Edition 2.0 2024-08

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Security for industrial automation and control systems – Part 2-1: Security program requirements for IACS asset owners

Sécurité des systèmes d'automatisation et de commande industrielles – Partie 2-1: Exigences de programme de sécurité pour les propriétaires d'actif IACS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

ICS 25.040.40, 35.100.05

ISBN 978-2-8322-9459-8

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –

Part 2-1: Security program requirements for IACS asset owners

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) IEC draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). IEC takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, IEC had not received notice of (a) patent(s), which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at https://patents.iec.ch. IEC shall not be held responsible for identifying any or all such patent rights.

IEC 62443-2-1 has been prepared by IEC technical committee 65: Industrial process measurement, control and automation, in collaboration with the liaison ISA99: ISA committee on Security for industrial automation and control systems. It is an International Standard.

This second edition cancels and replaces the first edition published in 2010. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

a) revised requirement structure into SP elements (SPEs),
b) revised requirements to eliminate duplication of an information security management system (ISMS), and
c) defined a maturity model for evaluating requirements.

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

Draft	Report on voting
65/1044/FDIS	65/1053/RVD

Full information on the voting for its approval can be found in the report on voting indicated in the above table.

The language used for the development of this International Standard is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/publications.

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 webstore.iec.ch in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn, or
- revised.

IMPORTANT – The "colour inside" logo on the cover page of this document 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 the part of the IEC 62443 series that contains security requirements for industrial automation and control system (IACS) asset owners. In the context of this document, asset owner also includes the operator of the IACS. Its requirements focus on cybersecurity and allow security capabilities that meet them to be provided as a combination of technical, physical, process and compensating security measures.

Cybersecurity is an increasingly important topic in modern organizations. The term cybersecurity is generally used to describe the set of security measures or practices taken to protect a computer or computer system against unauthorized access or attack. In IACS, the most significant concerns include unwanted access or attacks resulting in the IACS not performing the correct functions in the required timeframe.

A very common engineering approach when faced with a challenging problem is to break the problem into smaller pieces and address each piece in a disciplined manner. This approach is a sound one for addressing cybersecurity risks with IACS. However, a frequent mistake is to deal with cybersecurity one system at a time. Cybersecurity is a much larger challenge that should address all IACS components as well as the policies, procedures, practices and personnel that surround and utilize those IACS. Implementing such a wide-ranging management system can require a cultural change within the organization.

Addressing cybersecurity on an organization-wide basis can seem like a daunting task. There is no simple cookbook for security, nor is there a one-size-fits-all set of security practices. Absolute security can be achievable but is probably undesirable because of the loss of functionality that would be necessary to achieve this near perfect state. Security is a balance of risk versus cost.

Each situation will be different. In some situations, the risk can be related to health, safety and environmental (HSE) factors rather than purely economic impact. The risk can have an unrecoverable consequence rather than a temporary financial setback. Therefore, a predetermined set of mandatory security practices can either be overly restrictive and likely quite costly to implement or be insufficient to address the risk.

This document supports the need to address cybersecurity for an IACS in operation by providing requirements for establishing, implementing, maintaining and continually improving an IACS security program (SP). These requirements, when implemented conscientiously, provide security capabilities whose purpose is to reduce IACS security risks to a tolerable level. These requirements are written to be implementation independent, allowing asset owners to select approaches most suitable to their needs. IEC 62443-3-2 [1][1] describes the methodology for addressing cybersecurity risks in an IACS system design and that assists in the identification of risks and the selection of appropriate security requirements and associated capabilities for an IACS SP.

Commercial-off-the-shelf (COTS) products are often not ruggedized or rigorously engineered enough for IACS environments, where they can introduce additional vulnerabilities and threats to the IACS.

---

1 Numbers in square brackets refer to the Bibliography.

When COTS technologies are used in an IACS, they are often configured to meet IACS specific functional needs and operational constraints. For example, security event handling in COTS products may be configured differently for IACS applications than they are for traditional information technology (IT) applications. Typical COTS equipment is designed for environments where the primary objective is the protection of information. In an IACS environment, the primary objectives are the protection of the HSE of the facility and the minimization of the operational and business impact on facility operation. COTS technologies can be applied to IACS applications, but the risks associated with using these technologies need to be understood by the asset owner.

Some organizations can attempt to use pre-existing IT and business cybersecurity solutions to address security for IACS without understanding the consequences. While many of these solutions can be applied to IACS, it is important to apply them correctly to eliminate inadvertent and undesired consequences. For example, in an IACS, availability may have a higher priority than confidentiality, as opposed to typical IT applications.

Asset owners may wish to apply their IACS SP across the organization to address the organization needs and objectives, security requirements, business and work processes, as well as the organization size and structure. All of these influencing factors are dynamic and will likely change over time. Thus, the adoption of an IACS SP is a strategic decision for the organization.

The effectiveness of an IACS SP is often enhanced through coordination or integration with the organization’s processes and overall information security management system (ISMS). For example, security can be added to the organization supply chain processes to require security in the design of processes, systems and controls. It is also expected that IACS SP will be scaled in accordance with the needs of the IACS and the organization.

SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –

Part 2-1: Security program requirements for IACS asset owners

1 Scope

This part of IEC 62443 specifies asset owner security program (SP) policy and procedure requirements for an industrial automation and control system (IACS) in operation. This document uses the broad definition and scope of what constitutes an IACS as described in IEC TS 62443-1-1. In the context of this document, asset owner also includes the operator of the IACS.

This document recognizes that the lifespan of an IACS can exceed twenty years, and that many legacy systems contain hardware and software that are no longer supported. Therefore, the SP for most legacy systems addresses only a subset of the requirements defined in this document. For example, if IACS or component software is no longer supported, security patching requirements cannot be met. Similarly, backup software for many older systems is not available for all components of the IACS. This document does not specify that an IACS has these technical requirements. This document states that the asset owner needs to have policies and procedures around these types of requirements. In the case where an asset owner has legacy systems that do not have the native technical capabilities, compensating security measures can be part of the policies and procedures specified in this document.

This document also recognizes that not all requirements specified in this document apply to all IACSs. For example, requirements associated with certain technology (such as wireless) or functions (such as remote access) will not apply to IACSs that do not include these technologies or functions. Similarly, not all malware protection requirements apply to systems for which malware protection software is not available for any of their devices. Therefore, this document states that the asset owner needs to identify the IACS security requirements that are applicable to its IACSs in their specific operating environments.

The elements of an IACS SP described in this document define required security capabilities that apply to the secure operation of an IACS. Although the asset owner is ultimately accountable for the secure operation of an IACS, implementation of these security capabilities often includes support from its service providers and product suppliers. For this reason, this document provides guidance for an asset owner when stating security requirements for their service providers and product suppliers, referencing other parts of the IEC 62443 series.

Figure 1 illustrates the roles and responsibilities of the asset owner, service provider(s) and product supplier(s) of an IACS and their relationships to each other and to the Automation Solution. The Automation Solution is a technical solution implementing the control/safety and complementary functions necessary for the IACS. It is composed of hardware and software components that have been installed and configured to operate in the IACS. The IACS is a combination of the Automation Solution and the organizational measures necessary for its design, deployment, operation and maintenance.

Some of these capabilities rely on the appropriate application of integration maintenance capabilities defined in IEC 62443-2-4 [2] and technical security capabilities defined in IEC 62443-3-3 [3] and IEC 62443-4-2 [4].

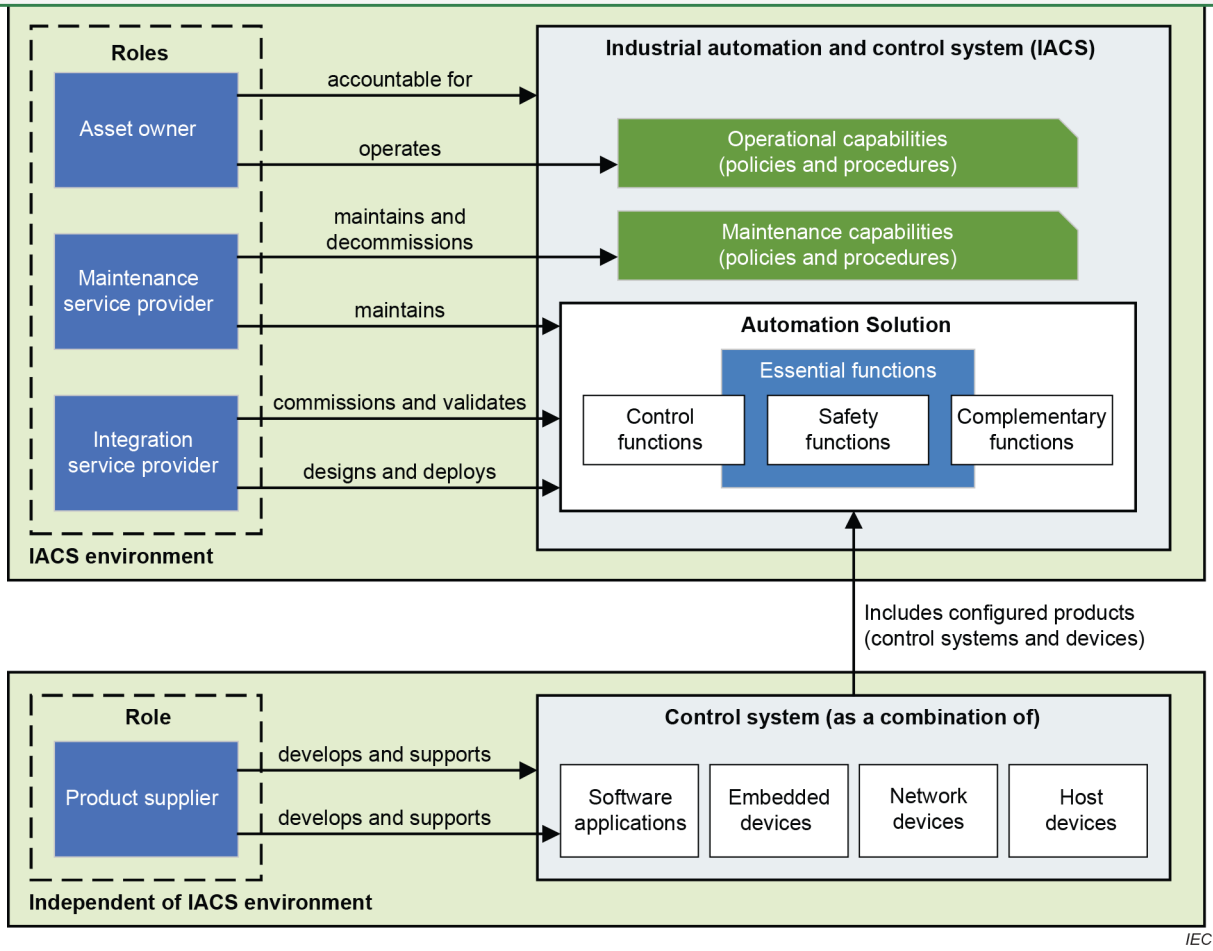

Figure 1 – Roles and responsibilities in the IEC 62443 series

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 62443-1-1:2009, *Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models*

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

SÉCURITÉ DES SYSTÈMES D'AUTOMATISATION ET DE COMMANDE INDUSTRIELLES –

Partie 2-1: Exigences de programme de sécurité pour les propriétaires d'actif IACS

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 du présent document de l'IEC peuvent faire l'objet de droits de brevets. L'IEC ne prend pas position quant à la preuve, à la validité et à la portée de ces droits de propriété. À la date de publication du présent document, l'IEC n'a reçu aucune déclaration relative à des droits de brevets, qui pourraient être exigés pour la mise en œuvre du présent document. Toutefois, il est rappelé aux responsables de cette mise en œuvre qu'il ne s'agit peut-être pas des informations les plus récentes, qui peuvent être obtenues dans la base de données disponible à l'adresse https://patents.iec.ch. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets.

L'IEC 62443-2-1 a été établie par le comité d'études 65 de l'IEC: Mesure, commande et automation dans les processus industriels, en collaboration avec le comité de liaison ISA99: Comité ISA pour la sécurité des systèmes d'automatisation et de commande industrielles. Il s'agit d'une Norme internationale.

Cette deuxième édition annule et remplace la première édition parue en 2010. Cette édition constitue une révision technique.

Cette édition inclut les modifications techniques majeures suivantes par rapport à l'édition précédente:

a) la structure des exigences a été révisée en éléments SP (SPE – SP element);
b) les exigences ont été révisées pour éliminer la répétition d'un système de management de la sécurité de l'information (SMSI); et
c) un modèle de stabilisation a été défini pour l'évaluation des exigences.

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

Projet	Rapport de vote
65/1044/FDIS	65/1053/RVD

Le rapport de vote indiqué dans le tableau ci-dessus donne toute information sur le vote ayant abouti à son approbation.

La langue employée pour l'élaboration de cette Norme internationale est l'anglais.

Le présent document a été rédigé selon les Directives ISO/IEC, Partie 2, il a été développé selon les Directives ISO/IEC, Partie 1 et les Directives ISO/IEC, Supplément IEC, disponibles sous www.iec.ch/members_experts/refdocs. Les principaux types de documents développés par l'IEC sont décrits plus en détail sous www.iec.ch/publications.

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*, se trouve sur le site web de l'IEC.

Les futures normes de cette série porteront le nouveau titre général cité ci-dessus. Le titre des normes qui existent déjà dans cette série sera mis à jour lors de leur 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 webstore.iec.ch dans les données relatives au document recherché. À cette date, le document sera

- reconduit,
- supprimé, ou
- révisé.

IMPORTANT – Le logo "colour inside" qui se trouve sur la page de couverture de ce document 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 est la partie de la série IEC 62443 qui contient les exigences de sécurité pour les propriétaires d'actif des systèmes d'automatisation et de commande industrielles (IACS – industrial automation and control system). Dans le contexte du présent document, le propriétaire d'actif inclut également l'opérateur de l'IACS. Ses exigences portent sur la cybersécurité et permettent aux capacités de sécurité qui les satisfont d'être fournies combinées à la fois avec des mesures de sécurité techniques, physiques, procédurales et compensatoires.

La cybersécurité est un sujet dont l'importance ne cesse de prendre de l'ampleur dans les organisations modernes. Le terme cybersécurité est généralement utilisé pour décrire l'ensemble des mesures de sécurité ou pratiques adoptées pour protéger un ordinateur ou un système informatique contre un accès non autorisé ou une attaque. Dans l'IACS, les problèmes principaux résident dans le fait qu'un accès indésirable ou des attaques peuvent empêcher la bonne exécution des fonctions l'IACS dans les délais exigés.

En général, lorsqu'un problème difficile se pose, l'approche technique consiste à subdiviser le problème en parties plus petites et à traiter méthodiquement chacune de ces parties. Cette approche est valable pour traiter les risques liés à la cybersécurité des IACS. Cependant, l'erreur fréquemment commise consiste à traiter le problème de cybersécurité d'un système à la fois. La cybersécurité est un défi beaucoup plus vaste pour lequel il convient de prendre en considération l'ensemble des composants IACS ainsi que les politiques, les procédures, les pratiques qui encadrent ces IACS et le personnel qui les utilise. La mise en œuvre d'un système de gestion d'une telle ampleur peut exiger une évolution culturelle de l'organisation.

Traiter le problème de cybersécurité au niveau d'une organisation complète peut sembler une tâche impossible. Il n'existe pas de livre de recettes simples pour la sécurité ni de "modèle à taille unique" pour les pratiques de sécurité. La sécurité absolue peut être atteinte, mais cela n'est pas souhaitable, car atteindre cet état de quasi-perfection se ferait au prix d'une certaine perte de fonctionnalité. La sécurité est un équilibre entre les risques et les coûts.

Aucune situation ne ressemble à une autre. Dans certaines situations, le risque peut être lié aux facteurs de santé, de sécurité et d'environnement (HSE – health, safety and environmental) plutôt qu'à un impact purement économique. Le risque peut être une conséquence irréversible plutôt qu'un contretemps financier temporaire. Par conséquent, un ensemble prédéfini de pratiques de sécurité obligatoires peut être soit trop restrictif et sans doute très coûteux à mettre en œuvre, soit insuffisant pour prendre en considération le risque.

Le présent document prend en charge le besoin de prise en considération de la cybersécurité d'un IACS opérationnel en spécifiant des exigences pour l'établissement, la mise en œuvre, la maintenance et l'amélioration continue du programme de sécurité (SP – security program) d'un IACS (SP IACS). La mise en œuvre consciencieuse de ces exigences offre des capacités de sécurité destinées à ramener les risques de sécurité pour l'IACS à un niveau tolérable. Ces exigences sont définies de manière à être indépendantes d'une mise en œuvre, ce qui permet aux propriétaires d'actif de choisir les approches les mieux adaptées à leurs besoins. L'IEC 62443-3-2 [1] [1] décrit la méthodologie qui permet de traiter les risques de cybersécurité lors de la conception d'un IACS, d'identifier les risques et de choisir des exigences de sécurité et des capacités associées appropriées pour un SP IACS.

Ces technologies disponibles dans le commerce (COTS – commercial-off-the-shelf) ne sont généralement pas assez renforcées ou assez rigoureusement conçues pour les environnements IACS dans lesquels elles peuvent introduire des vulnérabilités et des menaces supplémentaires pour l'IACS.

---

1 Les chiffres entre crochets renvoient à la Bibliographie.

Lorsque les technologies COTS sont utilisées dans un IACS, elles sont souvent configurées de manière à satisfaire aux besoins fonctionnels et aux contraintes opérationnelles spécifiques de ce système. Par exemple, la gestion des événements de sécurité dans les produits COTS peut être configurée différemment pour les applications IACS et pour les applications de technologie de l'information (TI) classiques. Les équipements COTS types sont conçus pour des environnements dont l'objectif principal est la protection de l'information. Les objectifs principaux d'un IACS sont la préservation de la santé, de la sécurité et de l'environnement dans l'installation, ainsi que la réduction le plus possible de l'impact opérationnel et professionnel sur le fonctionnement de l'installation. Les technologies COTS peuvent être utilisées dans les applications IACS, mais il est nécessaire que le propriétaire d'actif comprenne les risques associés à leur utilisation.

Les organisations peuvent essayer d'utiliser les solutions existantes de cybersécurité TI et professionnelles pour résoudre la sécurité des IACS, sans comprendre les conséquences. Nombre de ces solutions peuvent être appliquées aux équipements IACS, mais il est important qu'elles le soient de façon correcte pour éviter toute conséquence désastreuse et indésirable. Par exemple, dans un IACS, la disponibilité peut avoir une priorité plus élevée que la confidentialité, contrairement aux applications TI classiques.

Les propriétaires d'actifs peuvent souhaiter appliquer leur SP IACS dans l'ensemble de l'organisation pour satisfaire aux besoins, aux objectifs, aux exigences de sécurité, aux processus d'activité et aux processus de travail de l'organisation, ainsi qu'à sa taille et à sa structure. Tous ces facteurs d'influence sont dynamiques et varient probablement avec le temps. L'adoption d'un SP IACS est donc une décision stratégique pour l'organisation.

L'efficacité d'un SP IACS est souvent améliorée par la coordination ou l'intégration avec les processus de l'organisation et avec l'ensemble du système de management de la sécurité de l'information (SMSI). Par exemple, la fonction de sécurité peut être ajoutée aux processus de la chaîne logistique de l'organisation afin d'exiger une telle fonction dans la conception des processus, des systèmes et des commandes. Il est également prévu que le SP IACS soit dimensionné par rapport aux besoins de l'IACS et de l'organisation.

SÉCURITÉ DES SYSTÈMES D'AUTOMATISATION ET DE COMMANDE INDUSTRIELLES –

Partie 2-1: Exigences de programme de sécurité pour les propriétaires d'actif IACS

1 Domaine d'application

La présente partie de l'IEC 62443 spécifie les exigences de politiques et de procédures du programme de sécurité (SP) du propriétaire d'actif pour un système d'automatisation et de commande industrielle (IACS) opérationnel. Le présent document utilise, au sens large, la définition et le domaine d'application de ce qui constitue un IACS décrit dans l'IEC TS 62443-1-1. Dans le contexte du présent document, le propriétaire d'actif inclut également l'opérateur de l'IACS.

Le présent document reconnaît que la durée de vie d'un IACS peut dépasser vingt ans et que de nombreux systèmes patrimoniaux contiennent du matériel et du logiciel qui ne sont plus pris en charge. Par conséquent, le SP de la plupart des systèmes patrimoniaux ne concerne qu'un sous-ensemble des exigences définies dans le présent document. Les exigences en matière de correctifs de sécurité, par exemple, ne peuvent pas être satisfaites si l'IACS ou le logiciel composant n'est plus pris en charge. De même, le logiciel de sauvegarde de la plupart des systèmes plus anciens n'est pas disponible pour tous les composants de l'IACS. Le présent document ne précise pas qu'un IACS doit satisfaire à ces exigences techniques. Il indique qu'il est nécessaire que le propriétaire d'actif dispose de politiques et de procédures relatives à ces types d'exigences. Dans le cas où le propriétaire d'actif possède des systèmes patrimoniaux qui ne comportent pas des capacités techniques natives, des mesures de sécurité compensatoires peuvent faire partie des politiques et procédures spécifiées dans le présent document.

Le présent document reconnaît également que toutes les exigences spécifiées dans le présent document ne s'appliquent pas à tous les IACS. Par exemple, les exigences associées à certaines technologies (telles la technologie sans-fil) ou fonctions (comme l'accès distant) ne s'appliquent pas aux IACS qui ne comportent pas ces technologies ou fonctions. De même, les exigences en matière de protection contre les programmes malveillants ne sont pas toutes applicables lorsqu'aucun appareil des systèmes n'est équipé de logiciels anti-programme malveillant. Par conséquent, le présent document indique qu'il est nécessaire que le propriétaire d'actif identifie les exigences de sécurité IACS applicables à ses IACS dans leurs environnements d'exploitation spécifiques.

Les éléments d'un SP IACS décrits dans le présent document définissent des exigences en matière de capacités de sécurité qui s'appliquent au fonctionnement sécurisé d'un IACS. Bien que le fonctionnement sécurisé d'un IACS relève en définitive de la responsabilité du propriétaire d'actif, la mise en œuvre des capacités de sécurité intègre souvent les contributions de ses fournisseurs de service et fournisseurs de produit. Pour cette raison, le présent document donne des recommandations aux propriétaires d'actif en spécifiant des exigences de sécurité pour leurs fournisseurs de service et fournisseurs de produit, et en faisant référence à d'autres parties de l'IEC 62443 (toutes les parties).

La Figure 1 représente les rôles et responsabilités de sécurité du propriétaire d'actif, du ou des fournisseurs de service et du ou des fournisseurs de produit d'un IACS, et les relations qu'ils entretiennent entre eux et avec la Solution d'Automatisation. La Solution d'Automatisation est une solution technique qui met en œuvre les fonctions de contrôle/sécurité et les fonctions complémentaires nécessaires à l'IACS. Elle est constituée de composants matériels et logiciels qui ont été installés et configurés pour fonctionner dans l'IACS. L'IACS est une combinaison de la Solution d'Automatisation et des mesures organisationnelles nécessaires à sa conception, son déploiement, son exploitation et à sa maintenance.

Certaines de ces capacités reposent sur l'application appropriée des capacités de maintenance et d'intégration définies dans l'IEC 62443-2-4 [2] et des capacités de sécurité techniques définies dans les normes IEC 62443-3-3 [3] et IEC 62443-4-2 [4].

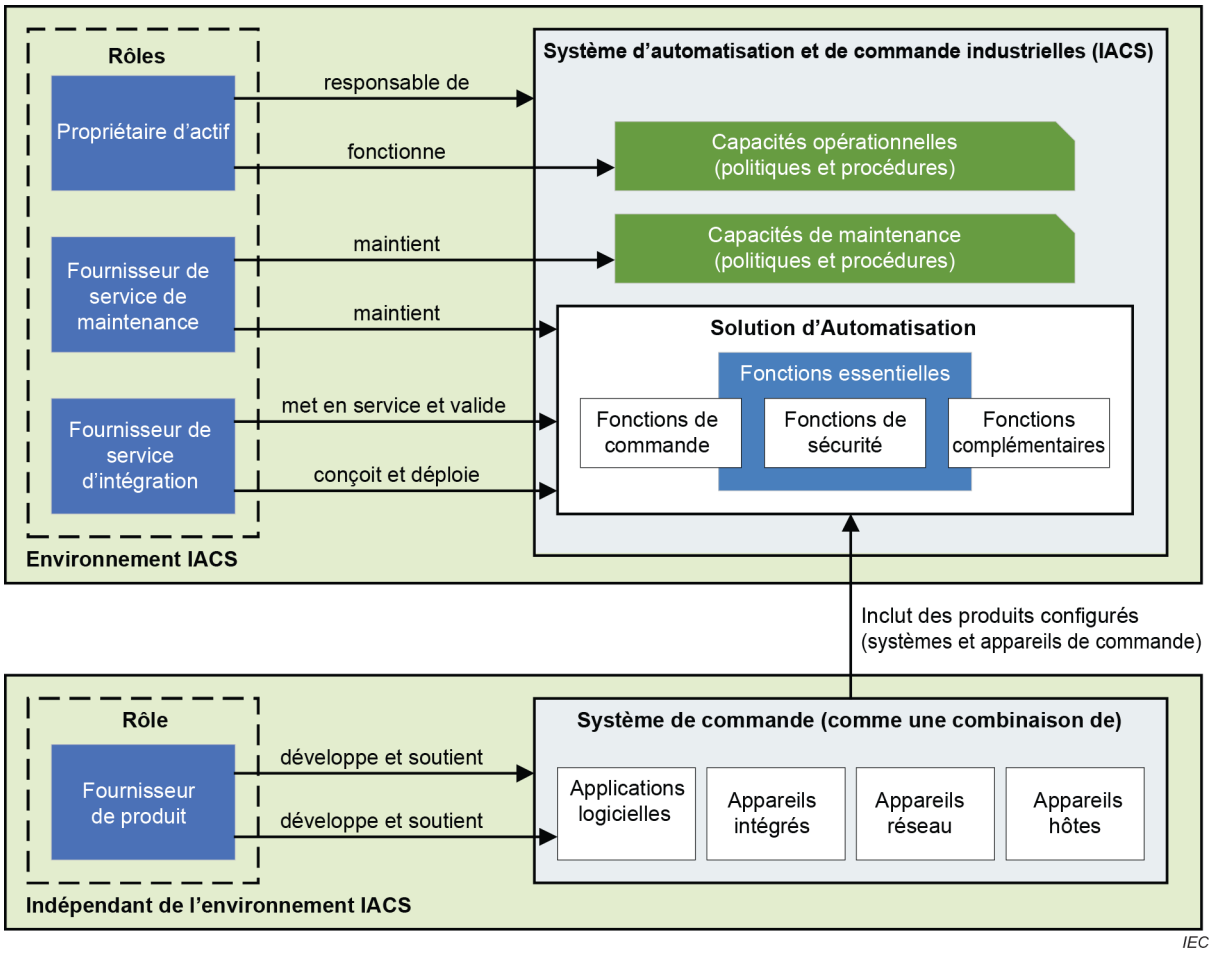

Figure 1 – Rôles et responsabilités dans la série IEC 62443

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