrité de la conception de système de commande donnée peut alors être vérifiée, et ainsi fournir les SL-A.



Anglais	Français
General	Généralités
Policies & procedures	Politiques et procédures
System	Système
Component	Composant

Figure 1 – Structure de la série IEC 62443

L'IEC/TS 62443-1-3 [2] utilise les exigences fondamentales (FR - *foundational requirement*), les SR, les RE et le mapping aux SL-C comme liste de vérification pour l'essai d'intégrité de la spécification des critères quantitatifs. Les critères quantitatifs de conformité à la sécurité dépendent du contexte. Avec l'IEC 62443-3-2, les évaluations SL-T du propriétaire d'actif sont traduites en critères quantitatifs pouvant être utilisés pour la prise en charge de l'analyse du système, pour la conception d'études de compromis, et pour l'élaboration d'une architecture de sécurité.

L'IEC 62443-4-1 [9] traite des exigences générales lors de l'élaboration de produits. Comme telle, l'IEC 62443-4-1 est centrée sur le fournisseur de produit. Les exigences de sécurité des produits sont issues de la liste des exigences de base et des RE spécifiées dans la présente norme. Les spécifications normatives de qualité de l'IEC 62443-4-1 sont utilisées lors de l'élaboration des capacités de ces produits.

L'IEC 62443-4-2 [10] contient des ensembles d'exigences dérivées qui fournissent un mapping détaillé des SR spécifiées dans la présente norme aux sous-systèmes et composants du SuC. Au moment de la rédaction de la présente norme, les catégories de composants traités dans l'IEC 62443-4-2 étaient: les appareils intégrés, les appareils hôtes, les dispositifs de réseau et les applications. En tant que telle, l'IEC 62443-4-2 est centrée sur le fournisseur (de produit et de service). Les exigences de sécurité des produits sont d'abord issues de la liste des exigences de base et des RE spécifiées dans la présente norme. Les exigences et critères de sécurité de l'IEC 62443-3-2 et de l'IEC/TS 62443-1-3 sont utilisés pour approfondir ces exigences normatives dérivées.

RÉSEAUX INDUSTRIELS DE COMMUNICATION – SÉCURITÉ DANS LES RÉSEAUX ET LES SYSTÈMES –

Partie 3-3: Exigences de sécurité des systèmes et niveaux de sécurité

1 Domaine d'application

La présente partie de la série IEC 62443 fournit des exigences système (SR) de commande techniques détaillées associées aux sept exigences fondamentales (FR) décrites dans l'IEC 62443-1-1, y compris la définition des exigences des niveaux de sécurité de capacité du système de commande, SL-C (système de commande). Ces exigences sont utilisées par plusieurs membres de la communauté des systèmes d'automatisation et de commande industrielles (IACS) ainsi que les zones et conduits définis pour le système à l'étude (SuC), tout en développant le SL cible du système de commande approprié, SL-T (système de commande) pour un actif spécifique.

Comme cela est défini dans l'IEC 62443-1-1, il existe sept FR au total:

a) Commande d'identification et d'authentification (IAC - *identification and authentication control*),
b) Commande d'utilisation (UC - *use control*),
c) Intégrité du système (SI - *system integrity*),
d) Confidentialité des données (DC - *data confidentiality*),
e) Flux de données réduit (RDF - *restricted data flow*),
f) Réponse rapide aux événements (TRE - *timely response to events*),
g) Disponibilité des ressources (RA - *ressource availability*).

Ces sept exigences constituent le fondement des SL de capacité du système de commande, SL-C (système de commande). La présente norme a pour objet de définir la capacité de sécurité au niveau du système de commande. Les SL cible (SL-T) ou les SL atteints (SL-A), quant à eux, ne relèvent pas du domaine d'application de la présente norme.

Voir l'IEC 62443-2-1 pour un ensemble équivalent de SR de capacité non techniques et relatives au programme nécessaires pour atteindre pleinement un SL cible de système de commande.

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 62443-1-1:2009, *Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models* (disponible en anglais seulement)

IEC 62443-2-1, *Réseaux industriels de communication – Sécurité dans les réseaux et les systèmes – Partie 2-1: Établissement d'un programme de sécurité pour les systèmes d'automatisation et de commande industrielles*