IEC 62443-2-4

Edition 1.0 2015-06

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Security for industrial automation and control systems – Part 2-4: Security program requirements for IACS service providers

Sécurité des automatismes industriels et des systèmes de commande – Partie 2-4: Exigences de programme de sécurité pour les fournisseurs de service IACS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

ICS 25.040.40; 35.040; 35.100

ISBN 978-2-8322-2767-1

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –

Part 2-4: Security program requirements for IACS service providers

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 62443-2-4 has been prepared by IEC technical committee 65: Industrial-process measurement, control and automation.

This publication contains an attached file in the form of an Excel 97-2003 spreadsheet version of Table A.1. This file is intended to be used as a complement and does not form an integral part of the publication.

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

CDV	Report on voting
65/545/CDV	65/561A/RVC

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

This publication 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 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.

The contents of the corrigendum of August 2015 have been included in this copy.

IMPORTANT – The 'colour inside' logo on the cover page of this publication indicates that it contains colours which are considered to be useful for the correct understanding of its contents. Users should therefore print this document using a colour printer.

INTRODUCTION

This standard is the part of the IEC 62443 series that contains security requirements for providers of integration and maintenance services for Industrial Automation and Control Systems (IACS). It has been developed by IEC Technical Committee 65 in collaboration with the International Instrumentation Users Association, referred to as the WIB from its original and now obsolete Dutch name, and ISA 99 committee members.

Figure 1 illustrates the relationship of the different parts of IEC 62443 being developed. Those that are normatively referenced are included in the list of normative references in Clause 2, and those that are referenced for informational purposes or that are in development are listed in the Bibliography.

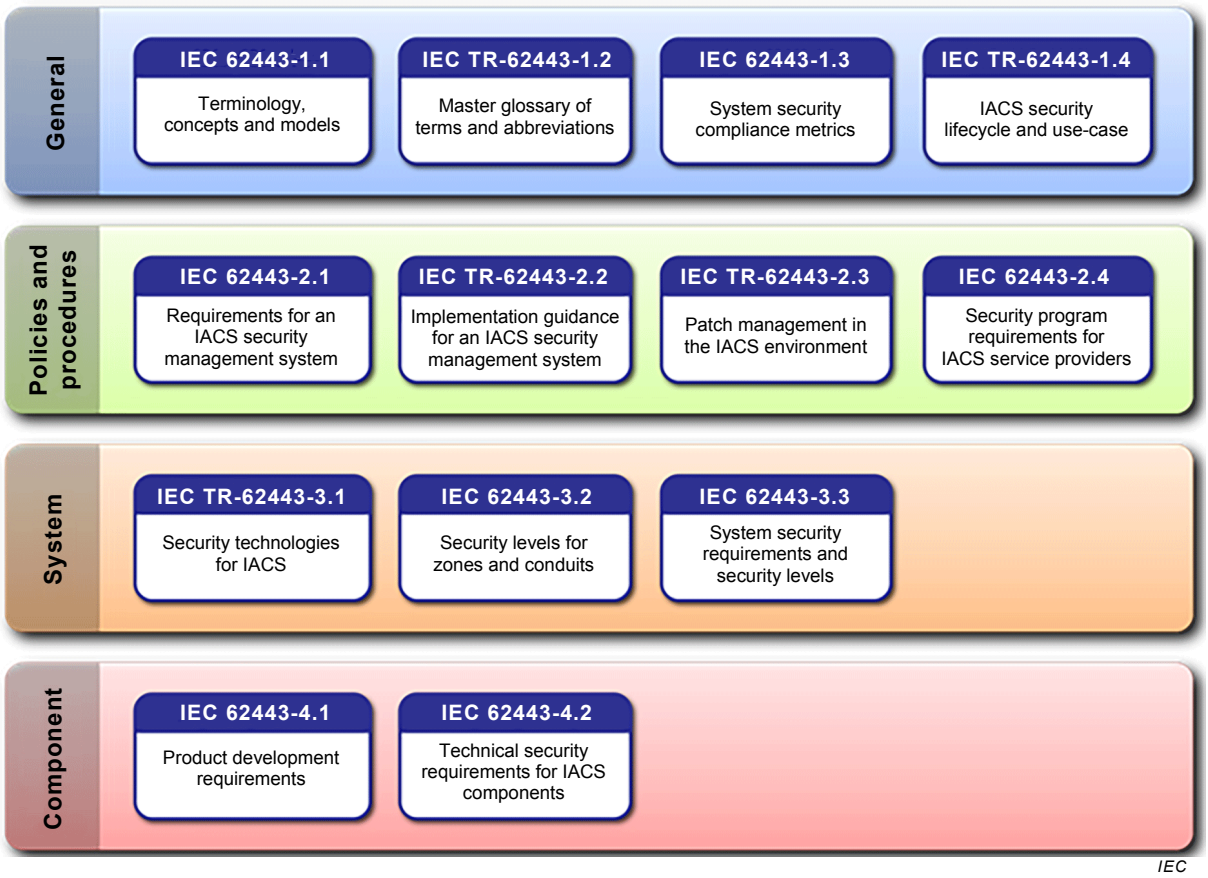

Figure 1 – Parts of the IEC 62443 Series

SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –

Part 2-4: Security program requirements for IACS service providers

1 Scope

This part of IEC 62443-2-4 specifies requirements for security capabilities for IACS service providers that they can offer to the asset owner during integration and maintenance activities of an Automation Solution.

NOTE 1 The term “Automation Solution” is used as a proper noun (and therefore capitalized) in this part of IEC 62443 to prevent confusion with other uses of this term.

Collectively, the security capabilities offered by an IACS service provider are referred to as its Security Program. In a related specification, IEC 62443-2-1 describes requirements for the Security Management System of the asset owner.

NOTE 2 In general, these security capabilities are policy, procedure, practice and personnel related.

Figure 2 illustrates how the integration and maintenance capabilities relate to the IACS and the control system product that is integrated into the Automation Solution. Some of these capabilities reference security measures defined in IEC 62443-3-3 that the service provider must ensure are supported in the Automation Solution (either included in the control system product or separately added to the Automation Solution).

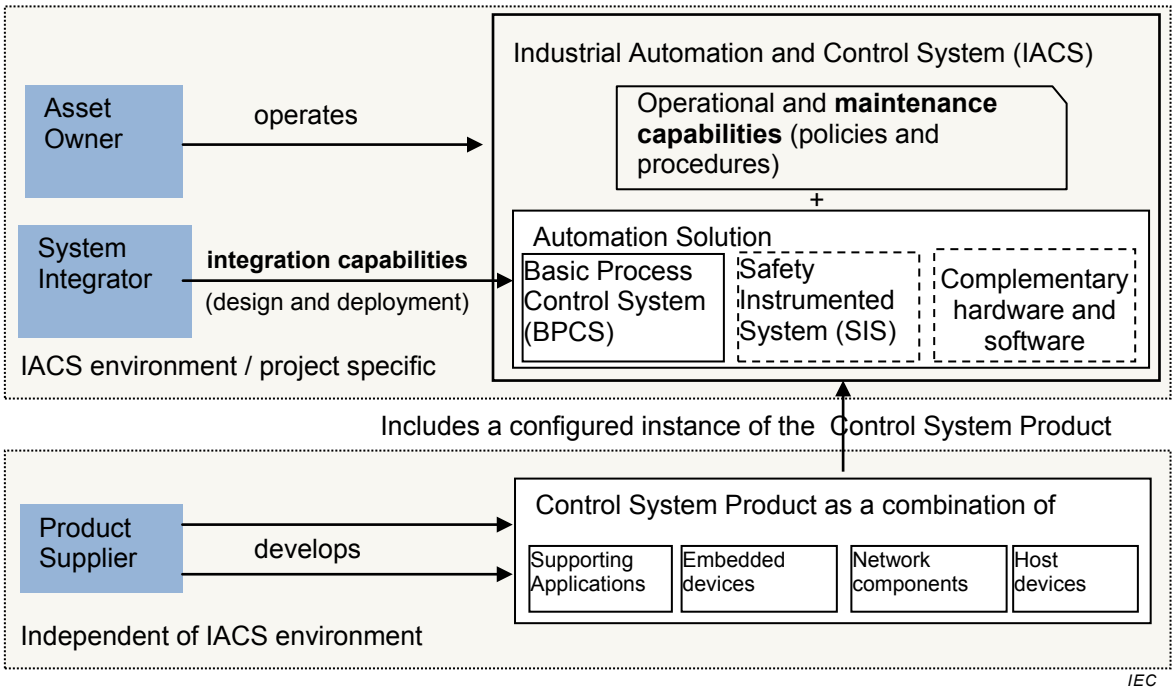

Figure 2 – Scope of service provider capabilities

In Figure 2, the Automation Solution is illustrated to contain a Basic Process Control System (BPCS), optional Safety Instrumented System (SIS), and optional supporting applications, such as advanced control. The dashed boxes indicate that these components are “optional”.

NOTE 3 The term “process” in BPCS may apply to a variety of industrial processes, including continuous processes and manufacturing processes.

NOTE 4 Clause 4.1.4 describes profiles and how they can be used by industry groups and other organizations to adapt this International Standard to their specific environments, including environments not based on an IACS.

NOTE 5 Automation Solutions typically have a single control system (product), but they are not restricted to do so. In general, the Automation Solution is the set of hardware and software, independent of product packaging, that is used to control a physical process (e.g. continuous or manufacturing) as defined by the asset owner.

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.

“None”

SOMMAIRE

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

SÉCURITÉ DES AUTOMATISMES INDUSTRIELS ET DES SYSTÈMES DE COMMANDE –

Partie 2-4: Exigences de programme de sécurité pour les fournisseurs de service 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. A 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 62443-2-4 a été établie par le comité d'études 65 de l'IEC: Mesure, commande et automation dans les processus industriels.

La présente publication contient un fichier joint sous la forme d'une feuille de calcul Excel version 97-2003. Ce fichier est destiné à être utilisé comme complément et ne fait pas partie intégrante de la publication.

Le texte de cette norme est issu des documents suivants:

CDV	Rapport de vote
65/545CDV	65/561A/RVC

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

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.

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 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. A cette date, la publication sera

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

Le contenu du corrigendum d'août 2015 a été pris en considération dans cet exemplaire.

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

La présente norme est la partie de la série IEC 62443 qui contient les exigences de sécurité pour les fournisseurs de service d'intégration et de maintenance pour les systèmes d'automatisation et de commande industrielles (IACS). Elle a été élaborée par la Comité d'études 65 de l'IEC en collaboration avec l'International Instrumentation Users Association (appelée WIB, qui est son nom d'origine et désormais obsolète en néerlandais) et les membres du comité ISA 99.

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

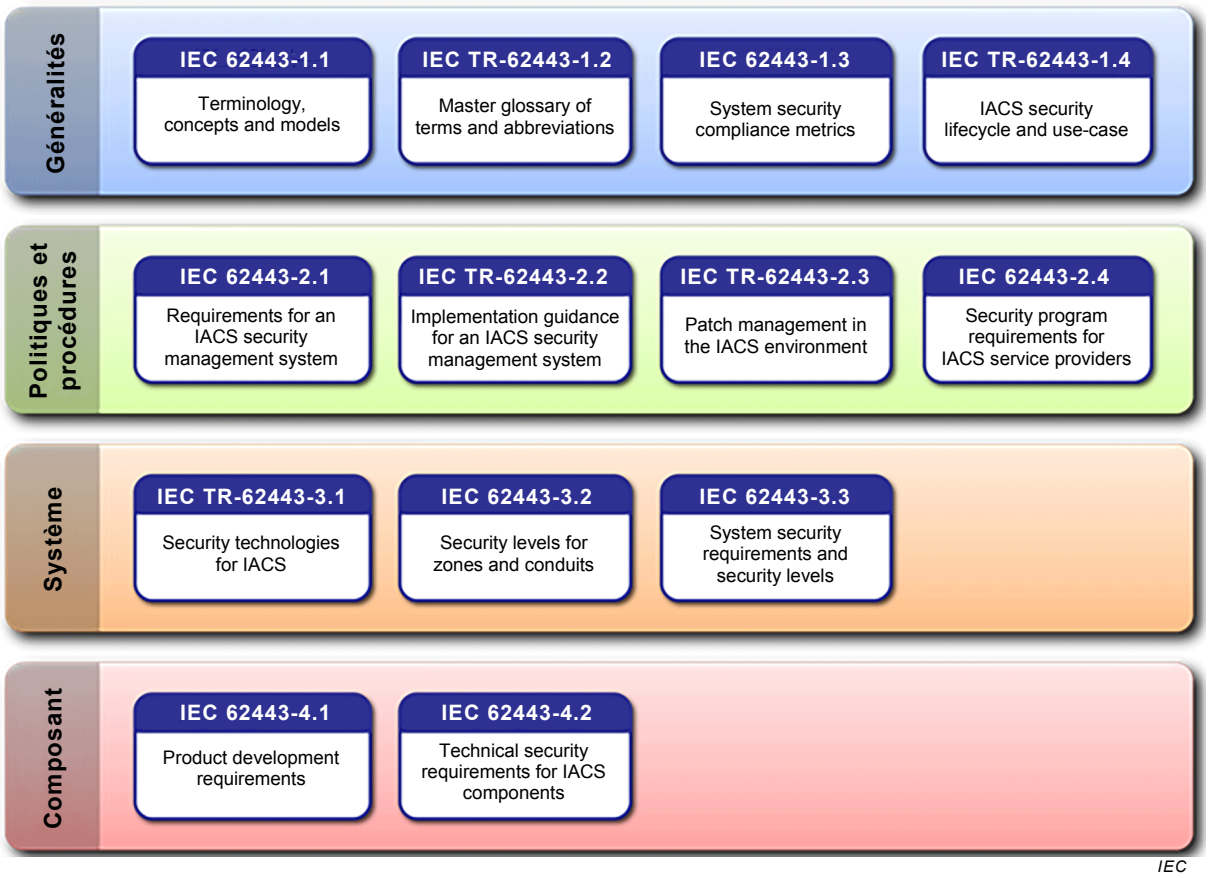

Figure 1 – Parties de la série IEC 62443

SÉCURITÉ DES AUTOMATISMES INDUSTRIELS ET DES SYSTÈMES DE COMMANDE –

Partie 2-4: Exigences de programme de sécurité pour les fournisseurs de service IACS

1 Domaine d'application

La présente partie de l'IEC 62443-2-4 spécifie les exigences de capacités de sécurité pour les fournisseurs de service IACS qu'ils peuvent proposer au propriétaire d'actif pendant les activités d'intégration et de maintenance d'une Solution d'Automatisation.

NOTE 1 Dans la présente partie de l'IEC 62443, le terme ''Solution d'Automatisation'' est utilisé comme un nom propre (et par conséquent écrit en majuscule) pour éviter toute confusion avec d'autres usages de ce terme.

De manière collective, les capacités de sécurité offertes par un fournisseur de service IACS sont appelées Programme de sécurité. Une spécification associée, l'IEC 62443-2-1 décrit les exigences pour le Système de gestion de sécurité du propriétaire d'actif.

NOTE 2 En général, ces capacités de sécurité sont liées à la politique, la procédure, la pratique et au personnel.

La Figure 2 représente la relation entre les capacités d'intégration et de maintenance et l'IACS ainsi que le produit de système de commande intégré à la Solution d'Automatisation. Certaines de ces mesures de sécurité de référence en matière de capacités définies dans l'IEC 62443-3-3 que le fournisseur de service doit assurer sont prises en charge dans la Solution d'Automatisation (soit incluses dans le produit de système de commande soit séparément ajoutées à la Solution d'Automatisation).

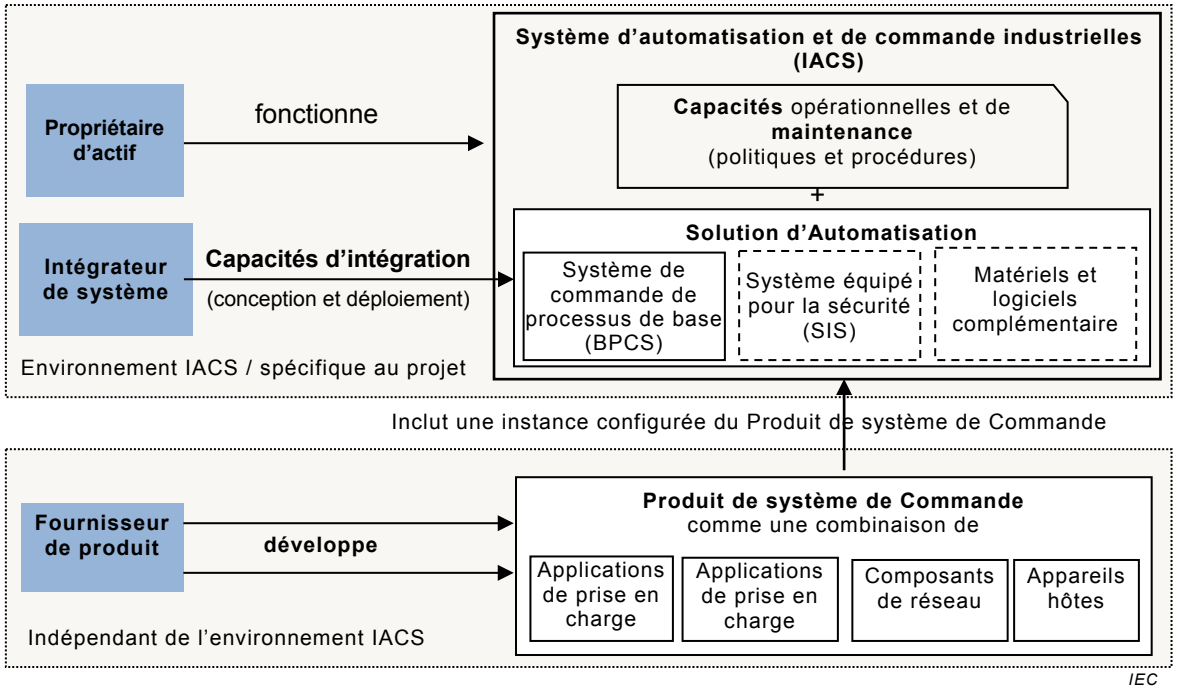

Figure 2 – Etendue des capacités du fournisseur de service

La Figure 2 représente la Solution d'Automatisation qui contient un Système de Commande de Processus de Base (BPCS), un Système Equipé pour la Sécurité (SIS) facultatif et des

Applications de Prise en Charge facultatives telles que la commande avancée. Les cases en pointillés indiquent que ces composants sont «facultatifs».

NOTE 3 Le terme «processus» dans BPCS peut s'appliquer à différents processus industriels, y compris les processus continus et les procédés de fabrication.

NOTE 4 L'Article 4.1.4 décrit les profils et la façon dont des groupes industriels et autres organisations peuvent les utiliser pour adapter la présente Norme internationale à leurs environnements spécifiques, y compris les environnements non fondés sur un IACS.

NOTE 5 En règle générale, les Solutions d'Automatisation disposent d'un seul système de commande (produit), sans toutefois s'y limiter. En général, la Solution d'Automatisation comprend l'ensemble des matériels et logiciels, indépendants de l'emballage du produit, qui est utilisé pour contrôler un processus physique (continu ou de fabrication, par exemple) tel que défini par le propriétaire d'actif.

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).

"Aucune référence normative"