IEC 62443-2-4

Edition 2.0 2023-12

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, 35.100.05

ISBN 978-2-8322-7779-9

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) 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.

This document has been prepared by of IEC technical committee 65: Industrial-process measurement, control and automation in collaboration with the liaison International Instrumentation Users Association, referred to as the WIB from its original and now obsolete Dutch name. It is an International Standard.

This publication contains an attached file in the form of a .CSV 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.

This second edition cancels and replaces the first edition published in 2015 and Amendment 1:2017. This edition constitutes a technical revision.

This edition contains editorial updates and clarifications and does not contain significant technical changes with respect to the previous edition. One area of clarification is that some of the requirements could have been interpreted as requirements for technical capabilities. These requirements were clarified so that they are expressed as requirements for the use/configuration of technical capabilities.

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

Draft	Report on voting
65/1021/FDIS	65/1029/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.

SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –

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

1 Scope

This part of IEC 62443 specifies a comprehensive set of requirements for security-related processes that IACS service providers can offer to the asset owner during integration and maintenance activities of an Automation Solution. Because not all requirements apply to all industry groups and organizations, Subclause 4.1.4 provides for the development of "profiles" that allow for the subsetting of these requirements. Profiles are used to adapt this document to specific environments, including environments not based on an IACS.

NOTE 1 The term "Automation Solution" is used as a proper noun (and therefore capitalized) in this document to prevent confusion with other uses of this term.

Collectively, the security processes offered by an IACS service provider are referred to as its Security Program (SP) for IACS asset owners. 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 1 illustrates the integration and maintenance security processes 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. Some of the requirements of this document relating to the safety program are associated with security requirements described in IEC 62443-3-3 and IEC 62443-4-2.

NOTE 3 The IACS is a combination of the Automation Solution and the organizational measures necessary for its design, deployment, operation, and maintenance.

NOTE 4 Maintenance of legacy system with insufficient security technical capabilities, implementation of policies, processes and procedures can be addressed through risk mitigation.

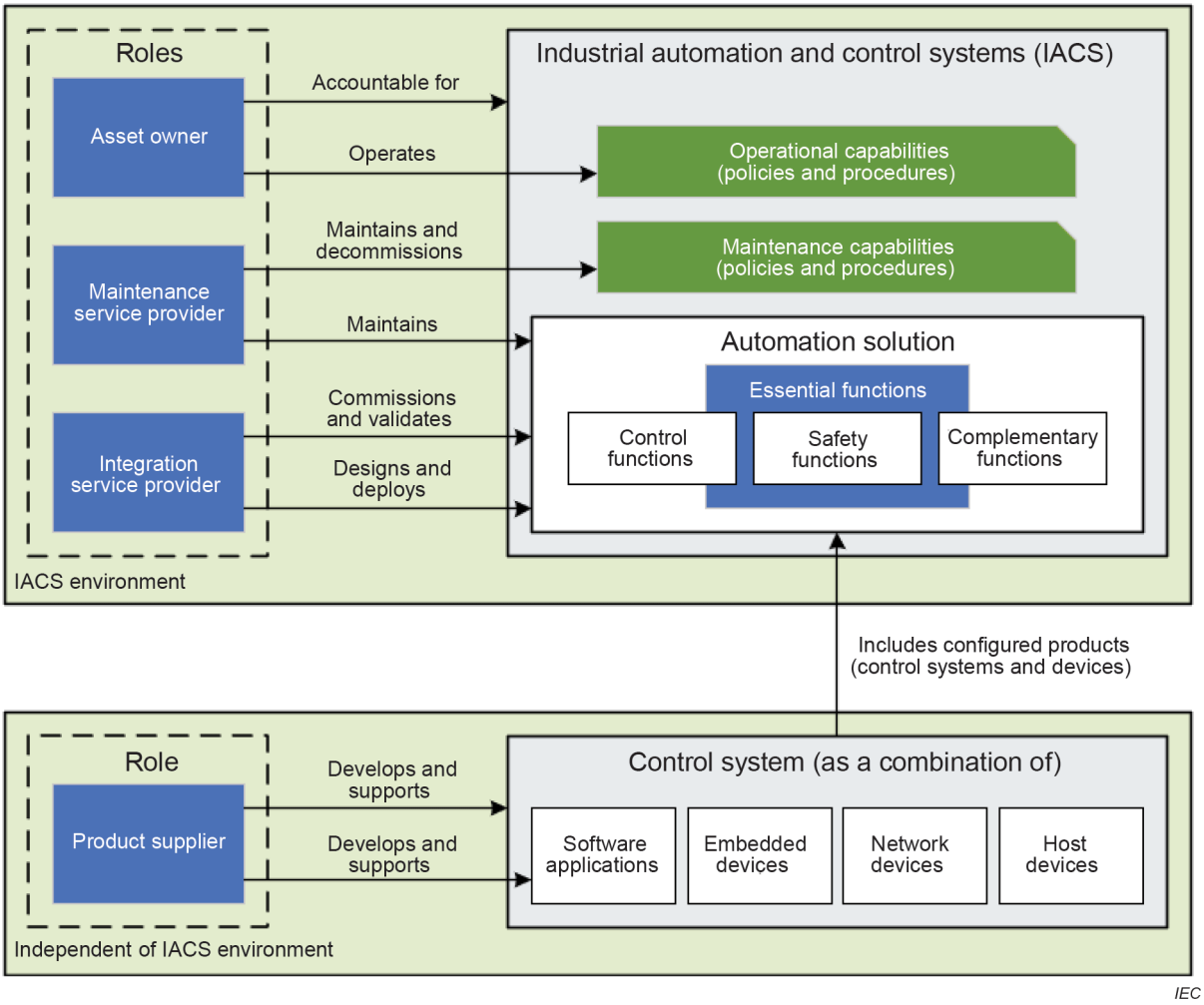

Figure 1 – Scope of service provider processes

In Figure 1, the Automation Solution is illustrated to contain essential functions that include safety functions, commonly implemented by a Safety Instrumented System (SIS), and complementary and control functions, commonly implemented by supporting applications, such as batch management, advanced control, historian, and security related applications. The dashed boxes identify organizational roles that perform the indicated actions.

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, which is used to control a physical process (e.g. continuous or manufacturing) as defined by the asset owner.

NOTE 6 Service providers often provide generic architectures that can be adapted for integration into an Automation Solution. These generic architectures are often referred to as "reference architectures".

2 Normative references

There are no normative references in this document.

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 services 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.

Le présent document a été établi par le comité d'études 65 de l'IEC: Mesure, commande et automation dans les processus industriels en collaboration avec l'organisme de liaison International Instrumentation Users Association, dénommé WIB en raison de son nom néerlandais d'origine et désormais obsolète. Il s'agit d'une Norme internationale.

La présente publication contient un fichier joint sous la forme d'une feuille de calcul CSV du Tableau A.1. Ce fichier est destiné à être utilisé comme complément et ne fait pas partie intégrante de la publication.

Cette seconde édition annule et remplace la première édition parue en 2015 et l'Amendement 1:2017. Cette édition constitue une révision technique.

La présente édition contient des mises à jour et des clarifications d'ordre rédactionnel et ne contient pas de modifications techniques significatives par rapport à l'édition précédente. Un point à clarifier concerne certaines des exigences susceptibles d'être interprétées comme des exigences relatives à des capacités techniques. Ces exigences ont été clarifiées et exprimées en tant qu'exigences relatives à l'utilisation/configuration des capacités techniques.

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

Projet	Rapport de vote
65/1021/FDIS	65/1029/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.

Ce 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 automatismes industriels et des systèmes de commande*, 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'il 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.

SÉCURITÉ DES AUTOMATISMES INDUSTRIELS ET DES SYSTÈMES DE COMMANDE –

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

1 Domaine d'application

La présente partie de l'IEC 62443 spécifie un ensemble exhaustif d'exigences pour les processus liés à la sécurité que les fournisseurs de services IACS peuvent proposer au propriétaire d'actif pendant les activités d'intégration et de maintenance d'une Solution d'Automatisation. Étant donné que toutes les exigences ne s'appliquent pas à tous les groupes et organismes industriels, le 4.1.4 prévoit le développement de Profils qui permettent la création de sous-ensembles de ces exigences. Les profils sont utilisés afin d'adapter le présent document aux environnements spécifiques, y compris les environnements qui ne reposent pas sur un IACS.

NOTE 1 Dans le présent document, 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 processus de sécurité proposés par un fournisseur de service IACS sont appelés Programme de sécurité (SP) pour les propriétaires d'actifs IACS. 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 1 représente les processus de sécurité d'intégration et de maintenance du propriétaire d'actif, du ou des fournisseurs de services et du ou des fournisseurs de produits d'un IACS ainsi que les relations qui les lient entre eux et qui les lient à la Solution d'Automatisation. Certaines des exigences du présent document relatives au programme de sécurité sont associées aux exigences de sécurité décrites dans l'IEC 62443-3-3 et l'IEC 62443-4-2.

NOTE 3 L'IACS est la combinaison de la Solution d'Automatisation et des mesures d'organisation nécessaires à sa conception, son déploiement, son fonctionnement et sa maintenance.

NOTE 4 La maintenance d'un système existant avec des capacités techniques de sécurité insuffisantes, la mise en œuvre de politiques, de processus et de procédures peuvent être traitées par l'atténuation des risques.

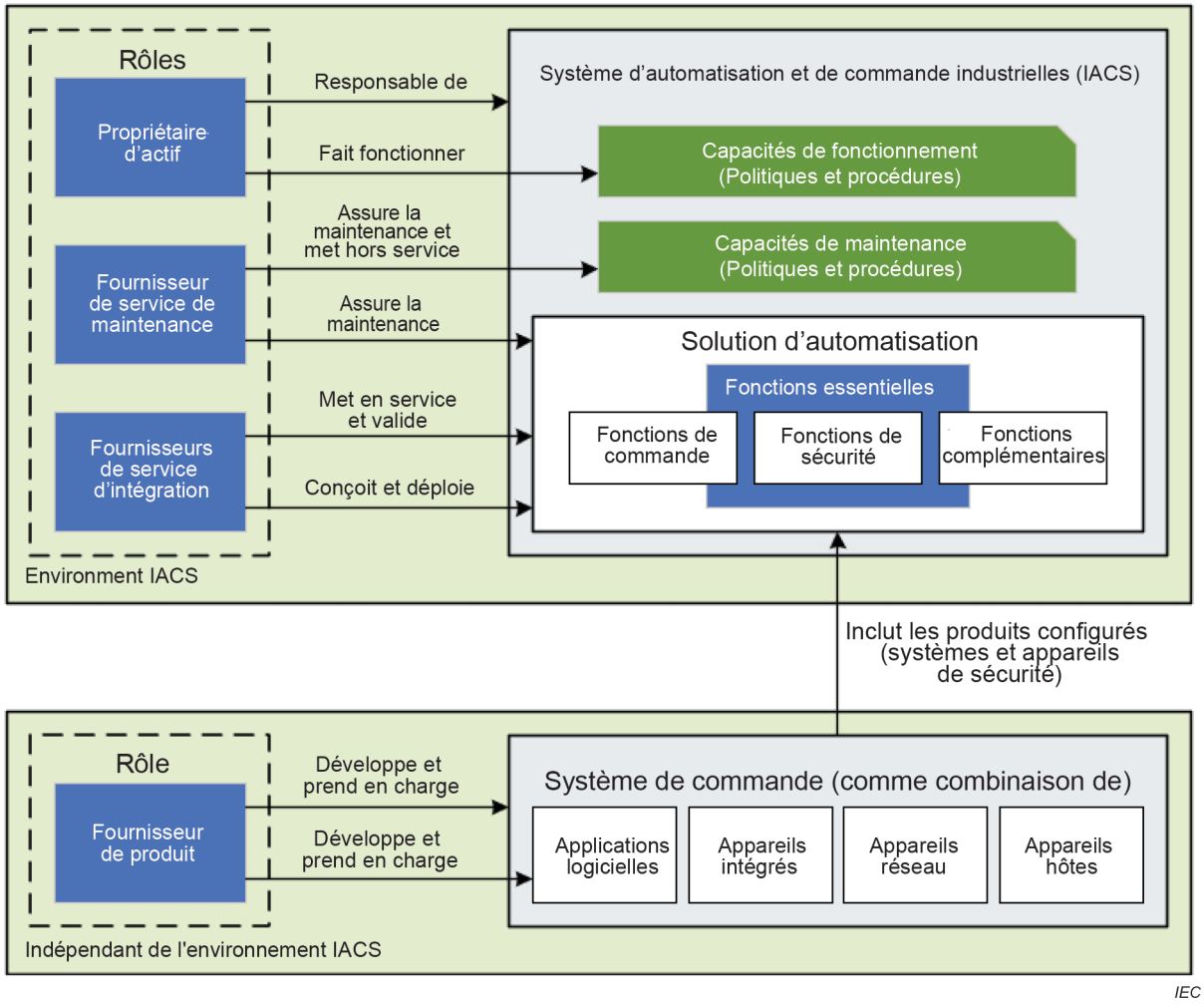

Figure 1 – Étendue des processus du fournisseur de service

À la Figure 1, la Solution d'Automatisation contient des fonctions essentielles qui comprennent les fonctions de sécurité, généralement mises en œuvre par un système équipé pour la sécurité (SIS - *Safety Instrumented System*), et les fonctions complémentaires et de commande, généralement mises en œuvre au moyen d'applications de prise en charge comme les applications de gestion par lots, de commande avancée, d'historisation et les applications liées à la sécurité. Les cases en pointillé indiquent les rôles organisationnels qui effectuent les actions indiquées.

NOTE 5 En règle générale, les Solutions d'Automatisation comportent 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) comme cela est défini par le propriétaire d'actif.

NOTE 6 Les fournisseurs de services proposent souvent des architectures génériques qui peuvent être adaptées pour être intégrées dans une Solution d'Automation. Ces architectures génériques sont souvent appelées "architectures de référence".

2 Références normatives

Le présent document ne contient aucune référence normative.