IEC 62443-2-1

Edition 1.0 2010-11

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

PRICE CODE XG
CODE PRIX

ICS 25.040.40; 33.040

ISBN 978-2-88912-037-6

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

INDUSTRIAL COMMUNICATION NETWORKS – NETWORK AND SYSTEM SECURITY –

Part 2-1: Establishing an industrial automation and control system security program

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 62443-2-1 has been prepared by IEC technical committee 65: Industrial-process measurement, control and automation.

This bilingual version (2012-04) corresponds to the monolingual English version, published in 2010-11.

The text of this standard is based on the following documents:

FDIS	Report on voting
65/457/FDIS	65/461/RVD

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

The French version of this standard has not been voted upon.

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

A list of all existing parts of IEC 62443 series, published under the general title *Industrial communication networks – Network and system security*, can be found on the IEC website. The full list of existing and intended parts can also be found in the Bibliography of this standard.

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

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- withdrawn,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

NOTE The revision of this international standard will be initiated shortly after this standard is published. The next revision will be aligned more closely with ISO/IEC 27001, which addresses many of the same issues but without consideration of the specialized requirements for continuous operation and safety that are common in the industrial automation and control systems environment.

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.

0 INTRODUCTION

0.1 Overview

Cyber security is an increasingly important topic in modern organizations. Many organizations involved in information technology (IT) and business have been concerned with cyber security for many years and have well-established cyber security management systems (CSMS) in place as defined by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) (see ISO/IEC 17799 [23][1] and ISO/IEC 27001 [24]). These management systems provide an organization with a well-established method for protecting its assets from cyber attacks.

Industrial automation and control system (IACS) organizations have begun using commercial off the shelf (COTS) technology developed for business systems in their everyday processes, which has provided an increased opportunity for cyber attack against the IACS equipment. These systems are not usually as robust, in the IACS environment, as are systems designed specifically as IACS at dealing with cyber attack for many reasons. This weakness may lead to health, safety and environmental (HSE) consequences.

Organizations may try to use the pre-existing IT and business cyber security solutions to address security for IACS without understanding the consequences. While many of these solutions can be applied to IACS, they need to be applied in the correct way to eliminate inadvertent consequences.

0.2 A cyber security management system for IACS

Management systems typically provide guidance on what should be included in a management system, but do not provide guidance on how to go about developing the management system. This standard addresses the aspects of the elements included in a CSMS for IACS and also provides guidance on how to go about developing the CSMS for IACS.

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 cyber security risks with IACS. However, a frequent mistake made in addressing cyber security is to deal with cyber security one system at a time. Cyber security is a much larger challenge that needs to address the entire set of IACS as well as the policies, procedures, practices and personnel that surround and utilize those IACS. Implementing such a wide-ranging management system may require a cultural change within the organization.

Addressing cyber security on an organization-wide basis can seem like a daunting task. Unfortunately there is no simple cookbook for security. There is good reason for this. There is not a one-size-fits-all set of security practices. Absolute security may be achievable, but is probably undesirable because of the loss of functionality that would be necessary to achieve this near perfect state. Security is really a balance of risk versus cost. All situations will be different. In some situations the risk may be related to HSE factors rather than purely economic impact. The risk may have an unrecoverable consequence rather than a temporary financial setback. Therefore a cookbook set of mandatory security practices will either be overly restrictive and likely quite costly to follow, or be insufficient to address the risk.

0.3 Relationship between this standard and ISO/IEC 17799 and ISO/IEC 27001

ISO/IEC 17799 [23] and ISO/IEC 27001 [24] are excellent standards that describe a cyber security management system for business/information technology systems. Much of the content in these standards is applicable to IACS as well. This standard emphasizes the need

---

1 Numbers in square brackets refer to the Bibliography.

for consistency between the practices to manage IACS cyber security with the practices to manage business/information technology systems cyber security. Economies will be realized by making these programs consistent. Users of this standard are encouraged to read ISO/IEC 17799 and ISO/IEC 27001 for additional supporting information. This standard builds on the guidance in these ISO/IEC standards. It addresses some of the important differences between IACS and general business/information technology systems. It introduces the important concept that cyber security risks with IACS may have HSE implications and should be integrated with other existing risk management practices addressing these risks.

INDUSTRIAL COMMUNICATION NETWORKS – NETWORK AND SYSTEM SECURITY –

Part 2-1: Establishing an industrial automation and control system security program

1 Scope

This part of IEC 62443 defines the elements necessary to establish a cyber security management system (CSMS) for industrial automation and control systems (IACS) and provides guidance on how to develop those elements. This standard uses the broad definition and scope of what constitutes an IACS described in IEC/TS 62443-1-1.

The elements of a CSMS described in this standard are mostly policy, procedure, practice and personnel related, describing what shall or should be included in the final CSMS for the organization.

NOTE 1 Other documents in the IEC 62443 series and in the Bibliography discuss specific technologies and/or solutions for cyber security in more detail.

The guidance provided on how to develop a CSMS is an example. It represents the author's opinion on how an organization could go about developing the elements and may not work in all situations. The users of this standard will have to read the requirements carefully and apply the guidance appropriately in order to develop a fully functioning CSMS for an organization. The policies and procedures discussed in this standard should be tailored to fit within the organization.

NOTE 2 There may be cases where a pre-existing CSMS is in place and the IACS portion is being added or there may be some organizations that have never formally created a CSMS at all. The authors of this standard cannot anticipate all cases where an organization will be establishing a CSMS for the IACS environment, so this standard does not attempt to create a solution for all cases.

2 Normative references

The following referenced documents are indispensable for the application 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[2] – *Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models*

[2] This standard is derived from ANSI/ISA 99.02.01:2009 and wholly replaces it for international use. It is intended that the second edition of IEC/TS 62443-1-1 be an International Standard, not a TS, after inclusion of some normative requirements to which conformance is possible.

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

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

Partie 2-1: Etablissement d'un programme de sécurité pour les systèmes d'automatisation et de commande industrielles

AVANT-PROPOS

1) La Commission Electrotechnique Internationale (CEI) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de la CEI). La CEI a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. A cet effet, la CEI – 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 la CEI"). 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 la CEI, participent également aux travaux. La CEI 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 la CEI concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de la CEI intéressés sont représentés dans chaque comité d'études.
3) Les Publications de la CEI se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de la CEI. Tous les efforts raisonnables sont entrepris afin que la CEI s'assure de l'exactitude du contenu technique de ses publications; la CEI 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 la CEI s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de la CEI dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de la CEI et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) La CEI 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 la CEI. La CEI 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 la CEI, 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 la CEI, 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 la CEI ou de toute autre Publication de la CEI, 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 la CEI peuvent faire l'objet de droits de brevet. La CEI 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 CEI 62443-2-1 a été établie par le comité d'études 65 de la CEI: Mesure, commande et automatisation dans les processus industriels.

La présente version bilingue (2012-04) correspond à la version anglaise monolingue publiée en 2010-11.

Le texte anglais de cette norme est issu des documents 65/457/FDIS et 65/461/RVD.

Le rapport de vote 65/461/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/CEI, Partie 2.

Une liste de toutes les parties existantes de la série de normes CEI 62443, publiée sous le titre générique *Réseaux industriels de communication – Sécurité dans les réseaux et les systèmes*, est disponible sur le site internet de la CEI. La liste complète des parties existantes et prévues est également disponible dans la Bibliographie de cette norme.

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 la CEI sous "http://webstore.iec.ch" dans les données relatives à la publication recherchée. A cette date, la publication sera

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

NOTE La révision de la présente norme internationale commencera peu après sa publication. La prochaine révision sera alignée plus étroitement sur l'ISO/CEI 27001, qui aborde de nombreux problèmes identiques, mais sans prendre en compte les exigences spécialisées concernant la poursuite du fonctionnement et la sécurité, courantes dans l'environnement des automatismes industriels et des systèmes de commande.

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.

0 INTRODUCTION

0.1 Vue d'ensemble

La cyber-sécurité est un sujet dont l'importance ne cesse de prendre de l'ampleur dans les organisations modernes. De nombreuses organisations concernées par le traitement de l'information (IT) se soucient de la cyber-sécurité depuis de nombreuses années et ont mis en place des systèmes de gestion de cyber-sécurité (CSMS) reconnus, tels que ceux définis par l'Organisation internationale de normalisation (ISO) et la Commission électrotechnique internationale (CEI) (voir ISO/CEI 17799 [23][1] et ISO/CEI 27001 [24]). Ces systèmes de gestion fournissent aux organisations une méthode bien établie pour protéger leurs actifs des cyber-attaques.

Les organisations utilisant des systèmes d'automatisation et de commande industrielle (IACS) ont commencé à utiliser la technologie disponible dans le commerce (COTS) développée pour les systèmes professionnels dans leurs procédés journaliers, ce qui a occasionné une multiplication des cyber-attaques contre les systèmes IACS. Ces systèmes ne sont généralement pas aussi robustes, dans l'environnement IACS, que le sont les systèmes spécifiquement conçus pour traiter les cyber-attaques, et ce pour de nombreuses raisons. Cette faiblesse peut avoir des conséquences sur la santé, la sécurité et l'environnement (HSE).

Les organisations peuvent essayer d'utiliser les solutions existantes de cyber-sécurité informatiques et professionnelles pour résoudre la sécurité des IACS, sans comprendre les conséquences. Nombre de ces solutions peuvent être appliquées aux équipements IACS, mais elles doivent l'être de façon correcte pour éviter toute conséquence désastreuse.

0.2 Un système de gestion de la cyber-sécurité pour les équipements IACS

Les systèmes de gestion fournissent habituellement des indications sur ce qu'un système de gestion doit inclure, mais n'indique pas la façon dont le système de gestion doit être développé. La présente norme traite des aspects concernant les éléments inclus dans un CSMS d'IACS et fournit des indications sur la façon de développer le CSMS pour l'IACS.

En général, lorsque l'on se trouve confronté à un problème difficile, 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 aborder les risques liés à la cyber-sécurité des IACS. Cependant, l'erreur fréquemment commise pour aborder les risques liés à la cyber-sécurité consiste à traiter la cyber-sécurité d'un système à la fois. La cyber-sécurité est un défi beaucoup plus vaste qui oblige à prendre en compte l'ensemble complet des 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 nécessite une évolution culturelle de l'organisation.

Traiter la cyber-sécurité au niveau d'une organisation complète peut sembler une tâche impossible. Malheureusement, il n'existe pas de livre de recettes simples pour la sécurité. Il y a une excellente raison à cela. Il n'y a pas 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, en réalité, est un équilibre entre les risques et les coûts. Aucune situation ne ressemble à une autre. Dans certains cas, le risque peut être lié aux facteurs HSE plutôt qu'à un impact purement économique. Le risque peut être une conséquence irréversible plutôt qu'un contretemps financier temporaire. Par conséquent, un recueil de recettes donnant les pratiques de sécurité obligatoires serait soit trop restrictif et sans doute très coûteux à suivre, soit insuffisant pour prendre en compte le risque.

---

[1] Les nombres entre crochets font référence à la Bibliographie.

0.3 Relations entre la présente norme et l'ISO/CEI 17799 et l'ISO/CEI 27001

Les normes ISO/CEI 17799 [23] et ISO/CEI 27001 [24] sont d'excellentes normes décrivant un système de gestion de cyber-sécurité pour des systèmes professionnels de traitement de l'information. Une grande partie du contenu de ces normes est également valable pour les IACS. La présente norme met l'accent sur la nécessité d'une uniformité entre les pratiques de gestion de la cyber-sécurité des IACS et les pratiques de gestion de la cyber-sécurité des systèmes professionnels de traitement de l'information. L'uniformisation de ces programmes permettra de réaliser des économies. Les utilisateurs de la présente norme sont invités à consulter les normes ISO/CEI 17799 et ISO/CEI 27001 pour toute information de support complémentaire. La présente norme se fonde sur les indications fournies par ces normes ISO/CEI. Elle aborde certaines différences importantes entre les IACS et les systèmes professionnels généraux de traitement de l'information. Elle sensibilise le lecteur au concept essentiel selon lequel les risques liés à la cyber-sécurité des IACS peuvent avoir des implications HSE et il convient pour traiter ces risques de l'intégrer aux pratiques existantes de gestion des risques.

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

Partie 2-1: Etablissement d'un programme de sécurité pour les systèmes d'automatisation et de commande industrielles

1 Domaine d'application

La présente partie de la CEI 62443 définit les éléments nécessaires à l'établissement d'un système de gestion de la cyber-sécurité (CSMS) pour les systèmes d'automatisation et de commande (IACS) industriels et fournit des indications sur la façon de développer ces éléments. La présente norme utilise, au sens large, la définition et le domaine d'application de ce qui constitue un IACS décrit dans la CEI/TS 62443-1-1.

Les éléments d'un CSMS décrits dans la présente norme sont essentiellement liés aux politiques, aux procédures, aux pratiques et au personnel; ils correspondent à ce doit être inclus ou à ce qu'il convient d'inclure dans le CSMS final de l'organisation.

NOTE 1 D'autres documents de la série CEI 62443 et de la Bibliographie décrivent plus en détail des technologies et/ou des solutions spécifiques pour la cyber-sécurité.

Les indications fournies sur la façon de développer un CSMS le sont à titre d'exemple. Elles représentent l'opinion de l'auteur concernant la façon dont une organisation doit s'y prendre pour développer les éléments, et peuvent ne pas fonctionner dans toutes les situations. Les utilisateurs de la présente norme doivent lire attentivement les exigences et appliquer les indications de façon appropriée afin de développer un CSMS entièrement fonctionnel pour une organisation. Il convient que les politiques et les procédures décrites dans cette norme soient adaptées aux besoins de l'organisation.

NOTE 2 Il peut y avoir le cas où un CSMS est déjà en place et où l'on ajoute la partie IACS, comme le cas où l'organisation n'a jamais créé formellement de CSMS. Les auteurs de la présente norme ne peuvent pas prévoir tous les cas dans lesquels l'organisation établira un CSMS pour l'environnement des IACS, aussi la présente norme n'a-t-elle pas vocation de proposer une solution pour tous les cas.

2 Références normatives

Les documents de référence suivants sont indispensables pour l'application 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[2] – *Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts and models*

[2] Cette norme est issue de la norme ANSI/ISA 99.02.01:2009, qu'elle remplace entièrement pour l'utilisation internationale. Il est attendu que la deuxième édition de la CEI/TS 62443-1-1 soit une Norme internationale, non une TS, après inclusion de certaines exigences normatives auxquelles il est possible de se conformer.