IEC 62443-3-3

Edition 1.0 2013-08

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels

Réseaux industriels de communication – Sécurité dans les réseaux et les systèmes – Partie 3-3: Exigences de sécurité des systèmes et niveaux de sécurité

IEC 62443-3-3:2013-08(en-fr)

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
info@iec.ch
www.iec.ch

About the IEC
The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

About IEC publications
The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigendum or an amendment might have been published.

IEC publications search - webstore.iec.ch/advsearchform
The advanced search enables to find IEC publications by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished
Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc
If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: sales@iec.ch.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
67 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

A propos de l'IEC
La Commission Electrotechnique Internationale (IEC) est la première organisation mondiale qui élabore et publie des Normes internationales pour tout ce qui a trait à l'électricité, à l'électronique et aux technologies apparentées.

A propos des publications IEC
Le contenu technique des publications IEC est constamment revu. Veuillez vous assurer que vous possédez l'édition la plus récente, un corrigendum ou amendement peut avoir été publié.

Recherche de publications IEC - webstore.iec.ch/advsearchform
La recherche avancée permet de trouver des publications IEC en utilisant différents critères (numéro de référence, texte, comité d'études,…). Elle donne aussi des informations sur les projets et les publications remplacées ou retirées.

IEC Just Published - webstore.iec.ch/justpublished
Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et une fois par mois par email.

Service Clients - webstore.iec.ch/csc
Si vous désirez nous donner des commentaires sur cette publication ou si vous avez des questions contactez-nous: sales@iec.ch.

Electropedia - www.electropedia.org
Le premier dictionnaire d'électrotechnologie en ligne au monde, avec plus de 22 000 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 16 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

Glossaire IEC - std.iec.ch/glossary
67 000 entrées terminologiques électrotechniques, en anglais et en français, extraites des articles Termes et Définitions des publications IEC parues depuis 2002. Plus certaines entrées antérieures extraites des publications des CE 37, 77, 86 et CISPR de l'IEC.

IEC 62443-3-3

Edition 1.0 2013-08

INTERNATIONAL STANDARD

NORME INTERNATIONALE

colour inside

Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels

Réseaux industriels de communication – Sécurité dans les réseaux et les systèmes – Partie 3-3: Exigences de sécurité des systèmes et niveaux de sécurité

INTERNATIONAL ELECTROTECHNICAL COMMISSION

COMMISSION ELECTROTECHNIQUE INTERNATIONALE

ICS 25.040.40; 35.110

ISBN 978-2-8322-6422-5

CONTENTS

CONTENTS 2
FOREWORD 9
0 Introduction 11
0.1 Overview 11
0.2 Purpose and intended audience 12
0.3 Usage within other parts of the IEC 62443 series 12
1 Scope 14
2 Normative references 14
3 Terms, definitions, abbreviated terms, acronyms, and conventions 14
3.1 Terms and definitions 14
3.2 Abbreviated terms and acronyms 20
3.3 Conventions 22
4 Common control system security constraints 22
4.1 Overview 22
4.2 Support of essential functions 23
4.3 Compensating countermeasures 23
4.4 Least privilege 24
5 FR 1 – Identification and authentication control 24
5.1 Purpose and SL-C(IAC) descriptions 24
5.2 Rationale 24
5.3 SR 1.1 – Human user identification and authentication 24
5.3.1 Requirement 24
5.3.2 Rationale and supplemental guidance 24
5.3.3 Requirement enhancements 25
5.3.4 Security levels 25
5.4 SR 1.2 – Software process and device identification and authentication 26
5.4.1 Requirement 26
5.4.2 Rationale and supplemental guidance 26
5.4.3 Requirement enhancements 26
5.4.4 Security levels 27
5.5 SR 1.3 – Account management 27
5.5.1 Requirement 27
5.5.2 Rationale and supplemental guidance 27
5.5.3 Requirement enhancements 27
5.5.4 Security levels 27
5.6 SR 1.4 – Identifier management 28
5.6.1 Requirement 28
5.6.2 Rationale and supplemental guidance 28
5.6.3 Requirement enhancements 28
5.6.4 Security levels 28
5.7 SR 1.5 – Authenticator management 28
5.7.1 Requirement 28
5.7.2 Rationale and supplemental guidance 28
5.7.3 Requirement enhancements 29
5.7.4 Security levels 29
5.8 SR 1.6 – Wireless access management 30

5.8.1 Requirement 30
5.8.2 Rationale and supplemental guidance 30
5.8.3 Requirement enhancements 30
5.8.4 Security levels 30
5.9 SR 1.7 – Strength of password-based authentication 30
5.9.1 Requirement 30
5.9.2 Rationale and supplemental guidance 30
5.9.3 Requirement enhancements 31
5.9.4 Security levels 31
5.10 SR 1.8 – Public key infrastructure (PKI) certificates 31
5.10.1 Requirement 31
5.10.2 Rationale and supplemental guidance 31
5.10.3 Requirement enhancements 32
5.10.4 Security levels 32
5.11 SR 1.9 – Strength of public key authentication 32
5.11.1 Requirement 32
5.11.2 Rationale and supplemental guidance 32
5.11.3 Requirement enhancements 33
5.11.4 Security levels 33
5.12 SR 1.10 – Authenticator feedback 33
5.12.1 Requirement 33
5.12.2 Rationale and supplemental guidance 33
5.12.3 Requirement enhancements 33
5.12.4 Security levels 33
5.13 SR 1.11 – Unsuccessful login attempts 34
5.13.1 Requirement 34
5.13.2 Rationale and supplemental guidance 34
5.13.3 Requirement enhancements 34
5.13.4 Security levels 34
5.14 SR 1.12 – System use notification 34
5.14.1 Requirement 34
5.14.2 Rationale and supplemental guidance 34
5.14.3 Requirement enhancements 35
5.14.4 Security levels 35
5.15 SR 1.13 – Access via untrusted networks 35
5.15.1 Requirement 35
5.15.2 Rationale and supplemental guidance 35
5.15.3 Requirement enhancements 35
5.15.4 Security levels 35
6 FR 2 – Use control 36
6.1 Purpose and SL-C(UC) descriptions 36
6.2 Rationale 36
6.3 SR 2.1 – Authorization enforcement 36
6.3.1 Requirement 36
6.3.2 Rationale and supplemental guidance 36
6.3.3 Requirement enhancements 37
6.3.4 Security levels 37
6.4 SR 2.2 – Wireless use control 37
6.4.1 Requirement 37

6.4.2 Rationale and supplemental guidance 38
6.4.3 Requirement enhancements 38
6.4.4 Security levels 38
6.5 SR 2.3 – Use control for portable and mobile devices 38
6.5.1 Requirement 38
6.5.2 Rationale and supplemental guidance 38
6.5.3 Requirement enhancements 39
6.5.4 Security levels 39
6.6 SR 2.4 – Mobile code 39
6.6.1 Requirement 39
6.6.2 Rationale and supplemental guidance 39
6.6.3 Requirement enhancements 39
6.6.4 Security levels 39
6.7 SR 2.5 – Session lock 40
6.7.1 Requirement 40
6.7.2 Rationale and supplemental guidance 40
6.7.3 Requirement enhancements 40
6.7.4 Security levels 40
6.8 SR 2.6 – Remote session termination 40
6.8.1 Requirement 40
6.8.2 Rationale and supplemental guidance 40
6.8.3 Requirement enhancements 40
6.8.4 Security levels 41
6.9 SR 2.7 – Concurrent session control 41
6.9.1 Requirement 41
6.9.2 Rationale and supplemental guidance 41
6.9.3 Requirement enhancements 41
6.9.4 Security levels 41
6.10 SR 2.8 – Auditable events 41
6.10.1 Requirement 41
6.10.2 Rationale and supplemental guidance 41
6.10.3 Requirement enhancements 42
6.10.4 Security levels 42
6.11 SR 2.9 – Audit storage capacity 42
6.11.1 Requirement 42
6.11.2 Rationale and supplemental guidance 42
6.11.3 Requirement enhancements 42
6.11.4 Security levels 43
6.12 SR 2.10 – Response to audit processing failures 43
6.12.1 Requirement 43
6.12.2 Rationale and supplemental guidance 43
6.12.3 Requirement enhancements 43
6.12.4 Security levels 43
6.13 SR 2.11 – Timestamps 43
6.13.1 Requirement 43
6.13.2 Rationale and supplemental guidance 43
6.13.3 Requirement enhancements 44
6.13.4 Security levels 44
6.14 SR 2.12 – Non-repudiation 44

6.14.1 Requirement 44
6.14.2 Rationale and supplemental guidance 44
6.14.3 Requirement enhancements 44
6.14.4 Security levels 44
7 FR 3 – System integrity 45
7.1 Purpose and SL-C(SI) descriptions 45
7.2 Rationale 45
7.3 SR 3.1 – Communication integrity 45
7.3.1 Requirement 45
7.3.2 Rationale and supplemental guidance 45
7.3.3 Requirement enhancements 46
7.3.4 Security levels 46
7.4 SR 3.2 – Malicious code protection 46
7.4.1 Requirement 46
7.4.2 Rationale and supplemental guidance 46
7.4.3 Requirement enhancements 47
7.4.4 Security levels 47
7.5 SR 3.3 – Security functionality verification 47
7.5.1 Requirement 47
7.5.2 Rationale and supplemental guidance 47
7.5.3 Requirement enhancements 48
7.5.4 Security levels 48
7.6 SR 3.4 – Software and information integrity 48
7.6.1 Requirement 48
7.6.2 Rationale and supplemental guidance 48
7.6.3 Requirement enhancements 49
7.6.4 Security levels 49
7.7 SR 3.5 – Input validation 49
7.7.1 Requirement 49
7.7.2 Rationale and supplemental guidance 49
7.7.3 Requirement enhancements 49
7.7.4 Security levels 49
7.8 SR 3.6 – Deterministic output 50
7.8.1 Requirement 50
7.8.2 Rationale and supplemental guidance 50
7.8.3 Requirement enhancements 50
7.8.4 Security levels 50
7.9 SR 3.7 – Error handling 50
7.9.1 Requirement 50
7.9.2 Rationale and supplemental guidance 50
7.9.3 Requirement enhancements 50
7.9.4 Security levels 51
7.10 SR 3.8 – Session integrity 51
7.10.1 Requirement 51
7.10.2 Rationale and supplemental guidance 51
7.10.3 Requirement enhancements 51
7.10.4 Security levels 51
7.11 SR 3.9 – Protection of audit information 52
7.11.1 Requirement 52

7.11.2 Rationale and supplemental guidance 52
7.11.3 Requirement enhancements 52
7.11.4 Security levels 52
8 FR 4 – Data confidentiality 52
8.1 Purpose and SL-C(DC) descriptions 52
8.2 Rationale 52
8.3 SR 4.1 – Information confidentiality 53
8.3.1 Requirement 53
8.3.2 Rationale and supplemental guidance 53
8.3.3 Requirement enhancements 53
8.3.4 Security levels 53
8.4 SR 4.2 – Information persistence 54
8.4.1 Requirement 54
8.4.2 Rationale and supplemental guidance 54
8.4.3 Requirement enhancements 54
8.4.4 Security levels 54
8.5 SR 4.3 – Use of cryptography 54
8.5.1 Requirement 54
8.5.2 Rationale and supplemental guidance 55
8.5.3 Requirement enhancements 55
8.5.4 Security levels 55
9 FR 5 – Restricted data flow 55
9.1 Purpose and SL-C(RDF) descriptions 55
9.2 Rationale 55
9.3 SR 5.1 – Network segmentation 56
9.3.1 Requirement 56
9.3.2 Rationale and supplemental guidance 56
9.3.3 Requirement enhancements 56
9.3.4 Security levels 57
9.4 SR 5.2 – Zone boundary protection 57
9.4.1 Requirement 57
9.4.2 Rationale and supplemental guidance 57
9.4.3 Requirement enhancements 57
9.4.4 Security levels 58
9.5 SR 5.3 – General purpose person-to-person communication restrictions 58
9.5.1 Requirement 58
9.5.2 Rationale and supplemental guidance 58
9.5.3 Requirement enhancements 58
9.5.4 Security levels 59
9.6 SR 5.4 – Application partitioning 59
9.6.1 Requirement 59
9.6.2 Rationale and supplemental guidance 59
9.6.3 Requirement enhancements 59
9.6.4 Security levels 59
10 FR 6 – Timely response to events 59
10.1 Purpose and SL-C(TRE) descriptions 59
10.2 Rationale 60
10.3 SR 6.1 – Audit log accessibility 60
10.3.1 Requirement 60

10.3.2 Rationale and supplemental guidance 60
10.3.3 Requirement enhancements 60
10.3.4 Security levels 60
10.4 SR 6.2 – Continuous monitoring 60
10.4.1 Requirement 60
10.4.2 Rationale and supplemental guidance 60
10.4.3 Requirement enhancements 61
10.4.4 Security levels 61
11 FR 7 – Resource availability 61
11.1 Purpose and SL-C(RA) descriptions 61
11.2 Rationale 61
11.3 SR 7.1 – Denial of service protection 62
11.3.1 Requirement 62
11.3.2 Rationale and supplemental guidance 62
11.3.3 Requirement enhancements 62
11.3.4 Security levels 62
11.4 SR 7.2 – Resource management 62
11.4.1 Requirement 62
11.4.2 Rationale and supplemental guidance 62
11.4.3 Requirement enhancements 62
11.4.4 Security levels 63
11.5 SR 7.3 – Control system backup 63
11.5.1 Requirement 63
11.5.2 Rationale and supplemental guidance 63
11.5.3 Requirement enhancements 63
11.5.4 Security levels 63
11.6 SR 7.4 – Control system recovery and reconstitution 63
11.6.1 Requirement 63
11.6.2 Rationale and supplemental guidance 63
11.6.3 Requirement enhancements 64
11.6.4 Security levels 64
11.7 SR 7.5 – Emergency power 64
11.7.1 Requirement 64
11.7.2 Rationale and supplemental guidance 64
11.7.3 Requirement enhancements 64
11.7.4 Security levels 64
11.8 SR 7.6 – Network and security configuration settings 64
11.8.1 Requirement 64
11.8.2 Rationale and supplemental guidance 64
11.8.3 Requirement enhancements 65
11.8.4 Security levels 65
11.9 SR 7.7 – Least functionality 65
11.9.1 Requirement 65
11.9.2 Rationale and supplemental guidance 65
11.9.3 Requirement enhancements 65
11.9.4 Security levels 65
11.10 SR 7.8 – Control system component inventory 66
11.10.1 Requirement 66
11.10.2 Rationale and supplemental guidance 66

11.10.3 Requirement enhancements 66
11.10.4 Security levels 66
Annex A (informative) Discussion of the SL vector 67
Annex B (informative) Mapping of SRs and REs to FR SL levels 1-4 75
Bibliography 79

Figure 1 – Structure of the IEC 62443 series 13
Figure A.1 – High-level process-industry example showing zones and conduits 69
Figure A.2 – High-level manufacturing example showing zones and conduits 70
Figure A.3 – Schematic of correlation of the use of different SL types 71

Table B.1 – Mapping of SRs and REs to FR SL levels 1-4 *(1 of 4)* 75

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

INDUSTRIAL COMMUNICATION NETWORKS – NETWORK AND SYSTEM SECURITY –

Part 3-3: System security requirements and security levels

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 62443-3-3 has been prepared by IEC technical committee 65: Industrial-process measurement, control and automation.

This bilingual version (2019-01) corresponds to the monolingual English version, published in 2013-08.

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

FDIS	Report on voting
65/531/FDIS	65/540/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 parts in the IEC 62443 series, published under the general title *Industrial communication networks – Network and system security*, can be found on the IEC website.

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 April 2014 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.

0 Introduction

0.1 Overview

NOTE 1 This standard is part of series of standards that addresses the issue of security for industrial automation and control systems (IACS). It has been developed by working group 4, task group 2 of the IEC99 committee in cooperation with IEC TC65/WG10. This document prescribes the security requirements for control systems related to the seven foundational requirements defined in IEC 62443-1-1 and assigns system security levels (SLs) to the system under consideration (SuC).

NOTE 2 The format of this standard follows the ISO/IEC requirements discussed in ISO/IEC Directives, Part 2 [11].[1] These directives specify the format of the standard as well as the use of terms like “shall”, “should”, and “may”. The requirements specified in normative clauses use the conventions discussed in Appendix H of the ISO/IEC Directives.

Industrial automation and control system (IACS) organizations increasingly use commercial-off-the-shelf (COTS) networked devices that are inexpensive, efficient and highly automated. Control systems are also increasingly interconnected with non-IACS networks for valid business reasons. These devices, open networking technologies and increased connectivity provide an increased opportunity for cyber attack against control system hardware and software. That weakness may lead to health, safety and environmental (HSE), financial and/or reputational consequences in deployed control systems.

Organizations deploying business information technology (IT) cyber security solutions to address IACS security may not fully comprehend the results of this decision. While many business IT applications and security solutions can be applied to IACS, they need to be applied in an appropriate way to eliminate inadvertent consequences. For this reason, the approach used to define system requirements needs to be based on a combination of functional requirements and risk assessment, often including an awareness of operational issues as well.

IACS security measures should not have the potential to cause loss of essential services and functions, including emergency procedures. (IT security measures, as often deployed, do have this potential.) IACS security goals focus on control system availability, plant protection, plant operations (even in a degraded mode) and time-critical system response. IT security goals often do not place the same emphasis on these factors; they may be more concerned with protecting information rather than physical assets. These different goals need to be clearly stated as security objectives regardless of the degree of plant integration achieved. A key step in risk assessment, as required by IEC 62443-2-1[2], should be the identification of which services and functions are truly essential for operations. (For example, in some facilities engineering support may be determined to be a non-essential service or function.) In some cases, it may be acceptable for a security action to cause temporary loss of a non-essential service or function, unlike an essential service or function that should not be adversely affected.

This standard assumes that a security program has been established and is being operated in accordance with IEC 62443-2-1. Furthermore, it is assumed that patch management is implemented consistently with the recommendations detailed in IEC/TR 62443-2-3 [5] utilizing the appropriate control system requirements and requirement enhancements as described in this standard. In addition, IEC 62443-3-2 [8] describes how a project defines risk-based security levels (SLs) which then are used to select products with the appropriate technical security capabilities as detailed in this standard. Key input to this standard included ISO/IEC 27002 [15] and NIST SP800-53, rev 3 [24] (see Clause 2 and the Bibliography for a more complete listing of source material).

---

1 Numbers in square brackets refer to the Bibliography.

2 Many documents in the IEC 62443 series are currently under review or in development.

The primary goal of the IEC 62443 series is to provide a flexible framework that facilitates addressing current and future vulnerabilities in IACS and applying necessary mitigations in a systematic, defensible manner. It is important to understand that the intention of the IEC 62443 series is to build extensions to enterprise security that adapt the requirements for business IT systems and combines them with the unique requirements for strong availability needed by IACS.

0.2 Purpose and intended audience

The IACS community audience for this standard is intended to be asset owners, system integrators, product suppliers, service providers and, where appropriate, compliance authorities. Compliance authorities include government agencies and regulators with the legal authority to perform audits to verify compliance with governing laws and regulations.

System integrators, product suppliers and service providers will use this standard to evaluate whether their products and services can provide the functional security capability to meet the asset owner's target security level (SL-T) requirements. As with the assignment of SL-Ts, the applicability of individual control system requirements (SRs) and requirement enhancements (REs) needs to be based on an asset owner's security policies, procedures and risk assessment in the context of their specific site. Note that some SRs contain specific conditions for permissible exceptions, such as where meeting the SR will violate fundamental operational requirements of a control system (which may trigger the need for compensating countermeasures).

When designing a control system to meet the set of SRs associated with specific SL-Ts, it is not necessary that every component of the proposed control system support every system requirement to the level mandated in this standard. Compensating countermeasures can be employed to provide the needed functionality to other subsystems, such that the overall SL-T requirements are met at the control system level. Inclusion of compensating countermeasures during the design phase should be accompanied by comprehensive documentation so that the resulting achieved control system SL, SL-A(control system), fully reflects the intended security capabilities inherent in the design. Similarly, during certification testing and/or post-installation audits, compensating countermeasures can be utilized and documented in order to meet the overall control system SL.

There is insufficient detail in this standard to design and build an integrated security architecture. That requires additional system-level analysis and development of derived requirements that are the subject of other standards in the IEC 62443 series (see 0). Note that providing specifications detailed enough to build a security architecture are not the goal of this standard. The goal is to define a common, minimum set of requirements to reach progressively more stringent security levels. The actual design of an architecture that meets these requirements is the job of system integrators and product suppliers. In this task, they retain the freedom to make individual choices, thus supporting competition and innovation. Thus this standard strictly adheres to specifying functional requirements, and does not address how these functional requirements should be met.

0.3 Usage within other parts of the IEC 62443 series

Figure 1 shows a graphical depiction of the IEC 62443 series when this standard was written.

IEC 62443-3-2 uses the SRs and REs as a checklist. After the system under consideration (SuC) has been described in terms of zones and conduits, and individual target SLs have been assigned to these zones and conduits, the SRs and REs in this standard, as well as their mapping to capability SLs (SL-Cs), are used to compile a list of requirements which the control system design needs to meet. A given control system design can then be checked for completeness, thereby providing the SL-As.

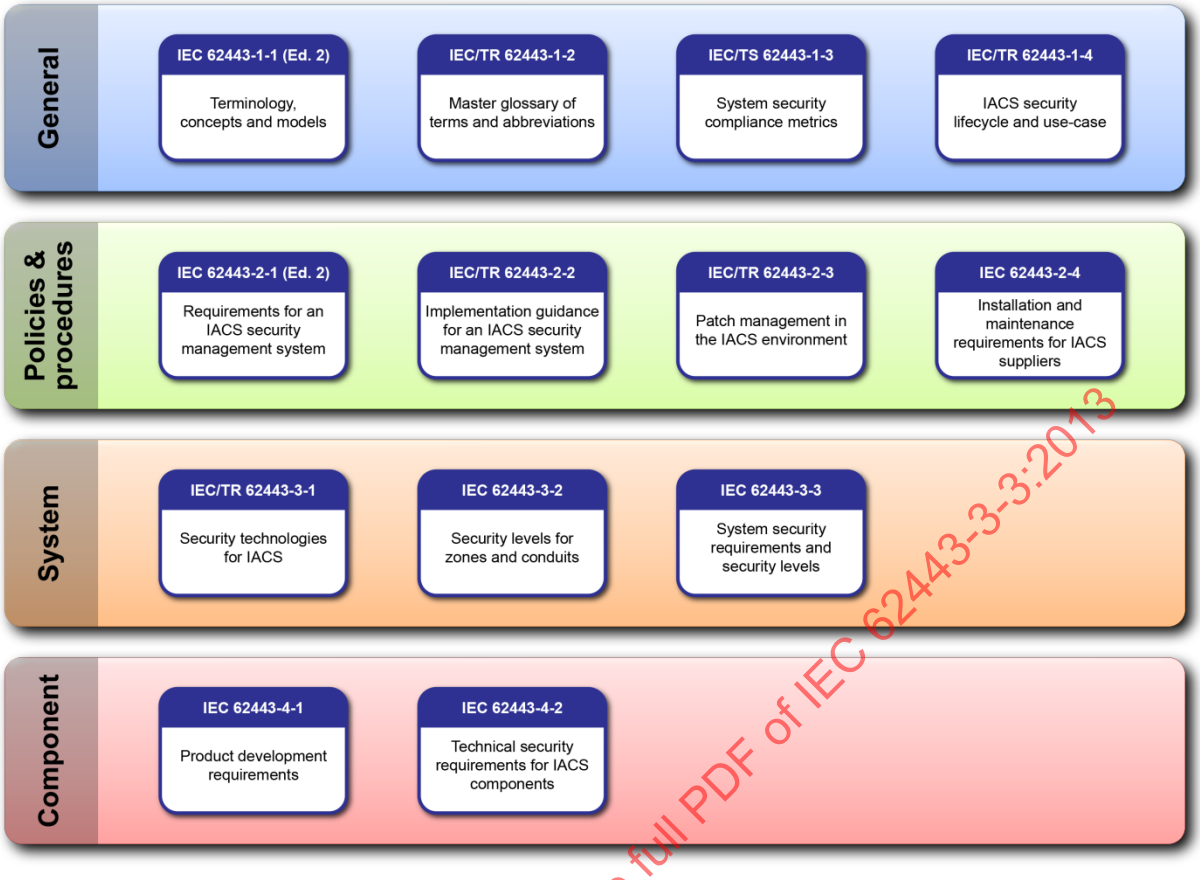


Figure 1 – Structure of the IEC 62443 series

IEC/TS 62443-1-3 [2] uses the foundational requirements (FRs), SRs, REs and the mapping to SL-Cs as a checklist to test for completeness of the specification of quantitative metrics. The quantitative security compliance metrics are context specific. Together with IEC 62443-3-2, the asset owner's SL-T assignments are translated into quantitative metrics that can be used to support system analysis and design trade-off studies, to develop a security architecture.

IEC 62443-4-1 [9] addresses the overall requirements during the development of products. As such, IEC 62443-4-1 is product supplier centric. Product security requirements are derived from the list of baseline requirements and REs specified in this standard. Normative quality specifications in IEC 62443-4-1 will be used when developing these product capabilities.

IEC 62443-4-2 [10] contains sets of derived requirements that provide a detailed mapping of the SRs specified in this standard to subsystems and components of the SuC. At the time this standard was written, the component categories addressed in IEC 62443-4-2 were: embedded devices, host devices, network devices and applications. As such, IEC 62443-4-2 is vendor (product supplier and service provider) centric. Product security requirements are first derived from the list of baseline requirements and REs specified in this standard. Security requirements and metrics from IEC 62443-3-2 and IEC/TS 62443-1-3 are used to refine these normative derived requirements.

INDUSTRIAL COMMUNICATION NETWORKS – NETWORK AND SYSTEM SECURITY –

Part 3-3: System security requirements and security levels

1 Scope

This part of the IEC 62443 series provides detailed technical control system requirements (SRs) associated with the seven foundational requirements (FRs) described in IEC 62443-1-1 including defining the requirements for control system capability security levels, SL-C(control system). These requirements would be used by various members of the industrial automation and control system (IACS) community along with the defined zones and conduits for the system under consideration (SuC) while developing the appropriate control system target SL, SL-T(control system), for a specific asset.

As defined in IEC 62443-1-1 there are a total of seven FRs:

a) Identification and authentication control (IAC),
b) Use control (UC),
c) System integrity (SI),
d) Data confidentiality (DC),
e) Restricted data flow (RDF),
f) Timely response to events (TRE), and
g) Resource availability (RA).

These seven requirements are the foundation for control system capability SLs, SL-C (control system). Defining security capability at the control system level is the goal and objective of this standard as opposed to target SLs, SL-T, or achieved SLs, SL-A, which are out of scope.

See IEC 62443-2-1 for an equivalent set of non-technical, program-related, capability SRs necessary for fully achieving a control system target SL.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

IEC 62443-2-1, *Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program*

3 Terms, definitions, abbreviated terms, acronyms, and conventions

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in IEC 62443-1-1 and in IEC 62443-2-1, as well as the following, apply.

NOTE Many of the following terms and definitions are originally based on relevant International Organization for Standardization (ISO), International Electrotechnical Commission (IEC) or U.S. National Institute of Standards and Technology (NIST) sources, sometimes with minor modifications to enhance suitability when defining control system security requirements.

3.1.1
asset
physical or logical object having either a perceived or actual value to the IACS

Note 1 to entry: In this standard, an asset is any item that should be protected as part of the IACS security management system.

3.1.2
asset owner
individual or company responsible for one or more IACS

Note 1 to entry: The term "asset owner" is used in place of the generic term "end user" to provide differentiation.

Note 2 to entry: This definition includes the components that are part of the IACS.

Note 3 to entry: In the context of this standard, an asset owner also includes the operator of the IACS.

3.1.3
attack
assault on a system that derives from an intelligent threat

Note 1 to entry: For example, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system

Note 2 to entry: There are different commonly recognized classes of attack:

- an "active attack" attempts to alter system resources or affect their operation;
- a "passive attack" attempts to learn or make use of information from the system but does not affect system resources;
- an "inside attack" is an attack initiated by an entity inside the security perimeter (an "insider"), for example, an entity that is authorized to access system resources but uses them in a way not approved by those who granted the authorization;
- an "outside attack" is initiated from outside the perimeter, by an unauthorized or illegitimate user of the system (including an insider attacking from outside the security perimeter). Potential outside attackers range from amateur pranksters to organized criminals, international terrorists and hostile governments.

3.1.4
authentication
provision of assurance that a claimed characteristic of an identity is correct

Note 1 to entry: Authentication is usually a prerequisite to allowing access to resources in a control system.

3.1.5
authenticator
means used to confirm the identity of a user (human, software process or device)

Note 1 to entry: For example, a password or token may be used as an authenticator.

3.1.6
authenticity
property that an entity is what it claims to be

Note 1 to entry: Authenticity is typically used in the context of confidence in the identity of an entity, or the validity of a transmission, a message or message originator.

3.1.7
automatic
process or equipment that, under specified conditions, functions without human intervention

3.1.8
availability
property of ensuring timely and reliable access to and use of control system information and functionality

3.1.9
communication channel
specific logical or physical communication link between assets

Note 1 to entry: A channel facilitates the establishment of a connection.

3.1.10
compensating countermeasure
countermeasure employed in lieu of or in addition to inherent security capabilities to satisfy one or more security requirements

Note 1 to entry: Examples include:

- (component-level): locked cabinet around a controller that doesn't have sufficient cyber access control countermeasures;
- (control system/zone-level): physical access control (guards, gates and guns) to protect a control room to restrict access to a group of known personnel to compensate for the technical requirement for personnel to be uniquely identified by the IACS; and
- (component-level): a vendor's programmable logic controller (PLC) can't meet the access control capabilities from an end-user, so the vendor puts a firewall in front of the PLC and sells it as a system.

3.1.11
compliance authority
entity with legal jurisdiction to determine the adequacy of a security assessment, implementation or effectiveness as specified in a governing document

3.1.12
conduit
logical grouping of communication channels, connecting two or more zones, that share common security requirements

Note 1 to entry: A conduit is allowed to traverse a zone as long as the security of the channels contained within the conduit is not impacted by the zone.

3.1.13
confidentiality
preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information

Note 1 to entry: When used in the context of an IACS, this term refers to protecting IACS data and information from unauthorized access.

3.1.14
connection
association established between two or more endpoints which supports the establishment of a session

3.1.15
consequence
condition or state that logically or naturally follows from an event

3.1.16
control system
hardware and software components of an IACS

3.1.17
countermeasure
action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken

Note 1 to entry: The term “control” is also used to describe this concept in some contexts. The term countermeasure has been chosen for this standard to avoid confusion with the term “control” in the context of “process control”.

3.1.18
degraded mode
mode of operation in the presence of faults which have been anticipated in the design of the control system

Note 1 to entry: Degraded modes allow the control system to continue to provide essential functions despite the deficiency of one or several system elements, for example malfunction or outage of control equipment, disruption of communication due to failure or intentional system isolation in response to identified or suspected compromise of subsystems.

3.1.19
demilitarized zone
common, limited network of servers joining two or more zones for the purpose of controlling data flow between zones

Note 1 to entry: Demilitarized zones (DMZs) are typically used to avoid direct connections between different zones.

3.1.20
device
asset incorporating one or more processors with the capability of sending or receiving data/control to or from another asset

Note 1 to entry: Examples include controllers, human-machine interfaces (HMIs), PLCs, remote terminal units (RTUs), transmitters, actuators, valves, network switches, etc.

3.1.21
environment
surrounding objects, region or circumstances which may influence the behavior of the IACS and/or may be influenced by the IACS

3.1.22
essential function
function or capability that is required to maintain health, safety, the environment and availability for the equipment under control

Note 1 to entry: Essential functions include, but are not limited to, the safety instrumented function (SIF), the control function and the ability of the operator to view and manipulate the equipment under control. The loss of essential functions is commonly termed loss of protection, loss of control and loss of view respectively. In some industries additional functions such as history may be considered essential.

3.1.23
event
occurrence of or change to a particular set of circumstances

Note 1 to entry: In an IACS this may be an action taken by an individual (authorized or unauthorized), a change detected within the control system (normal or abnormal) or an automated response from the control system itself (normal or abnormal).

3.1.24
firecall
method established to provide emergency access to a secure control system

Note 1 to entry: In an emergency situation, unprivileged users can gain access to key systems to correct the problem. When a firecall is used, there is usually a review process to ensure that the access was used properly to correct a problem. These methods generally either provide a one-time use user identifier (ID) or one-time password.

3.1.25
identifier
symbol, unique within its security domain, that identifies, indicates or names an entity which makes an assertion or claim of identity

3.1.26
identify
assertion of an identity

3.1.27
impact
evaluated consequence of a particular event

3.1.28
incident
event that is not part of the expected operation of a system or service that causes, or may cause, an interruption to, or a reduction in, the quality of the service provided by the control system

3.1.29
industrial automation and control system
collection of personnel, hardware, software and policies involved in the operation of the industrial process and that can affect or influence its safe, secure and reliable operation

3.1.30
integrity
property of protecting the accuracy and completeness of assets

3.1.31
least privilege
basic principle that holds that users (humans, software processes or devices) should be assigned the fewest privileges consistent with their assigned duties and functions

Note 1 to entry: Least privilege is commonly implemented as a set of roles in an IACS.

3.1.32
mobile code
program transferred between a remote, possibly “untrusted” system, across a network or via removable media that can be executed unchanged on a local system without explicit installation or execution by the recipient

Note 1 to entry: Examples of mobile code include JavaScript, VBScript, Java applets, ActiveX controls, Flash animations, Shockwave movies, and Microsoft Office macros.

3.1.33
non-repudiation
ability to prove the occurrence of a claimed event or action and its originating entities

Note 1 to entry: The purpose of non-repudiation is to resolve disputes about the occurrence or non-occurrence of the event or action and involvement of entities in the event.

3.1.34
product supplier
manufacturer of hardware and/or software product

Note 1 to entry: This term is used in place of the generic word “vendor” to provide differentiation.

3.1.35
remote access
access to a control system by any user (human, software process or device) communicating from outside the perimeter of the zone being addressed

3.1.36
role
set of connected behaviors, privileges and obligations associated with all users (humans, software processes or devices) of an IACS

Note 1 to entry: The privileges to perform certain operations are assigned to specific roles.

3.1.37
safety instrumented system
system used to implement one or more safety-related functions

3.1.38
security level
measure of confidence that the IACS is free from vulnerabilities and functions in the intended manner

Note 1 to entry: Vulnerabilities can either be designed into the IACS, inserted at any time during its lifecycle or result from changing threats. Designed-in vulnerabilities may be discovered long after the initial deployment of the IACS, for example an encryption technique has been broken or an improper policy for account management such as not removing old user accounts. Inserted vulnerabilities may be the result of a patch or a change in policy that opens up a new vulnerability.

3.1.39
service provider
organization (internal or external organization, manufacturer, etc.) that has agreed to undertake responsibility for providing a given support service and obtaining, when specified, supplies in accordance with an agreement

Note 1 to entry: This term is used in place of the generic word “vendor” to provide differentiation.

3.1.40
session
semi-permanent, stateful and interactive information interchange between two or more communicating devices

Note 1 to entry: Typically a session has clearly defined start and end processes.

3.1.41
session ID
identifier used to indicate a specific session entry

3.1.42
set point
target value identified within a control system that controls one or more actions within the control system

3.1.43
system integrator
person or company that specializes in bringing together component subsystems into a whole and ensuring that those subsystems perform in accordance with project specifications

3.1.44
threat
circumstance or event with the potential to adversely affect operations (including mission, functions, image or reputation), assets, control systems or individuals via unauthorized access, destruction, disclosure, modification of data and/or denial of service

3.1.45
trust
confidence that an operation, data transaction source, network or software process can be relied upon to behave as expected

Note 1 to entry: Generally, an entity can be said to 'trust' a second entity when it (the first entity) makes the assumption that the second entity will behave as the first entity expects.

Note 2 to entry: This trust may apply only for some specific function.

3.1.46
untrusted
not meeting predefined requirements to be trusted

Note 1 to entry: An entity may simply be declared as untrusted.

3.1.47
zone
grouping of logical or physical assets that share common security requirements

Note 1 to entry: A zone has a clear border. The security policy of a zone is typically enforced by a combination of mechanisms both at the zone edge and within the zone.

3.2 Abbreviated terms and acronyms

AES	Advanced encryption standard
API	Application programming interface
ASLR	Address space layout randomization
BPCS	Basic process control system
CA	Certification authority
CIP	Critical infrastructure protection
COTS	Commercial off the shelf
CRL	Certificate revocation list
DC	Data confidentiality
DEP	Data execution prevention
DHCP	Dynamic host configuration protocol
DMZ	Demilitarized zone
DNS	Domain name service
DoS	Denial of service
EICAR	European Institute for Computer Antivirus Research
EMI	Electromagnetic interference
FAT	Factory acceptance testing
FIPS	*[US NIST] Federal Information Processing Standard*
FR	Foundational requirement
FS-PLC	Functional safety PLC
FTP	File transfer protocol
GLONASS	Global Navigation Satellite System
GPS	Global Positioning System
HMI	Human-machine interface
HSE	Health, safety and environmental
HTTP	Hypertext transfer protocol

HTTPS	HTTP secure
IAC	Identification and authentication control
IACS	Industrial automation and control system(s)
IAMS	Instrument asset management system
ID	Identifier
IDS	Intrusion detection system
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IM	Instant messaging
IP	Internet Protocol
IPS	Intrusion prevention system
ISA	International Society of Automation
ISO	International Organization for Standardization
IT	Information technology
MES	Manufacturing execution system
NERC	North American Electric Reliability Corporation
NIST	U.S. National Institute of Standards and Technology
NX	No Execute
OCSP	Online certificate status protocol
OWASP	Open Web Application Security Project
PDF	Portable document format
PKI	Public key infrastructure
PLC	Programmable logic controller
RA	Resource availability
RAM	Random access memory
RDF	Restricted data flow
RE	Requirement enhancement
RFC	[IETF] Request for Comment
RJ	Registered jack
RTU	Remote terminal unit
SAT	Site acceptance testing
SHA	Secure hash algorithm
SI	System integrity
SIEM	Security Information and Event Management
SIF	Safety instrumented function
SIL	Safety integrity level
SIS	Safety instrumented system
SL	Security level
SL-A	Achieved security level
SL-C	Capability security level
SL-T	Target security level
SP	[US NIST] Special Publication

SR	System requirement
SSH	Secure socket shell
SuC	System under consideration
TCP	Transmission Control Protocol
TPM	Trusted platform module
TRE	Timely response to events
UC	Use control
USB	Universal serial bus
VoIP	Voice over internet protocol
WEP	Wired equivalent privacy
WLAN	Wireless local area network

3.3 Conventions

This standard expands the seven FRs defined in IEC 62443-1-1 into a series of SRs. Each SR has a baseline requirement and zero or more requirement enhancements (REs) to strengthen security. To provide clarity to the reader, rationale and supplemental guidance is provided for each baseline requirement and notes for any associated REs as is deemed necessary. The baseline requirement and REs, if present, are then mapped to the control system capability security level, SL-C(FR, control system) 1 to 4.

All seven FRs have a defined set of four SLs. The control system capability level 0 for a particular FR is implicitly defined as no requirements. For example, the purpose statement for Clause 8, FR 4 – Data confidentiality, is:

> Ensure the confidentiality of information on communication channels and in data repositories to prevent unauthorized disclosure.

The associated four SLs are defined as:

- SL 1 – Prevent the unauthorized disclosure of information via eavesdropping or casual exposure.
- SL 2 – Prevent the unauthorized disclosure of information to an entity actively searching for it using simple means with low resources, generic skills and low motivation.
- SL 3 – Prevent the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with moderate resources, IACS specific skills and moderate motivation.
- SL 4 – Prevent the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with extended resources, IACS specific skills and high motivation.

The individual SR and RE assignments are thus based on an incremental increase in overall control system security for that particular FR.

The SL-C(control system), used throughout this standard, signifies a capability required to meet a given SL rating for a given FR. A complete description of the SL vector concept can be found in Annex A.

4 Common control system security constraints

4.1 Overview

When reading, specifying and implementing the control system SRs detailed in Clauses 5 through 11 of this standard, there are a number of common constraints that shall be adhered to. The introduction of this standard provided some contextual, informative discussion of what

this standard is designed to accomplish. This clause and the subsequent FR-specific clauses furnish the normative material necessary to build extensions to existing enterprise security to support the rigorous integrity and availability requirements needed by IACS.

NOTE The contents of this clause will eventually be incorporated into IEC 62443-1-1.

4.2 Support of essential functions

As documented in 3.1.22, an essential function is a “function or capability that is required to maintain health, safety, the environment and availability for the equipment under control.”

- Security measures shall not adversely affect essential functions of a high availability IACS unless supported by a risk assessment.

  NOTE See IEC 62443-2-1 regarding the documentation requirements associated with the risk assessment required to support instances where security measures may affect essential functions.

When reading, specifying and implementing the SRs described in this standard, implementation of security measures should not cause loss of protection, loss of control, loss of view or loss of other essential functions. After a risk analysis, some facilities may determine certain types of security measures may halt continuous operations, but security measures shall not result in loss of protection that could result in health, safety and environmental (HSE) consequences. Some specific constraints include:

- Access Controls (IAC and UC) shall not prevent the operation of essential functions, specifically:
  - Accounts used for essential functions shall not be locked out, even temporarily (see 5.5, SR 1.3 – Account management, 5.6, SR 1.4 – Identifier management, 5.13, SR 1.11 – Unsuccessful login attempts and 6.7, SR 2.5 – Session lock).
  - Verifying and recording operator actions to enforce non-repudiation shall not add significant delay to system response time (see 6.14, SR 2.12 – Non-repudiation).
  - For high availability control systems, the failure of the certificate authority shall not interrupt essential functions (see 5.10, SR 1.8 – Public key infrastructure (PKI) certificates).
  - Identification and authentication shall not prevent the initiation of the SIF (see 5.3, SR 1.1 – Human user identification and authentication and 5.4, SR 1.2 – Software process and device identification and authentication). Similarly for authorization enforcement (see 6.3, SR 2.1 – Authorization enforcement).
  - Incorrectly timestamped audit records (see 6.10, SR 2.8 – Auditable events and 6.13 SR 2.11 – Timestamps) shall not adversely affect essential functions.
- Essential functions of an IACS shall be maintained if zone boundary protection goes into fail-close and/or island mode (see 9.4, SR 5.2 – Zone boundary protection).
- A denial of service (DoS) event on the control system or safety instrumented system (SIS) network shall not prevent the SIF from acting (see 11.3, SR 7.1 – Denial of service protection).

4.3 Compensating countermeasures

Compensating countermeasures, as used in this standard, shall adhere to the guidelines described in IEC 62443-3-2.

Throughout this standard, the SR normative language states that “the control system shall provide the capability to...” support some specific security requirement. The control system shall provide the capability, but it might be performed by an external component. In such a case, the control system shall provide an ‘interface’ to that external component. Some examples of compensating countermeasures include user identification (including centralized versus distributed), password strength enforcement, signature validity checking, security event correlation and device decommissioning (information persistence).

NOTE 1 The control system security requirements detailed in this standard pertain to all technical functions relevant to a control system including tools and applications. However, as noted here, some of these functions can be handled by an external resource.

NOTE 2 In some high resource availability applications (high SL-T(RA,control system)), compensating countermeasures external to the control system (such as additional physical security measures and/or enhanced personnel background checks) will be needed. In these cases, it is possible to see a normally high resource availability SL control system at a lower IAC SL 1 or 2 rating, depending upon the compensating countermeasures. Lockout or loss of control due to security measures is increased, not decreased for very high availability SL control system. Thus higher SLs are not always "better", even where cost is not a significant factor.

4.4 Least privilege

The capability to enforce the concept of least privilege shall be provided, with granularity of permissions and flexibility of mapping those permissions to roles sufficient to support it. Individual accountability should be available when required.

5 FR 1 – Identification and authentication control

5.1 Purpose and SL-C(IAC) descriptions

Identify and authenticate all users (humans, software processes and devices) before allowing them to access to the control system.

- SL 1 – Identify and authenticate all users (humans, software processes and devices) by mechanisms which protect against casual or coincidental access by unauthenticated entities.
- SL 2 – Identify and authenticate all users (humans, software processes and devices) by mechanisms which protect against intentional unauthenticated access by entities using simple means with low resources, generic skills and low motivation.
- SL 3 – Identify and authenticate all users (humans, software processes and devices) by mechanisms which protect against intentional unauthenticated access by entities using sophisticated means with moderate resources, IACS specific skills and moderate motivation.
- SL 4 – Identify and authenticate all users (humans, software processes and devices) by mechanisms which protect against intentional unauthenticated access by entities using sophisticated means with extended resources, IACS specific skills and high motivation.

5.2 Rationale

Asset owners will have to develop a list of all users (humans, software processes and devices) and to determine for each control system component the required level of IAC protection. The goal of IAC is to protect the control system by verifying the identity of any user requesting access to the control system before activating the communication. Recommendations and guidelines should include mechanisms that will operate in mixed modes. For example, some control system components require strong IAC, such as strong authentication mechanisms, and others do not.

5.3 SR 1.1 – Human user identification and authentication

5.3.1 Requirement

The control system shall provide the capability to identify and authenticate all human users. This capability shall enforce such identification and authentication on all interfaces which provide human user access to the control system to support segregation of duties and least privilege in accordance with applicable security policies and procedures.

5.3.2 Rationale and supplemental guidance

All human users need to be identified and authenticated for all access to the control system. Authentication of the identity of these users should be accomplished by using methods such

as passwords, tokens, biometrics or, in the case of multifactor authentication, some combination thereof. The geographic location of human users can also be used as part of the authentication process. This requirement should be applied to both local and remote access to the control system. In addition to identifying and authenticating all human users at the control system level (for example, at system logon), identification and authentication mechanisms are often employed at the application level.

Where human users function as a single group (such as control room operators), user identification and authentication may be role-based or group-based. For some control systems, the capability for immediate operator interaction is critical. It is essential that local emergency actions as well as control system essential functions not be hampered by identification or authentication requirements (see Clause 4 for a more complete discussion). Access to these systems may be restricted by appropriate physical security mechanisms (see IEC 62443-2-1). An example of such a situation is a critical operations room where strict physical access control and monitoring is in place and where shift plans allocate responsibility to a group of users. These users may then be using the same user identity. In addition, the designated operator workstation clients should be authenticated (see 5.4, SR 1.2 – Software process and device identification and authentication) or the use of this shared account should be limited to the constrained environment of the control room.

In order to support IAC policies, as defined according to IEC 62443-2-1, the control system verifies the identity of all human users as a first step. In a second step, the permissions assigned to the identified human user are enforced (see 6.3, SR 2.1 – Authorization enforcement).

5.3.3 Requirement enhancements

5.3.3.1 SR 1.1 RE 1 – Unique identification and authentication

The control system shall provide the capability to uniquely identify and authenticate all human users.

5.3.3.2 SR 1.1 RE 2 – Multifactor authentication for untrusted networks

The control system shall provide the capability to employ multifactor authentication for human user access to the control system via an untrusted network (see 5.15, SR 1.13 – Access via untrusted networks).

NOTE See 5.7.3.5.7.3.1,SR 1.5 – Authenticator management, RE 5.7.3.1 for enhanced authenticator management for software processes.

5.3.3.3 SR 1.1 RE 3 – Multifactor authentication for all networks

The control system shall provide the capability to employ multifactor authentication for all human user access to the control system.

5.3.4 Security levels

The requirements for the four SL levels that relate to SR 1.1 – Human user identification and authentication are:

- SL-C(IAC, control system) 1: SR 1.1
- SL-C(IAC, control system) 2: SR 1.1 (1)
- SL-C(IAC, control system) 3: SR 1.1 (1) (2)
- SL-C(IAC, control system) 4: SR 1.1 (1) (2) (3)

5.4 SR 1.2 – Software process and device identification and authentication

5.4.1 Requirement

The control system shall provide the capability to identify and authenticate all software processes and devices. This capability shall enforce such identification and authentication on all interfaces which provide access to the control system to support least privilege in accordance with applicable security policies and procedures.

5.4.2 Rationale and supplemental guidance

The function of identification and authentication is to map an ID to an unknown software process or device (henceforth referred to an entity in this sub-clause) so as to make it known before allowing any data exchange. Allowing rogue entities to send and receive control system specific data can result in detrimental behavior of the legitimate control system.

All entities need to be identified and authenticated for all access to the control system. Authentication of the identity of such entities should be accomplished by using methods such as passwords, tokens or location (physical or logical). This requirement should be applied to both local and remote access to the control system. However, in some scenarios where individual entities are used to connect to different target systems (for example, remote vendor support), it may be technically infeasible for an entity to have multiple identities. In these cases, compensating countermeasures would have to be applied.

Identification and authentication mechanisms for all entities are needed to protect against attacks such as man-in-the-middle or message spoofing. In some cases, these mechanisms may involve multiple software processes running on the same physical server, each having their own identity. In other cases, the identity may be bound to the physical device, such as all processes running on a given PLC.

Special attention needs to be made when identifying and authenticating portable and mobile devices. These types of devices are a known method of introducing undesired network traffic, malware and/or information exposure to control systems, including otherwise isolated networks.

Where entities function as a single group, identification and authentication may be role-based, group-based or entity-based, it is essential that local emergency actions as well as control system essential functions not be hampered by identification or authentication requirements (see Clause 4 for a more complete discussion). For example, in common protection and control schemes, a group of devices jointly execute the protection functions and communicate with multicast messages among the devices in the group. In these cases, group authentication based on shared accounts or shared symmetric keys are commonly used.

In order to support identification and authentication control policies as defined according to IEC 62443-2-1, the control system verifies the identity of all entities as a first step. In a second step, the permissions assigned to the identified entity are enforced (see 6.3, SR 2.1 – Authorization enforcement).

5.4.3 Requirement enhancements

5.4.3.1 SR 1.2 RE 1 – Unique identification and authentication

The control system shall provide the capability to uniquely identify and authenticate all software processes and devices.

5.4.3.2 Void

5.4.4 Security levels

The requirements for the four SL levels that relate to SR 1.2 – Software process and device identification and authentication are:

- SL-C(IAC, control system) 1: Not Selected
- SL-C(IAC, control system) 2: SR 1.2
- SL-C(IAC, control system) 3: SR 1.2 (1)
- SL-C(IAC, control system) 4: SR 1.2 (1)

5.5 SR 1.3 – Account management

5.5.1 Requirement

The control system shall provide the capability to support the management of all accounts by authorized users, including adding, activating, modifying, disabling and removing accounts.

5.5.2 Rationale and supplemental guidance

Account management may include grouping of accounts (for example, individual, role-based, device-based and control system), establishment of conditions for group membership and assignment of associated authorizations. In certain IACS instances, where individual accounts are determined to be unnecessary from a risk-analysis and/or regulatory aspect, shared accounts are acceptable as long as adequate compensating countermeasures (such as limited physical access or organizational measures for approval) are in place and documented.

Non-human user accounts (sometimes termed service accounts) that are utilized for software process-to-process communication (for example, control server to historian and PLC to control server) typically require different security policies and procedures from human user accounts. For enhanced security, management of accounts should be done according to unified policies and deployed locally in the relevant components of the control system. Unused default system accounts used for the first installation of the system should be removable. Security enhancement lies in the simplification and consistent application of account management.

5.5.3 Requirement enhancements

5.5.3.1 SR 1.3 RE 1 – Unified account management

The control system shall provide the capability to support unified account management.

5.5.3.2 Void

5.5.4 Security levels

The requirements for the four SL levels that relate to SR 1.3 – Account management are:

- SL-C(IAC, control system) 1: SR 1.3
- SL-C(IAC, control system) 2: SR 1.3
- SL-C(IAC, control system) 3: SR 1.3 (1)
- SL-C(IAC, control system) 4: SR 1.3 (1)

5.6 SR 1.4 – Identifier management

5.6.1 Requirement

The control system shall provide the capability to support the management of identifiers by user, group, role or control system interface.

5.6.2 Rationale and supplemental guidance

Identifiers are distinguished from the privileges which they permit an entity to perform within a specific control system control domain or zone (see 6.3, SR 2.1 – Authorization enforcement). Where human users function as a single group (such as control room operators), user identification may be role-based, group-based or device-based. For some control systems, the capability for immediate operator interaction is critical. Local emergency actions for the control system should not be hampered by identification requirements. Access to these systems may be restricted by appropriate compensating countermeasures. Identifiers may be required on portions of the control system but not necessarily the entire control system. For example, wireless devices typically require identifiers, whereas wired devices may not.

The management of identifiers will be determined by local policies and procedures established in compliance with IEC 62443-2-1.

5.6.3 Requirement enhancements

None.

5.6.4 Security levels

The requirements for the four SL levels that relate to SR 1.4 – Identifier management are:

- SL-C(IAC, control system) 1: SR 1.4
- SL-C(IAC, control system) 2: SR 1.4
- SL-C(IAC, control system) 3: SR 1.4
- SL-C(IAC, control system) 4: SR 1.4

5.7 SR 1.5 – Authenticator management

5.7.1 Requirement

The control system shall provide the capability to:

h) initialize authenticator content;

i) change all default authenticators upon control system installation;

j) change/refresh all authenticators; and

k) protect all authenticators from unauthorized disclosure and modification when stored and transmitted.

5.7.2 Rationale and supplemental guidance

In addition to an identifier (see 5.6, SR 1.4 – Identifier management) an authenticator is required to prove identity. Control system authenticators include, but are not limited to, tokens, symmetric keys, private keys (part of a public/private key pair), biometrics, passwords, physical keys and key cards. Human users should take reasonable measures to safeguard authenticators, including maintaining possession of their individual authenticators, not loaning or sharing authenticators with others and reporting lost or compromised authenticators immediately.

Authenticators have a lifecycle. When an account is created automatically a new authenticator needs to be created, in order for the account owner to be able to authenticate. For example,

in a password-based system, the account has a password associated with it. Definition of the initial authenticator content could be interpreted as the administrator defining the initial password which the account management system sets for all new accounts. Being able to configure these initial values makes it harder for an attacker to guess the password between account creation and first account use (which should involve the setting of a new password by the account owner). Some control systems are installed with unattended installers which create all necessary accounts with default passwords and some embedded devices are shipped with default passwords. Over time, these passwords often become general knowledge and are documented on the Internet. Being able to change the default passwords protects the system against unauthorized users using default passwords to gain access. Passwords can be obtained from storage or from transmission when used in network authentication. The complexity of this can be increased by cryptographic protections such as encryption or hashing or by handshake protocols which do not require transmission of the password at all. Still, passwords might be subject to attacks, for example brute force guessing or breaking the cryptographic protection of passwords in transit or storage. The window of opportunity can be reduced by changing/refreshing the passwords periodically. Similar considerations apply to authentication systems based on cryptographic keys. Enhanced protection can be achieved by using hardware mechanisms such as hardware security modules like trusted platform modules (TPMs).

The management of authenticators should be specified in applicable security policies and procedures, for example, constraints to change default authenticators, refresh periods, specification of the protection of authenticators or firecall (see 3.1.24) procedures.

Lockout or loss of control due to security measures is not acceptable. If the control system is required to have a high level of availability, measures should be taken to maintain this high level of availability (such as compensating physical countermeasures, duplicate keys and supervisory override).

Besides the capabilities for authenticator management specified in this requirement, the strength of the authentication mechanism depends on the strength of the chosen authenticator (for example password complexity or key length in public key authentication) and the policies for validating the authenticator in the authentication process (for example how long a password is valid or which checks are performed in public key certificate validation). For the most common authentication mechanisms password-based and public key authentication 5.9, SR 1.7 – Strength of password-based authentication, 5.10, SR 1.8 – Public key infrastructure (PKI) certificates and 5.11, SR 1.9 – Strength of public key authentication provide further requirements.

5.7.3 Requirement enhancements

5.7.3.1 SR 1.5 RE 1 – Hardware security for software process identity credentials

For software process and device users, the control system shall provide the capability to protect the relevant authenticators via hardware mechanisms.

5.7.3.2 Void

5.7.4 Security levels

The requirements for the four SL levels that relate to SR 1.5 – Authenticator management are:

- SL-C(IAC, control system) 1: SR 1.5
- SL-C(IAC, control system) 2: SR 1.5
- SL-C(IAC, control system) 3: SR 1.5 (1)
- SL-C(IAC, control system) 4: SR 1.5 (1)

5.8 SR 1.6 – Wireless access management

5.8.1 Requirement

The control system shall provide the capability to identify and authenticate all users (humans, software processes or devices) engaged in wireless communication.

5.8.2 Rationale and supplemental guidance

Any wireless technology can, and in most cases should, be considered just another communication protocol option, and thus subject to the same IACS security requirements as any other communication type utilized by the IACS. However, from a security point of view, there is at least one significant difference between wired and wireless communications: physical security countermeasures are typically less effective when using wireless. For this and possibly other reasons (for example regulatory differences), a risk analysis might legitimately result in a higher SL-T(IAC,control system) for wireless communications versus a wired protocol being used in an identical use case.

Wireless technologies include, but are not limited to, microwave, satellite, packet radio, Institute of Electrical and Electronics Engineers (IEEE) 802.11x, IEEE 802.15.4 (ZigBee, IEC 62591 – *Wireless*HART®, ISA-100.11a), IEEE 802.15.1 (Bluetooth), wireless LAN mobile routers, mobile phones with tethering and various infrared technologies.

5.8.3 Requirement enhancements

5.8.3.1 SR 1.6 RE 1 – Unique identification and authentication

The control system shall provide the capability to uniquely identify and authenticate all users (humans, software processes or devices) engaged in wireless communication.

5.8.3.2 Void

5.8.4 Security levels

The requirements for the four SL levels that relate to SR 1.6 – Wireless access management are:

- SL-C(IAC, control system) 1: SR 1.6
- SL-C(IAC, control system) 2: SR 1.6 (1)
- SL-C(IAC, control system) 3: SR 1.6 (1)
- SL-C(IAC, control system) 4: SR 1.6 (1)

5.9 SR 1.7 – Strength of password-based authentication

5.9.1 Requirement

For control systems utilizing password-based authentication, the control system shall provide the capability to enforce configurable password strength based on minimum length and variety of character types.

5.9.2 Rationale and supplemental guidance

User authentication based on a username and a secret password is a very commonly used mechanism. Many attacks on such mechanisms focus on guessing the password (for example, dictionary attacks or targeted social engineering) or breaking the cryptographic protection of the stored password representation (for example, using rainbow tables or brute-forcing a hash collision).

Increasing the size of the set of valid passwords by increasing the number of allowed characters makes such attacks more complex, but only if the increased set size is actually

used (generally users would tend to not include special characters in a password as they are perceived as harder to remember). Limiting the lifetime of a password decreases the window of opportunity for an attacker to breach a given password's secrecy. In order to prevent users from circumventing this control by once changing their password to a new one and then immediately changing back to their original password, a minimum lifetime for a password is commonly enforced as well. A notification to change the password prior the expiration allows the user to change the password at a convenient time according to process operations conditions.

This protection can be further enhanced by limiting the reuse of passwords (preventing small sets of alternating passwords), which further decreases the usefulness of a once-breached password. Extended protection beyond password based mechanisms can be achieved using multifactor authentication (see 5.3, SR 1.1 – Human user identification and authentication and 5.4, SR 1.2 – Software process and device identification and authentication).

5.9.3 Requirement enhancements

5.9.3.1 SR 1.7 RE 1 – Password generation and lifetime restrictions for human users

The control system shall provide the capability to prevent any given human user account from reusing a password for a configurable number of generations. In addition, the control system shall provide the capability to enforce password minimum and maximum lifetime restrictions for human users. These capabilities shall conform with commonly accepted security industry practices.

NOTE It is a commonly accepted good practice that the control system provides the capability to prompt the user to change his password upon a configurable time prior to expiration.

5.9.3.2 SR 1.7 RE 2 – Password lifetime restrictions for all users

The control system shall provide the capability to enforce password minimum and maximum lifetime restrictions for all users.

5.9.4 Security levels

The requirements for the four SL levels that relate to SR 1.7 – Strength of password-based authentication are:

- SL-C(IAC, control system) 1: SR 1.7
- SL-C(IAC, control system) 2: SR 1.7
- SL-C(IAC, control system) 3: SR 1.7 (1)
- SL-C(IAC, control system) 4: SR 1.7 (1) (2)

5.10 SR 1.8 – Public key infrastructure (PKI) certificates

5.10.1 Requirement

Where PKI is utilized, the control system shall provide the capability to operate a PKI according to commonly accepted best practices or obtain public key certificates from an existing PKI.

5.10.2 Rationale and supplemental guidance

Registration to receive a public key certificate needs to include authorization by a supervisor or a responsible official and needs to be accomplished using a secure process that verifies the identity of the certificate holder and ensures that the certificate is issued to the intended party. Any latency induced from the use of public key certificates should not degrade the operational performance of the control system.

The selection of an appropriate PKI should consider the organization's certificate policy which should be based on the risk associated with a breach of confidentiality of the protected

information. Guidance on the policy definition can be found in commonly accepted standards and guidelines, such as the Internet Engineering Task Force (IETF) Request for Comment (RFC) 3647 [29] for X.509-based PKI. For example, the appropriate location of a certification authority (CA), whether within the control system versus on the Internet, and the list of trusted CAs should be considered in the policy and depends on the network architecture (see also IEC 62443-2-1).

5.10.3 Requirement enhancements

None.

5.10.4 Security levels

The requirements for the four SL levels that relate to SR 1.8 – Public key infrastructure (PKI) certificates are:

- SL-C(IAC, control system) 1: Not Selected
- SL-C(IAC, control system) 2: SR 1.8
- SL-C(IAC, control system) 3: SR 1.8
- SL-C(IAC, control system) 4: SR 1.8

5.11 SR 1.9 – Strength of public key authentication

5.11.1 Requirement

For control systems utilizing public key authentication, the control system shall provide the capability to:

l) validate certificates by checking the validity of the signature of a given certificate;

m) validate certificates by constructing a certification path to an accepted CA or in the case of self-signed certificates by deploying leaf certificates to all hosts which communicate with the subject to which the certificate is issued;

n) validate certificates by checking a given certificate's revocation status;

o) establish user (human, software process or device) control of the corresponding private key; and

p) map the authenticated identity to a user (human, software process or device).

5.11.2 Rationale and supplemental guidance

Public/private key cryptography strongly depends on the secrecy of a given subject's private key and proper handling of the trust relationships. When verifying a trust between two entities based on public key authentication, it is essential to trace the public key certificate to a trusted entity. A common implementation error in certificate validation is to only check the validity of a certificate's signature, but not checking the trust in the signer. In a PKI setting, a signer is trusted if they are a trusted CA or have a certificate issued by a trusted CA, thus all verifiers need to trace certificates presented to them back to a trusted CA. If such a chain of trusted CAs cannot be established, the presented certificate should not be trusted.

If self-signed certificates are used instead of a PKI, the certificate subject itself signed its certificate, thus there never is a trusted third-party or CA. This should be compensated by deploying the self-signed public key certificates to all peers that need to validate them via an otherwise secured mechanism (for example, configuration of all peers in a trusted environment). Trusted certificates need to be distributed to peers through secure channels. During the validation process, a self-signed certificate should only be trusted if it is already present in the list of trusted certificates of the validating peer. The set of trusted certificates should be configured to the minimum necessary set.

In both cases, validation needs to also consider the possibility that a certificate is revoked. In a PKI setting this is typically done by maintaining certificate revocation lists (CRLs) or running an online certificate status protocol (OCSP) server. When revocation checking is not available due to control system constraints, mechanisms such as a short certificate lifetime can compensate for the lack of timely revocation information. Note that short lifetime certificates can sometimes create significant operational issues in a control system environment.

5.11.3 Requirement enhancements

5.11.3.1 SR 1.9 RE 1 – Hardware security for public key authentication

The control system shall provide the capability to protect the relevant private keys via hardware mechanisms according to commonly accepted security industry practices and recommendations.

5.11.3.2 Void

5.11.4 Security levels

The requirements for the four SL levels that relate to SR 1.9 – Strength of public key authentication are:

- SL-C(IAC, control system) 1: Not Selected
- SL-C(IAC, control system) 2: SR 1.9
- SL-C(IAC, control system) 3: SR 1.9 (1)
- SL-C(IAC, control system) 4: SR 1.9 (1)

5.12 SR 1.10 – Authenticator feedback

5.12.1 Requirement

The control system shall provide the capability to obscure feedback of authentication information during the authentication process.

5.12.2 Rationale and supplemental guidance

Obscuring feedback protects the information from possible exploitation by unauthorized individuals, for example, displaying asterisks or other random characters when a human user types in a password obscures feedback of authentication information. Other examples include the entry of wired equivalent privacy (WEP) keys, secure socket shell (SSH) token entry and RSA one-time passwords. The authenticating entity should not provide any hint as to the reason for the authentication failure, such as “unknown user name”.

5.12.3 Requirement enhancements

None.

5.12.4 Security levels

The requirements for the four SL levels that relate to SR 1.10 – Authenticator feedback are:

- SL-C(IAC, control system) 1: SR 1.10
- SL-C(IAC, control system) 2: SR 1.10
- SL-C(IAC, control system) 3: SR 1.10
- SL-C(IAC, control system) 4: SR 1.10

5.13 SR 1.11 – Unsuccessful login attempts

5.13.1 Requirement

The control system shall provide the capability to enforce a limit of a configurable number of consecutive invalid access attempts by any user (human, software process or device) during a configurable time period. The control system shall provide the capability to deny access for a specified period of time or until unlocked by an administrator when this limit has been exceeded.

For system accounts on behalf of which critical services or servers are run, the control system shall provide the capability to disallow interactive logons.

5.13.2 Rationale and supplemental guidance

Due to the potential for denial of service, the number of consecutive invalid access attempts may be limited. If enabled, the control system may automatically reset to zero the number of access attempts after a predetermined time period established by the applicable security policies and procedures. Resetting the access attempts to zero will allow users (human, software process or device) to gain access if they have the correct login identifier. Automatic denial of access for control system operator workstations or nodes should not be used when immediate operator responses are required in emergency situations. All lockout mechanisms should consider functional requirements for continuous operations so as to mitigate adverse denial of service operating conditions which could result in total system failure or injury to personnel. Allowing interactive logins to an account used for critical services could provide a potential for denial of service or other abuse.

5.13.3 Requirement enhancements

None.

5.13.4 Security levels

The requirements for the four SL levels that relate to SR 1.11 – Unsuccessful login attempts are:

- SL-C(IAC, control system) 1: SR 1.11
- SL-C(IAC, control system) 2: SR 1.11
- SL-C(IAC, control system) 3: SR 1.11
- SL-C(IAC, control system) 4: SR 1.11

5.14 SR 1.12 – System use notification

5.14.1 Requirement

The control system shall provide the capability to display a system use notification message before authenticating. The system use notification message shall be configurable by authorized personnel.

5.14.2 Rationale and supplemental guidance

Privacy and security policies and procedures need to be consistent with applicable laws, directives, policies, regulations, standards and guidance. Often the main justification for this requirement is legal prosecution of violators and proving intentional breach. This capability is thus necessary to support policy requirements, and does not improve IACS security. System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the control system. A warning banner implemented as a posted physical notice in the control system facility does not protect against remote login issues.

Examples of elements for inclusion in the system use notification message are:

a) that the individual is accessing a specific control system;

b) that system usage may be monitored, recorded and subject to audit;

c) that unauthorized use of the system is prohibited and subject to criminal and/or civil penalties; and

d) that use of the system indicates consent to monitoring and recording.

5.14.3 Requirement enhancements

None.

5.14.4 Security levels

The requirements for the four SL levels that relate to SR 1.12 – System use notification are:

- SL-C(IAC, control system) 1: SR 1.12
- SL-C(IAC, control system) 2: SR 1.12
- SL-C(IAC, control system) 3: SR 1.12
- SL-C(IAC, control system) 4: SR 1.12

5.15 SR 1.13 – Access via untrusted networks

5.15.1 Requirement

The control system shall provide the capability to monitor and control all methods of access to the control system via untrusted networks.

5.15.2 Rationale and supplemental guidance

Examples of access to the control system via untrusted networks typically include remote access methods (such as dial-up, broadband and wireless) as well as connections from a company's office (non-control system) network. The control system should restrict access achieved through dial-up connections (for example, limiting dial-up access based upon the source of the request) or protect against unauthorized connections or subversion of authorized connections (for example, using virtual private network technology). Access via untrusted networks to geographically remote control system component locations (for example, control centres and field locations) should only be enabled when necessary and authenticated. Security policies and procedures may require multifactor authentication for remote user access to the control system.

5.15.3 Requirement enhancements

5.15.3.1 SR 1.13 RE 1 – Explicit access request approval

The control system shall provide the capability to deny access requests via untrusted networks unless approved by an assigned role.

5.15.3.2 Void

5.15.4 Security levels

The requirements for the four SL levels that relate to SR 1.13 – Access via untrusted networks are:

- SL-C(IAC, control system) 1: SR 1.13
- SL-C(IAC, control system) 2: SR 1.13 (1)
- SL-C(IAC, control system) 3: SR 1.13 (1)
- SL-C(IAC, control system) 4: SR 1.13 (1)

6 FR 2 – Use control

6.1 Purpose and SL-C(UC) descriptions

Enforce the assigned privileges of an authenticated user (human, software process or device) to perform the requested action on the IACS and monitor the use of these privileges.

- SL 1 – Restrict use of the IACS according to specified privileges to protect against casual or coincidental misuse.
- SL 2 – Restrict use of the IACS according to specified privileges to protect against circumvention by entities using simple means with low resources, generic skills and low motivation.
- SL 3 – Restrict use of the IACS according to specified privileges to protect against circumvention by entities using sophisticated means with moderate resources, IACS specific skills and moderate motivation.
- SL 4 – Restrict use of the IACS according to specified privileges to protect against circumvention by entities using sophisticated means with extended resources, IACS specific skills and high motivation.

6.2 Rationale

Once the user is identified and authenticated, the control system has to restrict the allowed actions to the authorized use of the control system. Asset owners and system integrators will have to assign, to each user (human, software process or device), group, role, etc. (see 5.6, SR 1.4 – Identifier management) the privileges defining the authorized use of the IACS. The goal of use control is to protect against unauthorized actions on the control system resources by verifying that the necessary privileges have been granted before allowing a user to perform the actions. Examples of actions are reading or writing data, downloading programs and setting configurations. Recommendations and guidelines should include mechanisms that will operate in mixed modes. For example, some control system resources require strong use control protection, such as restrictive privileges, and others do not. By extension, use control requirements need to be extended to data at rest. User privileges may vary based on time-of-day/date, location and means by which access is made.

6.3 SR 2.1 – Authorization enforcement

6.3.1 Requirement

On all interfaces, the control system shall provide the capability to enforce authorizations assigned to all human users for controlling use of the control system to support segregation of duties and least privilege.

6.3.2 Rationale and supplemental guidance

Use control policies (for example, identity-based policies, role-based policies and rule-based policies) and associated read/write access enforcement mechanisms (for example, access control lists, access control matrices and cryptography) are employed to control usage between users (humans, software processes and devices) and assets (for example, devices, files, records, software processes, programs and domains).

After the control system has verified the identity of a user (human, software process or device) (see 5.3, SR 1.1 – Human user identification and authentication and 5.4, SR 1.2 – Software process and device identification and authentication), it also has to verify that a requested operation is actually permitted according to the defined security policies and procedures. For example, in a role-based access control policy, the control system would check which roles are assigned to a verified user or asset and which privileges are assigned to these roles – if the requested operation is covered by the permissions, it is executed, otherwise rejected. This allows the enforcement of segregation of duties and least privileges. Usage enforcement mechanisms should not be allowed to adversely affect the operational performance of the control system.

Planned or unplanned changes to control system components can have significant effects on the overall security of the control system. Accordingly, only qualified and authorized individuals should obtain the use of control system components for purposes of initiating changes, including upgrades and modifications.

6.3.3 Requirement enhancements

6.3.3.1 SR 2.1 RE 1 – Authorization enforcement for all users

On all interfaces, the control system shall provide the capability to enforce authorizations assigned to all users (humans, software processes and devices) for controlling use of the control system to support segregation of duties and least privilege.

6.3.3.2 SR 2.1 RE 2 – Permission mapping to roles

The control system shall provide the capability for an authorized user or role to define and modify the mapping of permissions to roles for all human users.

NOTE 1 It is a commonly accepted good practice to not limit roles to fixed nested hierarchies in which a higher level role is a superset of a lesser privileged role. For example, a system administrator generally does not necessarily encompass operator privileges.

NOTE 2 This RE is applicable to software processes and devices as well.

6.3.3.3 SR 2.1 RE 3 – Supervisor override

The control system shall support supervisor manual override of the current human user authorizations for a configurable time or event sequence.

NOTE Implementation of a controlled, audited and manual override of automated mechanisms in the event of emergencies or other serious events is often needed. This allows a supervisor to enable an operator to quickly react to unusual conditions without closing the current session and establishing a new session as a higher privilege human user.

6.3.3.4 SR 2.1 RE 4 – Dual approval

The control system shall support dual approval where an action can result in serious impact on the industrial process.

NOTE It is a commonly accepted good practice to limit dual approval to actions which require a very high level of confidence that they will be performed reliably and correctly. Requiring dual approval provides emphasis to the seriousness of consequences that would result from failure of a correct action. An example of a situation in which dual approval is required would be a change to a set point of a critical industrial process. It is a commonly accepted good practice to not employ dual approval mechanisms when an immediate response is necessary to safeguard HSE consequences, for example, emergency shutdown of an industrial process.

6.3.4 Security levels

The requirements for the four SL levels that relate to SR 2.1 – Authorization enforcement are:

- SL-C(UC, control system) 1: SR 2.1
- SL-C(UC, control system) 2: SR 2.1 (1) (2)
- SL-C(UC, control system) 3: SR 2.1 (1) (2) (3)
- SL-C(UC, control system) 4: SR 2.1 (1) (2) (3) (4)

6.4 SR 2.2 – Wireless use control

6.4.1 Requirement

The control system shall provide the capability to authorize, monitor and enforce usage restrictions for wireless connectivity to the control system according to commonly accepted security industry practices.

6.4.2 Rationale and supplemental guidance

Any wireless technology can, and in most cases should, be considered just another communication protocol option, and thus subject to the same IACS security requirements as any other communication type utilized by the IACS. However, a risk analysis may result in a requirement for wireless IACS components to support higher use control capabilities than are typically required of wired systems for the same use case and SL-T. Regulatory differences may also result in different required capabilities between wired and wireless communications.

As noted in 5.8, SR 1.6 – Wireless access management, wireless technologies include, but are not limited to, microwave, satellite, packet radio, IEEE 802.11x, IEEE 802.15.4 (ZigBee, IEC 62591 – *Wireless*HART®, ISA-100.11a), IEEE 802.15.1 (Bluetooth), wireless LAN mobile routers, mobile phones with tethering and various infrared technologies.

6.4.3 Requirement enhancements

6.4.3.1 SR 2.2 RE 1 – Identify and report unauthorized wireless devices

The control system shall provide the capability to identify and report unauthorized wireless devices transmitting within the control system physical environment.

6.4.3.2 Void

6.4.4 Security levels

The requirements for the four SL levels that relate to SR 2.2 – Wireless use control are:

- SL-C(UC, control system) 1: SR 2.2
- SL-C(UC, control system) 2: SR 2.2
- SL-C(UC, control system) 3: SR 2.2 (1)
- SL-C(UC, control system) 4: SR 2.2 (1)

6.5 SR 2.3 – Use control for portable and mobile devices

6.5.1 Requirement

The control system shall provide the capability to automatically enforce configurable usage restrictions that include:

a) preventing the use of portable and mobile devices;

b) requiring context specific authorization; and

c) restricting code and data transfer to/from portable and mobile devices.

6.5.2 Rationale and supplemental guidance

Portable and mobile devices may introduce undesired network traffic, malware and/or information exposure, so there should be specific control associated with their usage in the typical control system environment. Security policies and procedures may not allow certain functions or activities via portable and/or mobile devices. Refer to IEC 62443-2-1 for guidance on when and where portable and mobile devices usage should be permitted.

Protecting information residing on portable and mobile devices (for example, employing cryptographic mechanisms to provide confidentiality and integrity protections during storage and while in transit when outside of controlled areas) is covered elsewhere (see Clause 8, FR 4 – Data confidentiality).

6.5.3 Requirement enhancements

6.5.3.1 SR 2.3 RE 1 – Enforcement of security status of portable and mobile devices

The control system shall provide the capability to verify that portable or mobile devices attempting to connect to a zone comply with the security requirements of that zone.

6.5.3.2 Void

6.5.4 Security levels

The requirements for the four SL levels that relate to SR 2.3 – Use control for portable and mobile devices are:

- SL-C(UC, control system) 1: SR 2.3
- SL-C(UC, control system) 2: SR 2.3
- SL-C(UC, control system) 3: SR 2.3 (1)
- SL-C(UC, control system) 4: SR 2.3 (1)

6.6 SR 2.4 – Mobile code

6.6.1 Requirement

The control system shall provide the capability to enforce usage restrictions for mobile code technologies based on the potential to cause damage to the control system that include:

a) preventing the execution of mobile code;

b) requiring proper authentication and authorization for origin of the code;

c) restricting mobile code transfer to/from the control system; and

d) monitoring the use of mobile code.

6.6.2 Rationale and supplemental guidance

Mobile code technologies include, but are not limited to, Java, JavaScript, ActiveX, portable document format (PDF), Postscript, Shockwave movies, Flash animations and VBScript. Usage restrictions apply to both the selection and use of mobile code installed on servers and mobile code downloaded and executed on individual workstations. Control procedures should prevent the development, acquisition or introduction of unacceptable mobile code within the control system. For example, mobile code exchanges may be disallowed directly with the control system, but may be allowed in a controlled adjacent environment maintained by IACS personnel.

6.6.3 Requirement enhancements

6.6.3.1 SR 2.4 RE 1 – Mobile code integrity check

The control system shall provide the capability to verify integrity of the mobile code before allowing code execution.

6.6.3.2 Void

6.6.4 Security levels

The requirements for the four SL levels that relate to SR 2.4 – Mobile code are:

- SL-C(UC, control system) 1: SR 2.4
- SL-C(UC, control system) 2: SR 2.4
- SL-C(UC, control system) 3: SR 2.4 (1)

- SL-C(UC, control system) 4: SR 2.4 (1)

6.7 SR 2.5 – Session lock

6.7.1 Requirement

The control system shall provide the capability to prevent further access by initiating a session lock after a configurable time period of inactivity or by manual initiation. The session lock shall remain in effect until the human user who owns the session or another authorized human user re-establishes access using appropriate identification and authentication procedures.

6.7.2 Rationale and supplemental guidance

The entity responsible for a control system should employ session lock to prevent access to specified workstations or nodes. The control system should activate session lock mechanisms automatically after a configurable time period for designated workstations or nodes. In some cases, session lock for control system operator workstations or nodes is not advised (for example, sessions which are required for immediate operator responses in emergency situations). Session locks are not a substitute for logging out of the control system. In situations where the control system cannot support session lock, the responsible entity should employ appropriate compensating countermeasures (for example, providing increased physical security, personnel security and auditing measures).

6.7.3 Requirement enhancements

None.

6.7.4 Security levels

The requirements for the four SL levels that relate to SR 2.5 – Session lock are:

- SL-C(UC, control system) 1: SR 2.5
- SL-C(UC, control system) 2: SR 2.5
- SL-C(UC, control system) 3: SR 2.5
- SL-C(UC, control system) 4: SR 2.5

6.8 SR 2.6 – Remote session termination

6.8.1 Requirement

The control system shall provide the capability to terminate a remote session either automatically after a configurable time period of inactivity or manually by the user who initiated the session.

6.8.2 Rationale and supplemental guidance

A remote session is initiated whenever a control system is accessed across the boundary of a zone defined by the asset owner based on their risk assessment. This requirement may be limited to sessions that are used for control system monitoring and maintenance activities (not critical operations) based on the risk assessment of the control system and security policies and procedures. Some control systems or components may not allow sessions to be terminated.

6.8.3 Requirement enhancements

None.

6.8.4 Security levels

The requirements for the four SL levels that relate to SR 2.6 – Remote session termination are:

- SL-C(UC, control system) 1: Not Selected
- SL-C(UC, control system) 2: SR 2.6
- SL-C(UC, control system) 3: SR 2.6
- SL-C(UC, control system) 4: SR 2.6

6.9 SR 2.7 – Concurrent session control

6.9.1 Requirement

The control system shall provide the capability to limit the number of concurrent sessions per interface for any given user (human, software process or device) to a configurable number of sessions.

6.9.2 Rationale and supplemental guidance

A resource starvation DoS might occur if a limit is not imposed. There is a trade-off between potentially locking out a specific user versus locking out all users and services due to a lack of control system resources. Product supplier and/or system integrator guidance is likely required to provide sufficient information as to how the number of sessions value should be assigned.

6.9.3 Requirement enhancements

None.

6.9.4 Security levels

The requirements for the four SL levels that relate to SR 2.7 – Concurrent session control are:

- SL-C(UC, control system) 1: Not Selected
- SL-C(UC, control system) 2: Not Selected
- SL-C(UC, control system) 3: SR 2.7
- SL-C(UC, control system) 4: SR 2.7

6.10 SR 2.8 – Auditable events

6.10.1 Requirement

The control system shall provide the capability to generate audit records relevant to security for the following categories: access control, request errors, operating system events, control system events, backup and restore events, configuration changes, potential reconnaissance activity and audit log events. Individual audit records shall include the timestamp, source (originating device, software process or human user account), category, type, event ID and event result.

6.10.2 Rationale and supplemental guidance

The purpose of this requirement is to record the occurrence of important events which need to be audited as significant and relevant to the security of the control system. Auditing activity can affect control system performance. The security audit function is usually coordinated with the network health and status monitoring function which may be in a different zone. Commonly recognized and accepted checklists and configuration guides should be considered when compiling a list of auditable events. The security policies and procedures should define auditable events that are adequate to support after-the-fact investigations of

security incidents. In addition, audit records should be sufficient to monitor the effectiveness and proper operation of the security mechanisms utilized to meet the requirements in this standard.

It should be noted that the requirement for event recording is applicable within the given system functionality, specifically given system security requirements on a given level. For example, the requirement for recording of authentication events (in the access control category) on a SL 1 system is only applicable to the level of authentication functionality required for SL 1 according to the requirements in Clause 5. Events may occur in any control system component (for example login events) or may be observed by dedicated monitors. For example, port scanning might be detected by an intrusion detection system (IDS) or intrusion prevention system (IPS).

6.10.3 Requirement enhancements

6.10.3.1 SR 2.8 RE 1 – Centrally managed, system-wide audit trail

The control system shall provide the capability to centrally manage audit events and to compile audit records from multiple components throughout the control system into a system-wide (logical or physical), time-correlated audit trail. The control system shall provide the capability to export these audit records in industry standard formats for analysis by standard commercial log analysis tools, for example, security information and event management (SIEM).

6.10.3.2 Void

6.10.4 Security levels

The requirements for the four SL levels that relate to SR 2.8 – Auditable events are:

- SL-C(UC, control system) 1: SR 2.8
- SL-C(UC, control system) 2: SR 2.8
- SL-C(UC, control system) 3: SR 2.8 (1)
- SL-C(UC, control system) 4: SR 2.8 (1)

6.11 SR 2.9 – Audit storage capacity

6.11.1 Requirement

The control system shall allocate sufficient audit record storage capacity according to commonly recognized recommendations for log management and system configuration. The control system shall provide auditing mechanisms to reduce the likelihood of such capacity being exceeded.

6.11.2 Rationale and supplemental guidance

The control system should provide sufficient audit storage capacity, taking into account retention policy, the auditing to be performed and the online audit processing requirements. Guidelines to be considered could include the NIST Special Publication (SP) 800-92 [27]. The audit storage capacity should be sufficient to retain logs for a period of time required by applicable policies and regulations or business requirements.

6.11.3 Requirement enhancements

6.11.3.1 SR 2.9 RE 1 – Warn when audit record storage capacity threshold reached

The control system shall provide the capability to issue a warning when the allocated audit record storage volume reaches a configurable percentage of maximum audit record storage capacity.

6.11.3.2 Void

6.11.4 Security levels

The requirements for the four SL levels that relate to SR 2.9 – Audit storage capacity are:

- SL-C(UC, control system) 1: SR 2.9
- SL-C(UC, control system) 2: SR 2.9
- SL-C(UC, control system) 3: SR 2.9 (1)
- SL-C(UC, control system) 4: SR 2.9 (1)

6.12 SR 2.10 – Response to audit processing failures

6.12.1 Requirement

The control system shall provide the capability to alert personnel and prevent the loss of essential services and functions in the event of an audit processing failure. The control system shall provide the capability to support appropriate actions in response to an audit processing failure according to commonly accepted industry practices and recommendations.

6.12.2 Rationale and supplemental guidance

Audit generation typically occurs at the source of the event. Audit processing involves transmission, possible augmentation (such as the addition of a timestamp) and persistent storage of the audit records. Audit processing failures include, for example, software or hardware errors, failures in the audit capturing mechanisms and audit storage capacity being reached or exceeded. Guidelines to be considered when designing appropriate response actions may include the NIST SP800-92. It should be noted that either overwriting the oldest audit records or halting audit log generation are possible responses to audit storage capacity being exceeded but imply the loss of potentially essential forensic information.

6.12.3 Requirement enhancements

None.

6.12.4 Security levels

The requirements for the four SL levels that relate to SR 2.10 – Response to audit processing failures are:

- SL-C(UC, control system) 1: SR 2.10
- SL-C(UC, control system) 2: SR 2.10
- SL-C(UC, control system) 3: SR 2.10
- SL-C(UC, control system) 4: SR 2.10

6.13 SR 2.11 – Timestamps

6.13.1 Requirement

The control system shall provide timestamps for use in audit record generation.

6.13.2 Rationale and supplemental guidance

Timestamps (including date and time) of audit records should be generated using internal system clocks. If system-wide time synchronization is not present (which is typical in many installations), known offsets would be needed to support analysis of a sequence of events. In addition, synchronization of internally generated audit records with external events might require synchronization with a generally recognized external time source (such as the Global

Positioning System (GPS), Global Navigation Satellite System (GLONASS) and Galileo). The time source should be protected from unauthorized alteration.

6.13.3 Requirement enhancements

6.13.3.1 SR 2.11 RE 1 – Internal time synchronization

The control system shall provide the capability to synchronize internal system clocks at a configurable frequency.

6.13.3.2 SR 2.11 RE 2 – Protection of time source integrity

The time source shall be protected from unauthorized alteration and shall cause an audit event upon alteration.

6.13.4 Security levels

The requirements for the four SL levels that relate to SR 2.11 – Timestamps are:

- SL-C(UC, control system) 1: Not selected
- SL-C(UC, control system) 2: SR 2.11
- SL-C(UC, control system) 3: SR 2.11 (1)
- SL-C(UC, control system) 4: SR 2.11 (1) (2)

6.14 SR 2.12 – Non-repudiation

6.14.1 Requirement

The control system shall provide the capability to determine whether a given human user took a particular action.

6.14.2 Rationale and supplemental guidance

Examples of particular actions taken by a user include performing operator actions, changing control system configurations, creating information, sending a message, approving information (such as indicating concurrence) and receiving a message. Non-repudiation protects against later false claims by a user of not having taken a specific action, by an author of not having authored a particular document, by a sender of not having transmitted a message, by a receiver of not having received a message or by a signatory of not having signed a document. Non-repudiation services can be used to determine if information originated from a user, if a user took specific actions (for example, sending an email and approving a work order) or received specific information. Non-repudiation services are obtained by employing various techniques or mechanisms (for example, digital signatures, digital message receipts and timestamps).

6.14.3 Requirement enhancements

6.14.3.1 SR 2.12 RE 1 – Non-repudiation for all users

The control system shall provide the capability to determine whether a given user (human, software process or device) took a particular action.

6.14.3.2 Void

6.14.4 Security levels

The requirements for the four SL levels that relate to SR 2.12 – Non-repudiation are:

- SL-C(UC, control system) 1: Not Selected
- SL-C(UC, control system) 2: Not Selected

- SL-C(UC, control system) 3: SR 2.12
- SL-C(UC, control system) 4: SR 2.12 (1)

7 FR 3 – System integrity

7.1 Purpose and SL-C(SI) descriptions

Ensure the integrity of the IACS to prevent unauthorized manipulation.

- SL 1 – Protect the integrity of the IACS against casual or coincidental manipulation.
- SL 2 – Protect the integrity of the IACS against manipulation by someone using simple means with low resources, generic skills and low motivation.
- SL 3 – Protect the integrity of the IACS against manipulation by someone using sophisticated means with moderate resources, IACS specific skills and moderate motivation.
- SL 4 – Protect the integrity of the IACS against manipulation by someone using sophisticated means with extended resources, IACS specific skills and high motivation.

7.2 Rationale

IACS often go through multiple testing cycles (unit testing, factory acceptance testing (FAT), site acceptance testing (SAT), certification, commissioning, etc.) to establish that the systems will perform as intended before they even begin production. Once operational, asset owners are responsible for maintaining the integrity of the IACS. Using their risk assessment methodology, asset owners may assign different levels of integrity protection to different systems, communication channels and information in their IACS. The integrity of physical assets should be maintained in both operational and non-operational states, such as during production, when in storage or during a maintenance shutdown. The integrity of logical assets should be maintained while in transit and at rest, such as being transmitted over a network or when residing in a data repository.

7.3 SR 3.1 – Communication integrity

7.3.1 Requirement

The control system shall provide the capability to protect the integrity of transmitted information.

7.3.2 Rationale and supplemental guidance

Many common network attacks are based on the manipulation of data in transmission, for example manipulation of network packets. Switched or routed networks provide a greater opportunity for attackers to manipulate packets as undetected access to these networks is generally easier and the switching and routing mechanisms themselves can also be manipulated in order to get more access to transmitted information. Manipulation in the context of a control system could include the change of measurement values communicated from a sensor to a receiver or the alteration of command parameters sent from a control application to an actuator.

Depending on the context (for example transmission within a local network segment versus transmission via untrusted networks) and the network type used in the transmission (for example transmission control protocol (TCP) / internet protocol (IP) versus local serial links), feasible and appropriate mechanisms will vary. On a small network with direct links (point-to-point), physical access protection to all nodes may be sufficient on lower SLs if the endpoints' integrity is protected as well (see 7.6, SR 3.4 – Software and information integrity), while on a network distributed in areas with regular physical presence of staff or on a wide area network physical access is likely not enforceable. If a commercial service is used to provide communication services as a commodity item rather than a fully dedicated service (for example a leased line versus a T1 link), it may be more difficult to obtain the necessary

assurances regarding the implementation of needed security controls for communication integrity (for example because of legal restrictions). When it is infeasible or impractical to meet the necessary security requirements it may be appropriate to implement either appropriate compensating countermeasures or explicitly accept the additional risk.

Industrial equipment is often subject to environmental conditions that can lead to integrity issues and/or false positive incidents. Many times the environment contains particulates, liquids, vibration, gases, radiation, and electromagnetic interference (EMI) that can cause conditions that affect the integrity of the communication wiring and signals. The network infrastructure should be designed to minimize these physical/environmental effects on communication integrity. For example, when particulate, liquids, and/or gases are an issue, it may be necessary to use a sealed registered jack 45 (RJ-45) or M12 connector instead of a commercial-grade RJ-45 connector on the wire. The cable itself may need to use a different jacket instead to handle the particulate, liquid, and/or gas as well. In cases where vibration is an issue, M12 connectors may be necessary to prevent the spring pins on an RJ-45 connector from disconnecting during use. In cases where radiation and/or EMI are an issue, it may be necessary to use shielded twisted pair or fiber cables to prevent any effect on the communication signals. It may also be necessary to perform a wireless spectrum analysis in these areas if wireless networking is planned to verify that it is a viable solution.

7.3.3 Requirement enhancements

7.3.3.1 SR 3.1 RE 1 – Cryptographic integrity protection

The control system shall provide the capability to employ cryptographic mechanisms to recognize changes to information during communication.

NOTE It is a commonly accepted good practice to determine the appropriate use of cryptographic mechanisms for message authentication and integrity after careful consideration of the security needs and the potential ramifications on system performance and capability to recover from system failure.

7.3.3.2 Void

7.3.4 Security levels

The requirements for the four SL levels that relate to SR 3.1 – Communication integrity are:

- SL-C(SI, control system) 1: SR 3.1
- SL-C(SI, control system) 2: SR 3.1
- SL-C(SI, control system) 3: SR 3.1 (1)
- SL-C(SI, control system) 4: SR 3.1 (1)

7.4 SR 3.2 – Malicious code protection

7.4.1 Requirement

The control system shall provide the capability to employ protection mechanisms to prevent, detect, report and mitigate the effects of malicious code or unauthorized software. The control system shall provide the capability to update the protection mechanisms.

7.4.2 Rationale and supplemental guidance

The control system should use protection mechanisms to prevent, detect, mitigate and report instances of detected malicious code (for example, viruses, worms, Trojan horses and spyware) transported by electronic mail, electronic mail attachments, Internet access, removable media (for example, universal serial bus (USB) devices, diskettes or compact disks), PDF documents, web services, network connections and infected laptops or other common means.

Detection mechanisms should be able to detect integrity violations of application binaries and data files. Techniques may include, but are not limited to, binary integrity and attributes monitoring, hashing and signature techniques. Mitigation techniques may include, but are not limited to, file cleaning, quarantining, file deletion, host communication restriction and IPSs.

Prevention techniques may include, but are not limited to, application blacklisting and whitelisting techniques, removable media control, sandbox techniques and specific computing platforms mechanisms such as restricted firmware update capabilities, No Execute (NX) bit, data execution prevention (DEP), address space layout randomization (ASLR), stack corruption detection and mandatory access controls. See 10.4, SR 6.2 – Continuous monitoring for an associated requirement involving control system monitoring tools and techniques.

Prevention and mitigation mechanisms may include those designed for host elements (such as computers and servers) and network-based mechanisms (such as IDSs and IPSs) and those mechanisms focused on control system specific components (such as PLCs and HMIs).

7.4.3 Requirement enhancements

7.4.3.1 SR 3.2 RE 1 – Malicious code protection on entry and exit points

The control system shall provide the capability to employ malicious code protection mechanisms at all entry and exit points.

NOTE Such mechanisms are commonly provided on removable media, firewalls, unidirectional gateways, web servers, proxy servers or remote-access servers.

7.4.3.2 SR 3.2 RE 2 – Central management and reporting for malicious code protection

The control system shall provide the capability to manage malicious code protection mechanisms.

NOTE Such mechanisms are commonly provided by endpoint infrastructure centralized management or SIEM solutions.

7.4.4 Security levels

The requirements for the four SL levels that relate to SR 3.2 – Malicious code protection are:

- SL-C(SI, control system) 1: SR 3.2
- SL-C(SI, control system) 2: SR 3.2 (1)
- SL-C(SI, control system) 3: SR 3.2 (1) (2)
- SL-C(SI, control system) 4: SR 3.2 (1) (2)

7.5 SR 3.3 – Security functionality verification

7.5.1 Requirement

The control system shall provide the capability to support verification of the intended operation of security functions and report when anomalies are discovered during FAT, SAT and scheduled maintenance. These security functions shall include all those necessary to support the security requirements specified in this standard.

7.5.2 Rationale and supplemental guidance

The product supplier and/or system integrator should provide guidance on how to test the designed security controls. Asset owners need to be aware of the possible ramifications of running these verification tests during normal operations. Details of the execution of these

verifications need to be specified with careful consideration of the requirements for continuous operations (for example, scheduling or prior notification).

Examples of security verification functions include:

- Verification of antivirus measures by European Institute for Computer Antivirus Research (EICAR) testing of the control system file system. Antivirus software should detect this and appropriate incident handling procedures should be triggered.
- Verification of the identification, authentication and use control measures by attempting access with an unauthorized account (for some functionality this could be automated).
- Verification of IDSs as a security control by including a rule in the IDS that triggers on irregular, but known non-malicious traffic. The test could then be performed by introducing traffic that triggers this rule and the appropriate IDS monitoring and incident handling procedures.
- Confirmation that audit logging is occurring as required by security policies and procedures and has not been disabled by an internal or external entity.

7.5.3 Requirement enhancements

7.5.3.1 SR 3.3 RE 1 – Automated mechanisms for security functionality verification

The control system shall provide the capability to employ automated mechanisms to support management of security verification during FAT, SAT and scheduled maintenance.

7.5.3.2 SR 3.3 RE 2 – Security functionality verification during normal operation

The control system shall provide the capability to support verification of the intended operation of security functions during normal operations.

NOTE It is a commonly accepted good practice to carefully implement this requirement as it can lead to detrimental effects. It is often not considered suitable for safety systems.

7.5.4 Security levels

The requirements for the four SL levels that relate to SR 3.3 – Security functionality verification are:

- SL-C(SI, control system) 1: SR 3.3
- SL-C(SI, control system) 2: SR 3.3
- SL-C(SI, control system) 3: SR 3.3 (1)
- SL-C(SI, control system) 4: SR 3.3 (1) (2)

7.6 SR 3.4 – Software and information integrity

7.6.1 Requirement

The control system shall provide the capability to detect, record, report and protect against unauthorized changes to software and information at rest.

7.6.2 Rationale and supplemental guidance

Unauthorized changes are changes for which the entity attempting the change does not have the required privileges. This SR complements related SRs from FRs 1 and 2. FRs 1 and 2 involve enforcing the roles, privileges and use patterns as designed. Integrity verification methods are employed to detect, record, report and protect against software and information tampering that may occur if other protection mechanisms (such as authorization enforcement) have been circumvented. The control system should employ formal or recommended integrity mechanisms (such as cryptographic hashes). For example, such mechanisms could be used

to monitor field devices for their latest configuration information to detect security breaches (including unauthorized changes).

7.6.3 Requirement enhancements

7.6.3.1 SR 3.4 RE 1 – Automated notification about integrity violations

The control system shall provide the capability to use automated tools that provide notification to a configurable set of recipients upon discovering discrepancies during integrity verification.

7.6.3.2 Void

7.6.4 Security levels

The requirements for the four SL levels that relate to SR 3.4 – Software and information integrity are:

- SL-C(SI, control system) 1: Not selected
- SL-C(SI, control system) 2: SR 3.4
- SL-C(SI, control system) 3: SR 3.4 (1)
- SL-C(SI, control system) 4: SR 3.4 (1)

7.7 SR 3.5 – Input validation

7.7.1 Requirement

The control system shall validate the syntax and content of any input which is used as an industrial process control input or input that directly impacts the action of the control system.

7.7.2 Rationale and supplemental guidance

Rules for checking the valid syntax of control system inputs such as set points should be in place to verify that this information has not been tampered with and is compliant with the specification. Inputs passed to interpreters should be pre-screened to prevent the content from being unintentionally interpreted as commands. Note that this is a security SR, thus it does not address human error, for example supplying a legitimate integer number which is outside the expected range.

Generally accepted industry practices for input data validation include out-of-range values for a defined field type, invalid characters in data fields, missing or incomplete data and buffer overflow. Additional examples where invalid inputs lead to system security issues include SQL injection attacks, cross-site scripting or malformed packets (as commonly generated by protocol fuzzers). Guidelines to be considered could include the Open Web Application Security Project (OWASP) [31] Code Review Guide.

7.7.3 Requirement enhancements

None.

7.7.4 Security levels

The requirements for the four SL levels that relate to SR 3.5 – Input validation are:

- SL-C(SI, control system) 1: SR 3.5
- SL-C(SI, control system) 2: SR 3.5
- SL-C(SI, control system) 3: SR 3.5
- SL-C(SI, control system) 4: SR 3.5

7.8 SR 3.6 – Deterministic output

7.8.1 Requirement

The control system shall provide the capability to set outputs to a predetermined state if normal operation cannot be maintained as a result of an attack.

7.8.2 Rationale and supplemental guidance

The deterministic behavior of control system outputs as a result of threat actions against the control system is an important characteristic to ensure the integrity of normal operations. Ideally, the control system continues to operate normally while under attack, but if the control system cannot maintain normal operation, then the control system outputs need to fail to a predetermined state. The appropriate predetermined state of control system outputs is application dependent and could be one of the following user configurable options:

- Unpowered – the outputs fail to the unpowered state
- Hold – the outputs fail to the last-known good value
- Fixed – the outputs fail to a fixed value that is determined by the asset owner or an application

7.8.3 Requirement enhancements

None.

7.8.4 Security levels

The requirements for the four SL levels that relate to SR 3.6 – Deterministic output are:

- SR-C(SI, control system) 1: SR 3.6
- SR-C(SI, control system) 2: SR 3.6
- SR-C(SI, control system) 3: SR 3.6
- SR-C(SI, control system) 4: SR 3.6

7.9 SR 3.7 – Error handling

7.9.1 Requirement

The control system shall identify and handle error conditions in a manner such that effective remediation can occur. This shall be done in a manner which does not provide information that could be exploited by adversaries to attack the IACS unless revealing this information is necessary for the timely troubleshooting of problems.

7.9.2 Rationale and supplemental guidance

The structure and content of error messages should be carefully considered by the product supplier and/or system integrator. Error messages generated by the control system should provide timely and useful information without revealing potentially harmful information that could be used by adversaries to exploit the IACS. Since it may be unclear whether a particular error condition is due to a security event, all error messages may need to be easily accessible during incident response. Disclosure of this information should be justified by the necessity for timely resolution of error conditions. Guidelines to be considered could include the OWASP Code Review Guide [31].

7.9.3 Requirement enhancements

None.

7.9.4 Security levels

The requirements for the four SL levels that relate to SR 3.7 – Error handling are:

- SL-C(SI, control system) 1: Not Selected
- SL-C(SI, control system) 2: SR 3.7
- SL-C(SI, control system) 3: SR 3.7
- SL-C(SI, control system) 4: SR 3.7

7.10 SR 3.8 – Session integrity

7.10.1 Requirement

The control system shall provide the capability to protect the integrity of sessions. The control system shall reject any usage of invalid session IDs.

7.10.2 Rationale and supplemental guidance

This control focuses on communications protection at the session, versus packet, level. The intent of this control is to establish grounds for confidence at each end of a communications session in the ongoing identity of the other party and in the validity of the information being transmitted. For example, this control addresses man-in-the-middle attacks including session hijacking, insertion of false information into a session or replay attacks. Use of session integrity mechanisms can have a significant overhead and therefore their use should be considered in light of requirements for real-time communications.

7.10.3 Requirement enhancements

7.10.3.1 SR 3.8 RE 1 – Invalidation of session IDs after session termination

The control system shall provide the capability to invalidate session IDs upon user logout or other session termination (including browser sessions).

7.10.3.2 SR 3.8 RE 2 – Unique session ID generation

The control system shall provide the capability to generate a unique session ID for each session and treat all unexpected session IDs as invalid.

7.10.3.3 SR 3.8 RE 3 – Randomness of session IDs

The control system shall provide the capability to generate unique session IDs with commonly accepted sources of randomness.

NOTE Session hijacking and other man-in-the-middle attacks or injections of false information often take advantage of easy-to-guess session IDs (keys or other shared secrets) or use of session IDs which were not properly invalidated after session termination. Therefore the validity of a session authenticator needs to be tightly connected to the lifetime of a session. Employing randomness in the generation of unique session IDs helps to protect against brute-force attacks to determine future session IDs.

7.10.4 Security levels

The requirements for the four SL levels that relate to SR 3.8 – Session integrity are:

- SL-C(SI, control system) 1: Not Selected
- SL-C(SI, control system) 2: SR 3.8
- SL-C(SI, control system) 3: SR 3.8 (1) (2)
- SL-C(SI, control system) 4: SR 3.8 (1) (2) (3)

7.11 SR 3.9 – Protection of audit information

7.11.1 Requirement

The control system shall protect audit information and audit tools (if present) from unauthorized access, modification and deletion.

7.11.2 Rationale and supplemental guidance

Audit information includes all information (for example, audit records, audit settings and audit reports) needed to successfully audit control system activity. The audit information is important for error correction, security breach recovery, investigations and related efforts. Mechanisms for enhanced protection against modification and deletion include the storage of audit information to hardware-enforced write-once media.

7.11.3 Requirement enhancements

7.11.3.1 SR 3.9 RE 1 – Audit records on write-once media

The control system shall provide the capability to produce audit records on hardware-enforced write-once media.

7.11.3.2 Void

7.11.4 Security levels

The requirements for the four SL levels that relate to SR 3.9 – Protection of audit information are:

- SL-C(SI, control system) 1: Not selected
- SL-C(SI, control system) 2: SR 3.9
- SL-C(SI, control system) 3: SR 3.9
- SL-C(SI, control system) 4: SR 3.9 (1)

8 FR 4 – Data confidentiality

8.1 Purpose and SL-C(DC) descriptions

Ensure the confidentiality of information on communication channels and in data repositories to prevent unauthorized disclosure.

- SL 1 – Prevent the unauthorized disclosure of information via eavesdropping or casual exposure.
- SL 2 – Prevent the unauthorized disclosure of information to an entity actively searching for it using simple means with low resources, generic skills and low motivation.
- SL 3 – Prevent the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with moderate resources, IACS specific skills and moderate motivation.
- SL 4 – Prevent the unauthorized disclosure of information to an entity actively searching for it using sophisticated means with extended resources, IACS specific skills and high motivation.

8.2 Rationale

Some control system-generated information, whether at rest or in transit, is of a confidential or sensitive nature. This implies that some communication channels and data-stores require protection against eavesdropping and unauthorized access.

8.3 SR 4.1 – Information confidentiality

8.3.1 Requirement

The control system shall provide the capability to protect the confidentiality of information for which explicit read authorization is supported, whether at rest or in transit.

8.3.2 Rationale and supplemental guidance

Protection of information, at rest or in transit, can be maintained through physical means, compartmentalization or encryption, among other techniques. It is crucial that the technique chosen considers the potential ramifications on control system performance and the capability to recover from system failure or attack.

The decision whether the confidentiality of a given piece of information should be protected or not depends on the context and cannot be made at product design. However, the fact that an organization limits access to information by configuring explicit read authorizations in the control system is an indicator that this information is considered confidential by the organization. Thus, all information for which the control system supports the capability to assign explicit read authorizations should be considered potentially confidential and thus the control system should also provide the capability to protect it.

Different organizations and industries may require different levels of encryption strength for different categories of information, based on the sensitivity of the information as well as industry standards and regulatory requirements (see 8.5, SR 4.3 – Use of cryptography). In some situations network configuration information stored and processed in switches and routers may be considered as confidential.

Communications involving exposed information transfer may be vulnerable to eavesdropping or tampering. If the control system is depending upon an external communications service provider, it may be more difficult to obtain the necessary assurances regarding the implementation of needed security requirements for communication confidentiality. In such cases, it may be appropriate to implement compensating countermeasures or explicitly accept the additional risk.

Entities should also be cognizant of information confidentiality when portable and mobile devices are utilized (for example, engineering laptops and USB sticks).

As required by 5.7, SR 1.5 – Authenticator management, authentication information, such as passwords, should be considered confidential, and thus never be sent in the clear.

8.3.3 Requirement enhancements

8.3.3.1 SR 4.1 RE 1 – Protection of confidentiality at rest or in transit via untrusted networks

The control system shall provide the capability to protect the confidentiality of information at rest and remote access sessions traversing an untrusted network.

NOTE Cryptography is a common mechanism for ensuring information confidentiality.

8.3.3.2 SR 4.1 RE 2 – Protection of confidentiality across zone boundaries

The control system shall provide the capability to protect the confidentiality of information traversing any zone boundary.

8.3.4 Security levels

The requirements for the four SL levels that relate to SR 4.1 – Information confidentiality are:

- SL-C(DC, control system) 1: SR 4.1
- SL-C(DC, control system) 2: SR 4.1 (1)
- SL-C(DC, control system) 3: SR 4.1 (1)
- SL-C(DC, control system) 4: SR 4.1 (1) (2)

8.4 SR 4.2 – Information persistence

8.4.1 Requirement

The control system shall provide the capability to purge all information for which explicit read authorization is supported from components to be released from active service and/or decommissioned.

8.4.2 Rationale and supplemental guidance

Removal of a control system component from active service should not provide the opportunity for unintentional release of information for which explicit read authorization is supported. An example of such information would include 'join keys' (in the case of some wireless field devices) stored in non-volatile storage or other cryptographic information that would facilitate unauthorized or malicious activity.

Information produced by the actions of a user or role (or the actions of a software process acting on behalf of a user or role) should not be disclosed to a different user or role in an uncontrolled fashion. Control of control system information or data persistence prevents information stored on a shared resource from being unintentionally disclosed after that resource has been released back to the control system.

8.4.3 Requirement enhancements

8.4.3.1 SR 4.2 RE 1 – Purging of shared memory resources

The control system shall provide the capability to prevent unauthorized and unintended information transfer via volatile shared memory resources.

NOTE Volatile memory resources are those that typically do not retain information after being released to memory management. However, there are attacks against random access memory (RAM) that have the potential to extract key material or other confidential data before it is actually over-written. Therefore, it is a commonly accepted practice to purge all unique data and connections to unique data from volatile shared memory when that memory is released back to the control system for use by a different user, such that this data is not visible or accessible to the new user.

8.4.3.2 Void

8.4.4 Security levels

The requirements for the four SL levels that relate to SR 4.2 – Information persistence are:

- SL-C(DC, control system) 1: Not Selected
- SL-C(DC, control system) 2: SR 4.2
- SL-C(DC, control system) 3: SR 4.2 (1)
- SL-C(DC, control system) 4: SR 4.2 (1)

8.5 SR 4.3 – Use of cryptography

8.5.1 Requirement

If cryptography is required, the control system shall use cryptographic algorithms, key sizes and mechanisms for key establishment and management according to commonly accepted security industry practices and recommendations.

8.5.2 Rationale and supplemental guidance

The selection of cryptographic protection should match the value of the information being protected, the consequences of the confidentiality of the information being breached, the time period during which the information is confidential and control system operating constraints. This can involve either information at rest, in transit, or both. Note that backups are an example of information at rest, and should be considered as part of a data confidentiality assessment process. The control system product supplier should document the practices and procedures relating to cryptographic key establishment and management. The control system should utilize established and tested encryption and hash algorithms, such as the advanced encryption standard (AES) and the secure hash algorithm (SHA) series, and key sizes based on an assigned standard. Key generation needs to be performed using an effective random number generator. The security policies and procedures for key management need to address periodic key changes, key destruction, key distribution and encryption key backup in accordance with defined standards. Generally accepted practices and recommendations can be found in documents such as NIST SP800-57 [25]. Implementation requirements can be found for example in ISO/IEC 19790 [12].

This SR, along with 5.10, SR 1.8 – Public key infrastructure (PKI) certificates may be applicable when meeting many other requirements defined within this standard.

8.5.3 Requirement enhancements

None.

8.5.4 Security levels

The requirements for the four SL levels that relate to SR 4.3 – Use of cryptography are:

- SL-C(DC, control system) 1: SR 4.3
- SL-C(DC, control system) 2: SR 4.3
- SL-C(DC, control system) 3: SR 4.3
- SL-C(DC, control system) 4: SR 4.3

9 FR 5 – Restricted data flow

9.1 Purpose and SL-C(RDF) descriptions

Segment the control system via zones and conduits to limit the unnecessary flow of data.

- SL 1 – Prevent the casual or coincidental circumvention of zone and conduit segmentation.
- SL 2 – Prevent the intended circumvention of zone and conduit segmentation by entities using simple means with low resources, generic skills and low motivation.
- SL 3 – Prevent the intended circumvention of zone and conduit segmentation by entities using sophisticated means with moderate resources, IACS specific skills and moderate motivation.
- SL 4 – Prevent the intended circumvention of zone and conduit segmentation by entities using sophisticated means with extended resources, IACS specific skills and high motivation.

9.2 Rationale

Using their risk assessment methodology, asset owners need to determine necessary information flow restrictions and thus, by extension, determine the configuration of the conduits used to deliver this information. Derived prescriptive recommendations and guidelines should include mechanisms that range from disconnecting control system networks

from business or public networks to using unidirectional gateways, stateful firewalls and DMZs to manage the flow of information.

9.3 SR 5.1 – Network segmentation

9.3.1 Requirement

The control system shall provide the capability to logically segment control system networks from non-control system networks and to logically segment critical control system networks from other control system networks.

9.3.2 Rationale and supplemental guidance

Network segmentation is used by organizations for a variety of purposes, including cyber security. The main reasons for segmenting networks are to reduce the exposure, or ingress, of network traffic into a control system and reduce the spread, or egress, of network traffic from a control system. This improves overall system response and reliability as well as provides a measure of cyber security protection. It also allows different network segments within the control system, including critical control systems and safety-related systems, to be segmented from other systems for an additional level of protection.

Access from the control system to the World Wide Web should be clearly justified based on control system operational requirements.

Network segmentation and the level of protection it provides will vary greatly depending on the overall network architecture used by an asset owner in their facility and even system integrators within their control systems. Logically segmenting networks based on their functionality provides some measure of protection, but may still lead to single-points-of-failure if a network device is compromised. Physically segmenting networks provides another level of protection by removing that single-point-of-failure case, but will lead to a more complex and costly network design. These trade-offs will need to be evaluated during the network design process (see IEC 62443-2-1).

In response to an incident, it may be necessary to break the connections between different network segments. In that event, the services necessary to support essential operations should be maintained in such a way that the devices can continue to operate properly and/or shutdown in an orderly manner. This may require that some servers may need to be duplicated on the control system network to support normal network features, for example dynamic host configuration protocol (DHCP), domain name service (DNS) or local CAs. It may also mean that some critical control systems and safety-related systems be designed from the beginning to be completely isolated from other networks.

9.3.3 Requirement enhancements

9.3.3.1 SR 5.1 RE 1 – Physical network segmentation

The control system shall provide the capability to physically segment control system networks from non-control system networks and to physically segment critical control system networks from non-critical control system networks.

9.3.3.2 SR 5.1 RE 2 – Independence from non-control system networks

The control system shall have the capability to provide network services to control system networks, critical or otherwise, without a connection to non-control system networks.

9.3.3.3 SR 5.1 RE 3 – Logical and physical isolation of critical networks

The control system shall provide the capability to logically and physically isolate critical control system networks from non-critical control system networks.

9.3.4 Security levels

The requirements for the four SL levels that relate to SR 5.1 – Network segmentation are:

- SL-C(RDF, control system) 1: SR 5.1
- SL-C(RDF, control system) 2: SR 5.1 (1)
- SL-C(RDF, control system) 3: SR 5.1 (1) (2)
- SL-C(RDF, control system) 4: SR 5.1 (1) (2) (3)

9.4 SR 5.2 – Zone boundary protection

9.4.1 Requirement

The control system shall provide the capability to monitor and control communications at zone boundaries to enforce the compartmentalization defined in the risk-based zones and conduits model.

9.4.2 Rationale and supplemental guidance

Any connections to external networks or other control systems should occur through managed interfaces consisting of appropriate boundary protection devices (for example, proxies, gateways, routers, firewalls, unidirectional gateways, guards and encrypted tunnels) arranged in an effective architecture (for example, firewalls protecting application gateways residing in a DMZ). Control system boundary protections at any designated alternate processing sites should provide the same levels of protection as that of the primary site.

As part of a defense-in-depth protection strategy, higher impact control systems should be partitioned into separate zones utilizing conduits to restrict or prohibit network access in accordance with security policies and procedures and an assessment of risk. SL-T(system) categorization guides the selection of appropriate candidates for zone partitioning (see IEC 62443-3-2 [8]).

9.4.3 Requirement enhancements

9.4.3.1 SR 5.2 RE 1 – Deny by default, allow by exception

The control system shall provide the capability to deny network traffic by default and allow network traffic by exception (also termed deny all, permit by exception).

9.4.3.2 SR 5.2 RE 2 – Island mode

The control system shall provide the capability to prevent any communication through the control system boundary (also termed island mode).

NOTE Examples of when this capability may be used include where a security violation and/or breach has been detected within the control system, or an attack is occurring at the enterprise level (see also 4.2, Support of essential functions).

9.4.3.3 SR 5.2 RE 3 – Fail close

The control system shall provide the capability to prevent any communication through the control system boundary when there is an operational failure of the boundary protection mechanisms (also termed fail close). This 'fail close' functionality shall be designed such that it does not interfere with the operation of a SIS or other safety-related functions.

NOTE Examples of when this capability may be used include scenarios where a hardware failure or power failure causes boundary protection devices to function in a degraded mode or fail entirely (see also 4.2, Support of essential functions).

9.4.4 Security levels

The requirements for the four SL levels that relate to SR 5.2 – Zone boundary protection are:

- SL-C(RDF, control system) 1: SR 5.2
- SL-C(RDF, control system) 2: SR 5.2 (1)
- SL-C(RDF, control system) 3: SR 5.2 (1) (2) (3)
- SL-C(RDF, control system) 4: SR 5.2 (1) (2) (3)

9.5 SR 5.3 – General purpose person-to-person communication restrictions

9.5.1 Requirement

The control system shall provide the capability to prevent general purpose person-to-person messages from being received from users or systems external to the control system.

9.5.2 Rationale and supplemental guidance

General purpose person-to-person communications systems include but are not limited to: email systems, forms of social media (Twitter, Facebook, picture galleries, etc.) or any message systems that permit the transmission of any type of executable file. These systems are usually utilized for private purposes which are not related to control system operations, and therefore the risks imposed by these systems normally outweigh any perceived benefit.

These types of general purpose communications systems are commonly used attack vectors to introduce malware to the control system, pass information for which read authorization exists to locations external to the control system, and introduce excessive network loading that can be used to create security problems or launch attacks on the control system. Application of a broad range of other system requirements covering, for example, usage restrictions and limiting data flow as described elsewhere in this standard to general purpose person-to-person communication systems can provide adequate compensating countermeasures to meet this requirement.

The control system may provide the capability to utilize these types of two-way communication systems, but only between servers and/or workstations within the control system. Note that this SR needs to support the requirements associated with 8.3, SR 4.1 – Information confidentiality.

The control system may also restrict email or other messaging solutions that provide internal computer-to-external computer communications using outbound messages. These internal-to-external communications may be limited to the purpose of sending system alerts or other computer generated information messages to users or systems external to the control system. To prevent the passing of information for which explicit read authorization is supported, pre-configured messages (perhaps with the ability to include some limited text) should be used to transmit the alerts or status information. Users may not be given the ability to attach files or other information to these outbound-only messages at the time the messages are created by the system.

9.5.3 Requirement enhancements

9.5.3.1 SR 5.3 RE 1 – Prohibit all general purpose person-to-person communications

The control system shall provide the capability to prevent both transmission and receipt of general purpose person-to-person messages.

9.5.3.2 Void

9.5.4 Security levels

The requirements for the four SL levels that relate to SR 5.3 – General purpose person-to-person communication restrictions are:

- SL-C(RDF, control system) 1: SR 5.3
- SL-C(RDF, control system) 2: SR 5.3
- SL-C(RDF, control system) 3: SR 5.3 (1)
- SL-C(RDF, control system) 4: SR 5.3 (1)

9.6 SR 5.4 – Application partitioning

9.6.1 Requirement

The control system shall provide the capability to support partitioning of data, applications and services based on criticality to facilitate implementing a zoning model.

9.6.2 Rationale and supplemental guidance

Partitioning may be accomplished via physical or logical means through the use of different computers, different central processing units, different instances of the operating system, different network addresses and combinations of these methods or other methods as appropriate. Examples of applications and services that could be considered for different partitions include, but are not limited to, emergency and/or safety systems, closed-loop control applications, operator workstations and engineering workstations.

9.6.3 Requirement enhancements

None.

9.6.4 Security levels

The requirements for the four SL levels that relate to SR 5.4 – Application partitioning are:

- SL-C(RDF, control system) 1: SR 5.4
- SL-C(RDF, control system) 2: SR 5.4
- SL-C(RDF, control system) 3: SR 5.4
- SL-C(RDF, control system) 4: SR 5.4

10 FR 6 – Timely response to events

10.1 Purpose and SL-C(TRE) descriptions

Respond to security violations by notifying the proper authority, reporting needed evidence of the violation and taking timely corrective action when incidents are discovered.

- SL 1 – Monitor the operation of the IACS and respond to incidents when they are discovered by collecting and providing the forensic evidence when queried.
- SL 2 – Monitor the operation of the IACS and respond to incidents when they are discovered by actively collecting and periodically reporting forensic evidence.
- SL 3 – Monitor the operation of the IACS and respond to incidents when they are discovered by actively collecting and pushing forensic evidence to the proper authority.
- SL 4 – Monitor the operation of the IACS and respond to incidents when they are discovered by actively collecting and pushing forensic evidence to the proper authority in near real-time.

10.2 Rationale

Using their risk assessment methodology, asset owners should establish security policies and procedures and proper lines of communication and control needed to respond to security violations. Derived prescriptive recommendations and guidelines should include mechanisms that collect, report, preserve and automatically correlate the forensic evidence to ensure timely corrective action. The use of monitoring tools and techniques should not adversely affect the operational performance of the control system.

10.3 SR 6.1 – Audit log accessibility

10.3.1 Requirement

The control system shall provide the capability for authorized humans and/or tools to access audit logs on a read-only basis.

10.3.2 Rationale and supplemental guidance

The control system generates audit records about events occurring in the system (see 6.10, SR 2.8 – Auditable events). Access to these audit logs is necessary to support filtering audit logs, identifying and removing information that is redundant, reviewing and reporting activity during after-the-fact investigations of security incidents. This access should not alter the original audit records. In general, audit reduction and report generation should be performed on a separate information system. Manual access to the audit records (such as screen views or printouts) is sufficient for meeting the base requirement, but is insufficient for higher SLs. Programmatic access is commonly used to provide the audit log information to analysis mechanisms such as SIEM. See relevant SRs in Clauses 5, 6 and 9 regarding the creation of, protection of and access to audit logs.

10.3.3 Requirement enhancements

10.3.3.1 SR 6.1 RE 1 – Programmatic access to audit logs

The control system shall provide programmatic access to audit records using an application programming interface (API).

10.3.3.2 Void

10.3.4 Security levels

The requirements for the four SL levels that relate to SR 6.1 – Audit log accessibility are:

- SL-C(TRE, control system) 1: SR 6.1
- SL-C(TRE, control system) 2: SR 6.1
- SL-C(TRE, control system) 3: SR 6.1 (1)
- SL-C(TRE, control system) 4: SR 6.1 (1)

10.4 SR 6.2 – Continuous monitoring

10.4.1 Requirement

The control system shall provide the capability to continuously monitor all security mechanism performance using commonly accepted security industry practices and recommendations to detect, characterize and report security breaches in a timely manner.

NOTE Response time is a local matter outside the scope of this standard.

10.4.2 Rationale and supplemental guidance

Control system monitoring capability can be achieved through a variety of tools and techniques (for example, IDS, IPS, malicious code protection mechanisms and network

monitoring mechanisms). As attacks become more sophisticated, these monitoring tools and techniques will need to become more sophisticated as well, including for example behavior-based IDS/IPS.

Monitoring devices should be strategically deployed within the control system (for example, at selected perimeter locations and near server farms supporting critical applications) to collect essential information. Monitoring mechanisms may also be deployed at ad hoc locations within the control system to track specific transactions.

Monitoring should include appropriate reporting mechanisms to allow for a timely response to events. To keep the reporting focused and the amount of reported information to a level that can be processed by the recipients, mechanisms such as SIEM are commonly applied to correlate individual events into aggregate reports which establish a larger context in which the raw events occurred.

Additionally, these mechanisms can be used to track the effect of security changes to the control system (see 6.10, SR 2.8 – Auditable events). Having forensic tools pre-installed can facilitate incident analysis.

10.4.3 Requirement enhancements

None.

10.4.4 Security levels

The requirements for the four SL levels that relate to SR 6.2 – Continuous monitoring are:

- SL-C(TRE, control system) 1: Not Selected
- SL-C(TRE, control system) 2: SR 6.2
- SL-C(TRE, control system) 3: SR 6.2
- SL-C(TRE, control system) 4: SR 6.2

11 FR 7 – Resource availability

11.1 Purpose and SL-C(RA) descriptions

Ensure the availability of the control system against the degradation or denial of essential services.

- SL 1 – Ensure that the control system operates reliably under normal production conditions and prevents DoS situations caused by the casual or coincidental actions of an entity.
- SL 2 – Ensure that the control system operates reliably under normal and abnormal production conditions and prevents DoS situations by entities using simple means with low resources, generic skills and low motivation.
- SL 3 – Ensure that the control system operates reliably under normal, abnormal, and extreme production conditions and prevents DoS situations by entities using sophisticated means with moderate resources, IACS specific skills and moderate motivation.
- SL 4 – Ensure that the control system operates reliably under normal, abnormal, and extreme production conditions and prevents DoS situations by entities using sophisticated means with extended resources, IACS specific skills and high motivation.

11.2 Rationale

The aim of this series of SRs is to ensure that the control system is resilient against various types of DoS events. This includes the partial or total unavailability of system functionality at

various levels. In particular, security incidents in the control system should not affect SIS or other safety-related functions.

11.3 SR 7.1 – Denial of service protection

11.3.1 Requirement

The control system shall provide the capability to operate in a degraded mode during a DoS event.

11.3.2 Rationale and supplemental guidance

A variety of technologies exist to limit, or in some cases, eliminate the effects of DoS situations. For example, boundary protection devices can filter certain types of packets to protect devices on an internal, trusted network from being directly affected by DoS events or restricting the information flow to be unidirectional outbound. Specifically, as noted in Clause 4, a DoS event on the control system should not adversely impact any safety-related systems.

11.3.3 Requirement enhancements

11.3.3.1 SR 7.1 RE 1 – Manage communication loads

The control system shall provide the capability to manage communication loads (such as using rate limiting) to mitigate the effects of information flooding types of DoS events.

11.3.3.2 SR 7.1 RE 2 – Limit DoS effects to other systems or networks

The control system shall provide the capability to restrict the ability of all users (humans, software processes and devices) to cause DoS events which affect other control systems or networks.

11.3.4 Security levels

The requirements for the four SL levels that relate to SR 7.1 – Denial of service protection are:

- SL-C(RA, control system) 1: SR 7.1
- SL-C(RA, control system) 2: SR 7.1 (1)
- SL-C(RA, control system) 3: SR 7.1 (1) (2)
- SL-C(RA, control system) 4: SR 7.1 (1) (2)

11.4 SR 7.2 – Resource management

11.4.1 Requirement

The control system shall provide the capability to limit the use of resources by security functions to prevent resource exhaustion.

11.4.2 Rationale and supplemental guidance

Resource management (for example, network segmentation or priority schemes) prevents a lower-priority software process from delaying or interfering with the control system servicing any higher-priority software process. For example, initiating network scans, patching and/or antivirus checks on an operating system can cause severe disruption to normal operations. Traffic rate limiting schemes should be considered as a mitigation technique.

11.4.3 Requirement enhancements

None.

11.4.4 Security levels

The requirements for the four SL levels that relate to SR 7.2 – Resource management are:

- SL-C(RA, control system) 1: SR 7.2
- SL-C(RA, control system) 2: SR 7.2
- SL-C(RA, control system) 3: SR 7.2
- SL-C(RA, control system) 4: SR 7.2

11.5 SR 7.3 – Control system backup

11.5.1 Requirement

The identity and location of critical files and the ability to conduct backups of user-level and system-level information (including system state information) shall be supported by the control system without affecting normal plant operations.

11.5.2 Rationale and supplemental guidance

The availability of up-to-date backups is essential for recovery from a control system failure and/or mis-configuration. Automating this function ensures that all required files are captured, reducing operator overhead. Although not usually required for control system recovery, information required for post-incident forensic activity (for example, audit logs) should be specifically included in the backup (see 10.4, SR 6.2 – Continuous monitoring). If the resulting backups contain confidential information, encryption should be considered (see 8.5, SR 4.3 – Use of cryptography).

11.5.3 Requirement enhancements

11.5.3.1 SR 7.3 RE 1 – Backup verification

The control system shall provide the capability to verify the reliability of backup mechanisms.

11.5.3.2 SR 7.3 RE 2 – Backup automation

The control system shall provide the capability to automate the backup function based on a configurable frequency.

11.5.4 Security levels

The requirements for the four SL levels that relate to SR 7.3 – Control system backup are:

- SL-C(RA, control system) 1: SR 7.3
- SL-C(RA, control system) 2: SR 7.3 (1)
- SL-C(RA, control system) 3: SR 7.3 (1) (2)
- SL-C(RA, control system) 4: SR 7.3 (1) (2)

11.6 SR 7.4 – Control system recovery and reconstitution

11.6.1 Requirement

The control system shall provide the capability to recover and reconstitute to a known secure state after a disruption or failure.

11.6.2 Rationale and supplemental guidance

Control system recovery and reconstitution to a known secure state means that all system parameters (either default or configurable) are set to secure values, security-critical patches are reinstalled, security-related configuration settings are reestablished, system

documentation and operating procedures are available, application and system software is reinstalled and configured with secure settings, information from the most recent, known secure backups is loaded and the system is fully tested and functional.

11.6.3 Requirement enhancements

None.

11.6.4 Security levels

The requirements for the four SL levels that relate to SR 7.4 – Control system recovery and reconstitution are:

- SL-C(RA, control system) 1: SR 7.4
- SL-C(RA, control system) 2: SR 7.4
- SL-C(RA, control system) 3: SR 7.4
- SL-C(RA, control system) 4: SR 7.4

11.7 SR 7.5 – Emergency power

11.7.1 Requirement

The control system shall provide the capability to switch to and from an emergency power supply without affecting the existing security state or a documented degraded mode.

11.7.2 Rationale and supplemental guidance

There may be instances where compensating countermeasures such as physical door access control may be affected by loss of base power supply, in which case the emergency power supply should cover those associated systems. If this is not possible, other compensating countermeasures may be needed during such an emergency situation.

11.7.3 Requirement enhancements

None.

11.7.4 Security levels

The requirements for the four SL levels that relate to SR 7.5 – Emergency power are:

- SL-C(RA, control system) 1: SR 7.5
- SL-C(RA, control system) 2: SR 7.5
- SL-C(RA, control system) 3: SR 7.5
- SL-C(RA, control system) 4: SR 7.5

11.8 SR 7.6 – Network and security configuration settings

11.8.1 Requirement

The control system shall provide the capability to be configured according to recommended network and security configurations as described in guidelines provided by the control system supplier. The control system shall provide an interface to the currently deployed network and security configuration settings.

11.8.2 Rationale and supplemental guidance

These configuration settings are the adjustable parameters of the control system components. In order to be able to detect and correct any deviations from the approved and/or recommended configuration settings, the control system needs to support monitoring and

control of changes to the configuration settings in accordance with security policies and procedures. For enhanced security, an automated check may be performed where the current settings are automatically collected by an agent and compared to approved settings.

11.8.3 Requirement enhancements

11.8.3.1 SR 7.6 RE 1 – Machine-readable reporting of current security settings

The control system shall provide the capability to generate a report listing the currently deployed security settings in a machine-readable format.

11.8.3.2 Void

11.8.4 Security levels

The requirements for the four SL levels that relate to SR 7.6 – Network and security configuration settings are:

- SL-C(RA, control system) 1: SR 7.6
- SL-C(RA, control system) 2: SR 7.6
- SL-C(RA, control system) 3: SR 7.6 (1)
- SL-C(RA, control system) 4: SR 7.6 (1)

11.9 SR 7.7 – Least functionality

11.9.1 Requirement

The control system shall provide the capability to specifically prohibit and/or restrict the use of unnecessary functions, ports, protocols and/or services.

11.9.2 Rationale and supplemental guidance

Control systems are capable of providing a wide variety of functions and services. Some of the functions and services provided may not be necessary to support essential functions. Therefore, by default, functions beyond a baseline configuration should be disabled. Additionally, it is sometimes convenient to provide multiple services from a single component of a control system, but doing so increases risk over limiting the services provided by any one component. Many functions and services commonly provided by commercial-off-the-shelf (COTS) equipment may be candidates for elimination, for example, email, voice over internet protocol (VoIP), instant messaging (IM), file transfer protocol (FTP), hypertext transfer protocol (HTTP) and file sharing.

11.9.3 Requirement enhancements

None.

11.9.4 Security levels

The requirements for the four SL levels that relate to SR 7.7 – Least functionality are:

- SL-C(RA, control system) 1: SR 7.7
- SL-C(RA, control system) 2: SR 7.7
- SL-C(RA, control system) 3: SR 7.7
- SL-C(RA, control system) 4: SR 7.7

11.10 SR 7.8 – Control system component inventory

11.10.1 Requirement

The control system shall provide the capability to report the current list of installed components and their associated properties.

11.10.2 Rationale and supplemental guidance

A control system component inventory may include but is not limited to component ID, capability and revision level. The component inventory should be consistent with the SuC. A formal process of configuration management should be deployed to keep control of the changes in the component inventory baseline (see IEC 62443-2-1).

11.10.3 Requirement enhancements

None.

11.10.4 Security levels

The requirements for the four SL levels that relate to SR 7.8 – Control system component inventory are:

- SL-C(RA, control system) 1: Not Selected
- SL-C(RA, control system) 2: SR 7.8
- SL-C(RA, control system) 3: SR 7.8
- SL-C(RA, control system) 4: SR 7.8

Annex A
(informative)

Discussion of the SL vector

NOTE 1 This annex is based on the paper titled “Security Assurance Levels: A Vector Approach to Describing Security Requirements” [28]. The content in this annex has been modified from that original paper to respond to changes in the IEC 62443 series and comments received from reviewers.

NOTE 2 The ultimate home for the majority of the material contained in this annex will be IEC 62443-1-1 and IEC 62443-3-2. At the time of this documents publication, these other documents were being written and/or revised and did not contain the material on the SL vector. This annex has been provided to aid the reader in understanding the SL vector concept. The material in this annex is informative and will be superseded by any normative content included in those other standards.

A.1 Overview

Safety systems have used the concept of safety integrity levels (SILs) for almost two decades. This allows the safety integrity capability of a component or the safety integrity level of a deployed system to be represented by a single number that defines a protection factor required to ensure the health and safety of people or the environment based on the probability of failure of that component or system. The process to determine the required protection factor for a safety system, while complex, is manageable since the probability of a component or system failure due to random hardware failures can be measured in quantitative terms. The overall risk can be calculated based on the consequences that those failures could potentially have on HSE.

Security systems have much broader application, a much broader set of consequences and a much broader set of possible circumstances leading up to a possible event. Security systems are still meant to protect HSE, but they are also meant to protect the industrial process itself, company-proprietary information, public confidence and national security among other things in situations where random hardware failures may not be the root cause. In some cases, it may be a well-meaning employee that makes a mistake, and in other cases it may be a devious attacker bent on causing an event and hiding the evidence. The increased complexity of security systems makes compressing the protection factor down to a single number much more difficult.

A.2 Security levels

A.2.1 Definition

The following is an excerpt from 5.11.1 of IEC/TS 62443-1-1:2009 that provides a good explanation of what SLs are and how they can be used.

> *Security levels provide a qualitative approach to addressing security for a zone. As a qualitative method, security level definition has applicability for comparing and managing the security of zones within an organization. As more data becomes available and the mathematical representations of risk, threats, and security incidents are developed, this concept will move to a quantitative approach for selection and verification of Security Levels (SL). It will have applicability to both end user companies, and vendors of IACS and security products. It will be used to select IACS devices and countermeasures to be used within a zone and to identify and compare security of zones in different organizations across industry segments.*

In the first phase of development, the IEC 62443 series of standards tends to use qualitative SLs, using terms such as “low”, “medium”, and “high”. The asset owner will be required to come up with their own definition of what those classifications mean for their particular application. The long-term goal for the IEC 62443 series is to move as many of the security levels and requirements to quantitative descriptions, requirements and metrics as possible to establish repeatable applications of the standard across multiple companies and industries.

Achieving this goal will take time, since more experience in applying the standards and data on industrial security systems will need to be acquired to justify the quantitative approach.

When mapping requirements to the different SLs, standard developers need some frame of reference describing what the different SLs mean and how they differ from each other. The goal of this annex is to propose such a frame of reference.

A.2.2 Types of SLs

SLs have been broken down into three different types: target, achieved and capability. These types, while they all are related have to do with different aspects of the security lifecycle.

- **Target SLs (SL-T)** are the desired level of security for a particular system. This is usually determined by performing a risk assessment on a system and determining that it needs a particular level of security to ensure its correct operation.
- **Achieved SLs (SL-A)** are the actual level of security for a particular system. These are measured after a system design is available or when a system is in place. They are used to establish that a security system is meeting the goals that were originally set out in the target SLs.
- **Capability SLs (SL-C)** are the security levels that components or systems can provide when properly configured. These levels state that a particular component or system is capable of meeting the target SLs natively without additional compensating countermeasures when properly configured and integrated.

Each of these SLs is intended to be used in different phases of the security lifecycle according the IEC 62443 series. Starting with a target for a particular system, an organization would need to build a design that included the capabilities to achieve the desired result. In other words, the design team would first develop the target SL necessary for a particular system. They would then design the system to meet those targets, usually in an iterative process where after each iteration the achieved SLs of the proposed design are measured and compared to the target SLs. As part of that design process, the designers would select components and systems with the necessary capability SLs to meet the target SL requirements – or where such systems and components are not available, complement the available ones with compensating countermeasures. After the system went into operation, the actual SL would be measured as the achieved SL and compared to the target SL.

A.2.3 Using SLs

When designing a new system (green field) or revising the security of an existing system (brown field), the first step is to break the system into different zones and define conduits connecting these zones where necessary. Details on how to accomplish this are given in IEC 62443-3-2. Once a zone model of the system is established each zone and conduit is assigned a target SL, based on a consequence analysis, which describes the desired security for the respective zone or conduit. During this initial zone and conduit analysis, it is not necessary to have completed a detailed system design. It is sufficient to describe the functionality that should be provided by assets in a zone and the connections between zones in order to meet the security objectives.

Figure A.1 and Figure A.2 show high-level examples of systems broken down into zones connected by conduits. Figure A.1 is a graphical representation of a control system for a chlorine truck loading station. The full use-case that accompanies this figure will be discussed in IEC/TR 62443-1-4. It has five zones shown: the basic process control system (BPCS), the SIS, the control center, the plant DMZ, and the enterprise. The BPCS and SIS both use PLCs to operate different aspects of the loading station with the SIS using a special functional safety PLC (FS-PLC) rated for use in safety systems. The two PLCs are connected via a non-routable serial or Ethernet connection using a boundary protection device. Each of the PLCs is connected to a local switch with an engineering workstation for programming and HMI for operating. The BPCS and SIS zones also contain an instrument asset management system (IAMS) to measure and test the instruments. A control center containing multiple workstations and the BPCS are both connected to the plant DMZ. A plant DMZ can house a variety of

components and systems, for example a data historian and a maintenance workstation as shown in the figure. The plant DMZ is shown connected to the enterprise systems, which contain the corporate wireless local area network (WLAN) and web server. Multiple domain controllers and boundary protection devices are shown in the figure to indicate some of the countermeasures that may be applied to improve security.

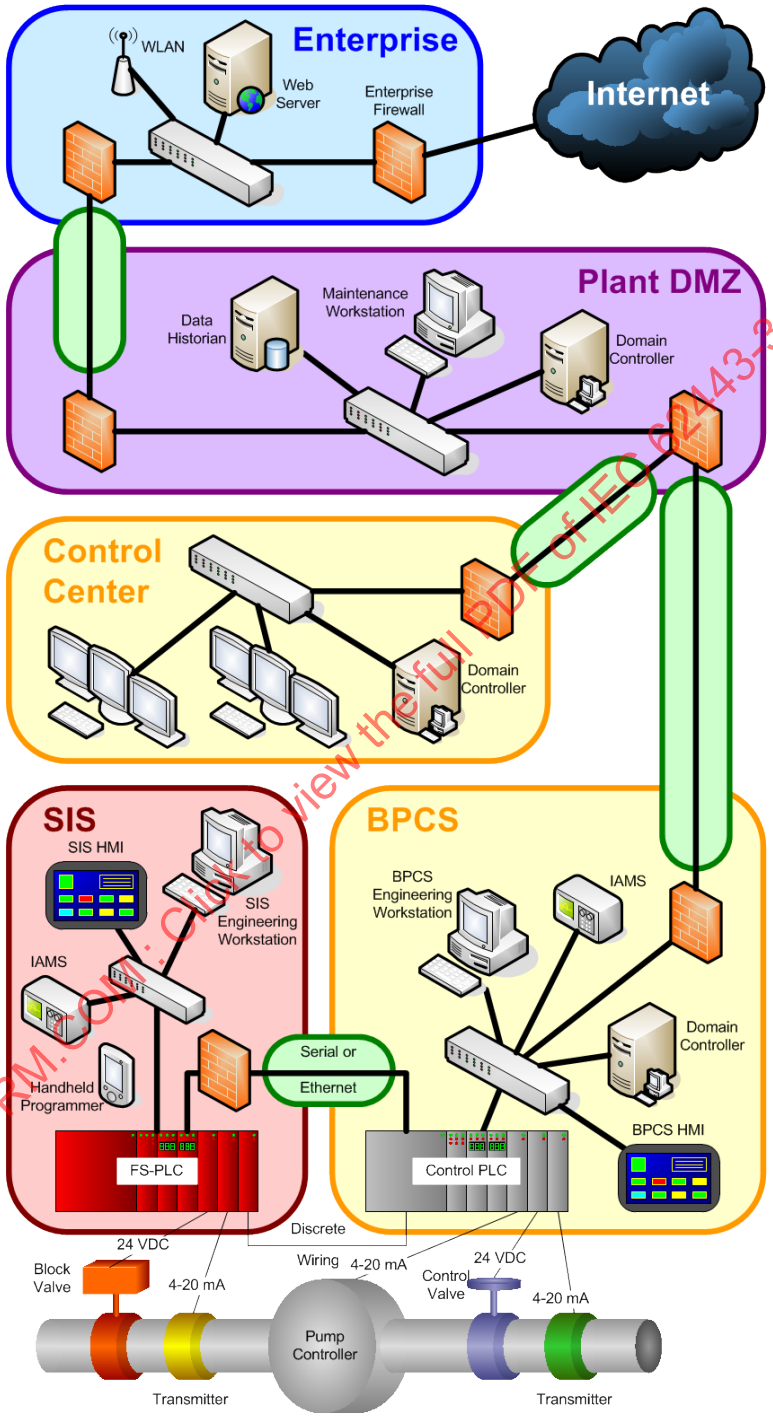


Figure A.1 – High-level process-industry example showing zones and conduits

Figure A.2 is a graphical representation of a manufacturing plant. It has four zones defined: the enterprise network, the industrial/enterprise DMZ, and two industrial networks. The enterprise infrastructure has a WLAN and a connection to the Internet. Many companies use a DMZ between important parts of their systems to isolate the network traffic. In this particular example, each industrial network operates relatively independent of each other with its own PLC, field devices, and HMI.

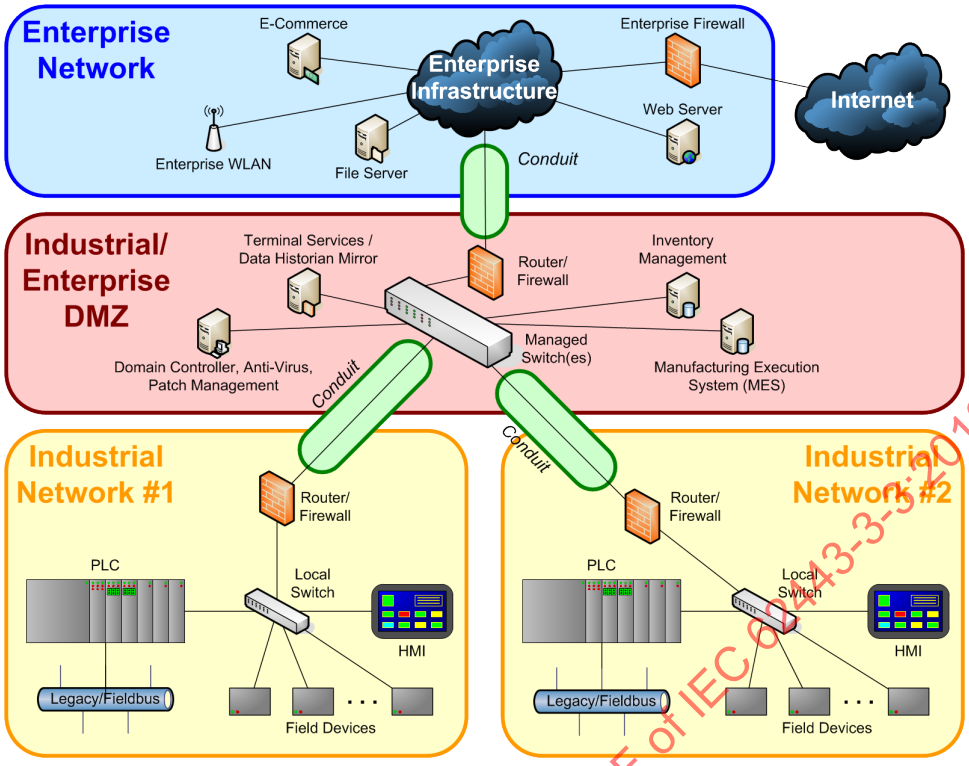


Figure A.2 – High-level manufacturing example showing zones and conduits

After determining the target SLs, the system can be designed (green field) or redesigned (brown field) to try to meet those target SLs. The design process is usually an iterative approach where the system design is checked against the target multiple times throughout the process. Multiple parts of the IEC 62443 series contain guidance on different aspects of the programmatic and technical requirements that go into the design process. IEC 62443-2-1 provides guidance on the programmatic aspects of the design process while IEC 62443-3-3 (this standard) and IEC 62443-4-2 [10] define system-level and component-level technical security requirements and relate them to different capability SLs.

During the design process for a system, it is necessary to evaluate the security capabilities of different components and subsystems. Product suppliers will have to provide these as capability SLs for their components or systems by comparing features and capabilities with the requirements defined in the IEC 62443 series for the different capability SLs. These capability SLs can be used to determine whether a given component or system is capable of meeting the target SL for the system. The product supplier or system integrator will also have to provide guidance on how to configure the component or system to meet the claimed SLs.

It is likely that in a particular design there will be some components or systems that cannot fully meet the target SL. Where the capability SL of a component or system is lower than the target SL, compensating countermeasures need to be considered to meet the desired target SL. Compensating countermeasures may include changing the design of the component or system to increase its capabilities, choosing another component or system to meet the target SL or adding additional components or systems to meet the target SL. After each iteration in the design process, the system design's achieved SLs should be reevaluated to see how they compare to the target SLs for the system.

Once the system design is approved and implemented, the system needs to be evaluated to prevent or mitigate deterioration of the system's security level. It should be evaluated during or after system modifications and on a regular schedule. IEC 62443-2-1 provides guidance on the steps necessary to operate the security program and how to evaluate its effectiveness. After the achieved SLs have been determined, it will be necessary to evaluate whether the system is still meeting the original target SLs (for example, using the system requirements

from IEC 62443-3-3). If the system is not meeting those requirements, there may be multiple reasons including the lack of maintenance of the program or the need to redesign parts of the system.

In essence, the control system security capabilities are determined independent from a given use context, but are used in a given context in order to achieve the target SL of the respective system architecture, zones and/or conduits (see Figure A.3).

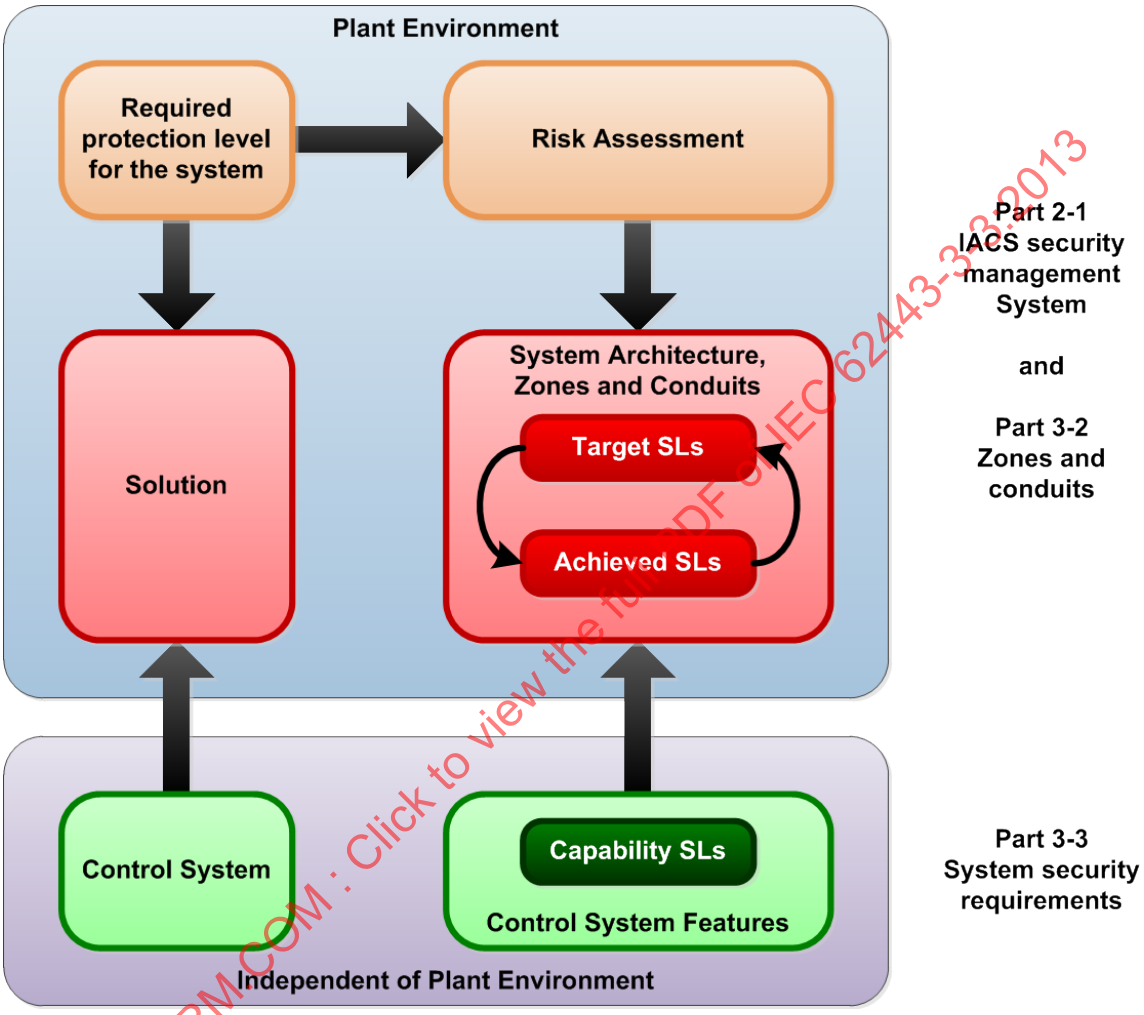


Figure A.3 – Schematic of correlation of the use of different SL types

A.3 SL vector

A.3.1 Foundational requirements

SLs are based on the seven FRs for security as defined in IEC 62443-1-1:

1) Identification and authentication control (IAC),
2) Use control (UC),
3) System integrity (SI),
4) Data confidentiality (DC),
5) Restricted data flow (RDF),
6) Timely response to events (TRE), and
7) Resource availability (RA).

Instead of compressing SLs down to a single number, it is possible to use a vector of SLs that uses the seven FRs above instead of a single protection factor. This vector of SLs allows definable separations between SLs for the different FRs using language. This language can be based on the additional consequences associated with security systems or different attacks against the security objectives addressed by the FRs. The language used in the SL definitions can contain practical explanations of how one system is more secure than another without having to relate everything to HSE consequences.

A.3.2 Level definitions

A.3.2.1 Overview

The IEC 62443 series define SLs in terms of five different levels (0, 1, 2, 3 and 4), each with an increasing level of security. The current model for defining SLs depends on protecting an increasingly more complex threat and differs slightly depending on what type of SL it is applied. For SL-C, this means that a particular component or system is capable of being configured by an asset owner or system integrator to protect against an increasingly complex type of threat. For SL-T, this means that the asset owner or system integrator has determined through a risk assessment that they need to protect this particular zone, system or component against this level of threat. For SL-A, this means that the asset owner, system integrator, product supplier and/or any combination of these has configured the zone, system or component to meet the particular security requirements defined for that SL.

The language used for each of the SLs uses terms like casual, coincidental, simple, sophisticated and extended. This language is intentionally vague to allow the same basic language to be used for all of the documents in the IEC 62443 series. Each of the individual documents in the series will define the requirements for the SLs that apply to their particular purpose.

While the requirements for each of the SLs will be different throughout the IEC 62443 series, there needs to be a general understanding of what each of the SLs should protect against. The following sections will provide some guidance on how to differentiate between the SLs.

A.3.2.2 SL 0: No specific requirements or security protection necessary

SL 0 has multiple meanings depending on the situation in which it is applied. In defining SL-C it would mean that the component or system fails to meet some of the SL 1 requirements for that particular FR. This would most likely be for components or systems that would be part of a larger zone where other components or systems would provide compensating countermeasures. In defining SL-T for a particular zone it means that the asset owner has determined that the results of their risk analysis indicate that less than the full SL 1 specific requirements are necessary for that particular FR on that component or system. This would more likely happen for individual components within a system or zone that do not contribute in any way to the FR-specific requirements. In defining SL-A it would mean that the particular zone fails to meet some of the SL 1 requirements for that particular FR.

A.3.2.3 SL 1: Protection against casual or coincidental violation

Casual or coincidental violations of security are usually through the lax application of security policies. These can be caused by well-meaning employees just as easily as they can be by an outsider threat. Many of these violations will be security program related and will be handled by enforcing policies and procedures.

Using Figure A.1, a simple example would be an operator able to change a set point on the engineering station in the BPCS zone to a value outside certain conditions determined by the engineering staff. The system did not enforce the proper authentication and use control restrictions to disallow the change by the operator. Also using Figure A.1, another example would be a password being sent in clear text over the conduit between the BPCS zone and the DMZ zone, allowing a network engineer to view the password while troubleshooting the system. The system did not enforce proper data confidentiality to protect the password. Using

Figure A.2, a third example would be an engineer that means to access the PLC in Industrial Network #1 but actually accesses the PLC in Industrial Network #2. The system did not enforce the proper restriction of data flow preventing the engineer from accessing the wrong system.

A.3.2.4 SL 2: Protection against intentional violation using simple means with low resources, generic skills and low motivation

Simple means do not require much knowledge on the part of the attacker. The attacker does not need detailed knowledge of security, the domain or the particular system under attack. These attack vectors are well known and there may be automated tools for aiding the attacker. They are also designed to attack a wide range of systems instead of targeting a specific system, so an attacker does not need a significant level of motivation or resources at hand.

Using Figure A.1, an example would be a virus that infects the maintenance workstation in the Plant DMZ zone spreading to the BPCS engineering workstation since they both use the same general purpose operating system. Using Figure A.2, another example would be an attacker compromising a web server in the enterprise network by an exploit downloaded from the Internet for a publicly known vulnerability in the general purpose operating system of the web server. The attacker uses the web server as a pivot point in an attack against other systems in the enterprise network as well as the industrial network. Also using Figure A.2, a third example would be an operator that views a website on the HMI located in Industrial Network #1 which downloads a Trojan that opens a hole in the routers and firewalls to the Internet.

A.3.2.5 SL 3: Protection against intentional violation using sophisticated means with moderate resources, IACS specific skills and moderate motivation

Sophisticated means require advanced security knowledge, advanced domain knowledge, advanced knowledge of the target system or any combination of these. An attacker going after a SL 3 system will likely be using attack vectors that have been customized for the specific target system. The attacker may use exploits in operating systems that are not well known, weaknesses in industrial protocols, specific information about a particular target to violate the security of the system or other means that require a greater motivation as well as skill and knowledge set than are required for SL 1 or 2.

An example of sophisticated means could be password or key cracking tools based on hash tables. These tools are available for download, but applying them takes knowledge of the system (such as the hash of a password to crack). Using Figure A.1, another example would be an attacker that gains access to the FS-PLC through the serial conduit after gaining access to the control PLC through a vulnerability in the Ethernet controller. Using Figure A.2, a third example would be an attacker that gains access to the data historian by using a brute-force attack through the industrial/enterprise DMZ firewall initiated from the enterprise wireless network.

A.3.2.6 SL 4: Protection against intentional violation using sophisticated means with extended resources, IACS specific skills and high motivation

SL 3 and SL 4 are very similar in that they both involve sophisticated means used to violate the security requirements of the system. The difference comes from the attacker being even more motivated and having extended resources at their disposal. These may involve high-performance computing resources, large numbers of computers or extended periods of time.

An example of sophisticated means with extended resources would be using super computers or computer clusters to conduct brute-force password cracking using large hash tables. Another example would be a botnet used to attack a system using multiple attack vectors at once. A third example would be an organized crime organization that has the motivation and resources to spend weeks attempting to analyze a system and develop custom “zero-day” exploits.

A.3.3 SL vector format

A vector can be used to describe the security requirements for a zone, conduit, component or system better than a single number. This vector may contain either a specific SL requirement or a zero value for each of the foundational requirements (see A.3.1).

FORMAT → SL-?([FR,]domain) = { IAC UC SI DC RDF TRE RA }

where

SL-? = (Required) The SL type (see A.2.2). The possible formats are:

- SL-T = Target SL
- SL-A = Achieved SL
- SL-C = Capabilities SL

[FR,] = (Optional) Field indicating the FR that the SL value applies. The FRs are written out in abbreviated form instead of numerical form to aid in readability.

domain = (Required) The applicable domain that the SL applies. Domains can refer to zones, control systems, subsystems or components. Some examples of different domains from Figure A.1 are SIS zone, BPCS zone, BPCS HMI, Plant DMZ domain controller, Plant DMZ to Control Center conduit and SIS to BPCS serial conduit. In this particular standard, all requirements refer to a control system, so the domain term is not used as it would be by other documents in the IEC 62443 series.

EXAMPLE 1 → SL-T(BPCS Zone) = { 2 2 0 1 3 1 3 }

EXAMPLE 2 → SL-C(SIS Engineering Workstation) = { 3 3 2 3 0 0 1 }

EXAMPLE 3 → SL-C(RA, FS-PLC) = 4

NOTE The last example specifies only the RA component of a 7-dimension SL-C.

Annex B
(informative)

Mapping of SRs and REs to FR SL levels 1-4

B.1 Overview

This annex is intended to provide overall guidance to the reader as to how SL levels 0 to 4 are differentiated on an FR-by-FR basis via the defined SRs and their associated REs.

B.2 SL mapping table

Table B.1 indicates which system level requirements apply to which FRs for a given system capability SL – SL-C(xx, control system). For a given FR, the required system level requirements to meet a given SL-C are denoted by a check mark. Thus, as an example, the SL=1 system security capabilities for FR 5 (or SL-C(RDF, control system)=1), would include the base requirements of all four defined SRs. A system unable to meet all four of these SRs would have an SL-C(RDF, control system)=0. To meeting SL-C(RDF, control system)=2, a system needs to support the four SR base requirements plus RE(1) of SR 5.1 and SR 5.2. As another example, only the SR 6.1 base requirement is required to meet SL-C(TRE, control system)=1, but both SRs defined are required in order to meet SL-C(TRE, control system)=2. Refer to A.3.3 for how a full SL vector would be denoted.

Table B.1 – Mapping of SRs and REs to FR SL levels 1-4 *(1 of 4)*

SRs and REs		SL 1	SL 2	SL 3	SL 4
FR 1 – Identification and authentication control (IAC)					
SR 1.1 – Human user identification and authentication	5.3	✓	✓	✓	✓
SR 1.1 RE 1 – Unique identification and authentication	5.3.3.1		✓	✓	✓
SR 1.1 RE 2 – Multifactor authentication for untrusted networks	5.3.3.2			✓	✓
SR 1.1 RE 3 – Multifactor authentication for all networks	5.3.3.3				✓
SR 1.2 – Software process and device identification and authentication	5.4		✓	✓	✓
SR 1.2 RE 1 – Unique identification and authentication	5.4.3.1			✓	✓
SR 1.3 – Account management	5.5	✓	✓	✓	✓
SR 1.3 RE 1 – Unified account management	5.5.3.1			✓	✓
SR 1.4 – Identifier management	5.6	✓	✓	✓	✓
SR 1.5 – Authenticator management	5.7	✓	✓	✓	✓
SR 1.5 RE 1 – Hardware security for software process identity credentials	5.7.3.1			✓	✓
SR 1.6 – Wireless access management	5.8	✓	✓	✓	✓
SR 1.6 RE 1 – Unique identification and authentication	5.8.3.1		✓	✓	✓
SR 1.7 – Strength of password-based authentication	5.9	✓	✓	✓	✓
SR 1.7 RE 1 – Password generation and lifetime restrictions for human users	5.9.3.1			✓	✓

Table B.1 *(2 of 4)*

SRs and REs		SL 1	SL 2	SL 3	SL 4
SR 1.7 RE 2 – Password lifetime restrictions for all users	5.9.3.2				✓
SR 1.8 – Public key infrastructure certificates	5.10		✓	✓	✓
SR 1.9 – Strength of public key authentication	5.11		✓	✓	✓
SR 1.9 RE 1 – Hardware security for public key authentication	5.11.3.1			✓	✓
SR 1.10 – Authenticator feedback	5.12	✓	✓	✓	✓
SR 1.11 – Unsuccessful login attempts	5.13	✓	✓	✓	✓
SR 1.12 – System use notification	5.14	✓	✓	✓	✓
SR 1.13 – Access via untrusted networks	5.15	✓	✓	✓	✓
SR 1.13 RE 1 – Explicit access request approval	5.15.3.1		✓	✓	✓
FR 2 – Use control (UC)					
SR 2.1 – Authorization enforcement	6.3	✓	✓	✓	✓
SR 2.1 RE 1 – Authorization enforcement for all users	6.3.3.1		✓	✓	✓
SR 2.1 RE 2 – Permission mapping to roles	6.3.3.2		✓	✓	✓
SR 2.1 RE 3 – Supervisor override	6.3.3.3			✓	✓
SR 2.1 RE 4 – Dual approval	6.3.3.4				✓
SR 2.2 – Wireless use control	6.4	✓	✓	✓	✓
SR 2.2 RE 1 – Identify and report unauthorized wireless devices	6.4.3.1			✓	✓
SR 2.3 – Use control for portable and mobile devices	6.5	✓	✓	✓	✓
SR 2.3 RE 1 – Enforcement of security status of portable and mobile devices	6.5.3.1			✓	✓
SR 2.4 – Mobile code	6.6	✓	✓	✓	✓
SR 2.4 RE 1 – Mobile code integrity check	6.6.3.1			✓	✓
SR 2.5 – Session lock	6.7	✓	✓	✓	✓
SR 2.6 – Remote session termination	6.8		✓	✓	✓
SR 2.7 – Concurrent session control	6.9			✓	✓
SR 2.8 – Auditable events	6.10	✓	✓	✓	✓
SR 2.8 RE 1 – Centrally managed, system-wide audit trail	6.10.3.1			✓	✓
SR 2.9 – Audit storage capacity	6.11	✓	✓	✓	✓
SR 2.9 RE 1 – Warn when audit record storage capacity threshold reached	6.11.3.1			✓	✓
SR 2.10 – Response to audit processing failures	6.12	✓	✓	✓	✓
SR 2.11 – Timestamps	6.13		✓	✓	✓
SR 2.11 RE 1 – Internal time synchronization	6.13.3.1			✓	✓
SR 2.11 RE 2 – Protection of time source integrity	6.13.3.2				✓
SR 2.12 – Non-repudiation	6.14			✓	✓
SR 2.12 RE 1 – Non-repudiation for all users	6.14.3.1				✓

Table B.1 *(3 of 4)*

SRs and REs		SL 1	SL 2	SL 3	SL 4
FR 3 – System integrity (SI)					
SR 3.1 – Communication integrity	7.3	✓	✓	✓	✓
SR 3.1 RE 1 – Cryptographic integrity protection	7.3.3.1			✓	✓
SR 3.2 – Malicious code protection	7.4	✓	✓	✓	✓
SR 3.2 RE 1 – Malicious code protection on entry and exit points	7.4.3.1		✓	✓	✓
SR 3.2 RE 2 – Central management and reporting for malicious code protection	7.4.3.2			✓	✓
SR 3.3 – Security functionality verification	7.5	✓	✓	✓	✓
SR 3.3 RE 1 – Automated mechanisms for security functionality verification	7.5.3.1			✓	✓
SR 3.3 RE 2 – Security functionality verification during normal operation	7.5.3.2				✓
SR 3.4 – Software and information integrity	7.6		✓	✓	✓
SR 3.4 RE 1 – Automated notification about integrity violations	7.6.3.1			✓	✓
SR 3.5 – Input validation	7.7	✓	✓	✓	✓
SR 3.6 – Deterministic output	7.8	✓	✓	✓	✓
SR 3.7 – Error handling	7.9		✓	✓	✓
SR 3.8 – Session integrity	7.10		✓	✓	✓
SR 3.8 RE 1 – Invalidation of session IDs after session termination	7.10.3.1			✓	✓
SR 3.8 RE 2 – Unique session ID generation	7.10.3.2			✓	✓
SR 3.8 RE 3 – Randomness of session IDs	7.10.3.3				✓
SR 3.9 – Protection of audit information	7.11		✓	✓	✓
SR 3.9 RE 1 – Audit records on write-once media	7.11.3.1				✓
FR 4 – Data confidentiality (DC)					
SR 4.1 – Information confidentiality	8.3	✓	✓	✓	✓
SR 4.1 RE 1 – Protection of confidentiality at rest or in transit via untrusted networks	8.3.3.1		✓	✓	✓
SR 4.1 RE 2 – Protection of confidentiality across zone boundaries	8.3.3.2				✓
SR 4.2 – Information persistence	8.4		✓	✓	✓
SR 4.2 RE 1 – Purging of shared memory resources	8.4.3.1			✓	✓
SR 4.3 – Use of cryptography	8.5	✓	✓	✓	✓
FR 5 – Restricted data flow (RDF)					
SR 5.1 – Network segmentation	9.3	✓	✓	✓	✓
SR 5.1 RE 1 – Physical network segmentation	9.3.3.1		✓	✓	✓
SR 5.1 RE 2 – Independence from non-control system networks	9.3.3.2			✓	✓
SR 5.1 RE 3 – Logical and physical isolation of critical networks	9.3.3.3				✓

Table B.1 *(4 of 4)*

SRs and REs		SL 1	SL 2	SL 3	SL 4
SR 5.2 – Zone boundary protection	9.4	✓	✓	✓	✓
SR 5.2 RE 1 – Deny by default, allow by exception	9.4.3.1		✓	✓	✓
SR 5.2 RE 2 – Island mode	9.4.3.2			✓	✓
SR 5.2 RE 3 – Fail close	9.4.3.3			✓	✓
SR 5.3 – General purpose person-to-person communication restrictions	9.5	✓	✓	✓	✓
SR 5.3 RE 1 – Prohibit all general purpose person-to-person communications	9.5.3.1			✓	✓
SR 5.4 – Application partitioning	9.6	✓	✓	✓	✓
FR 6 – Timely response to events (TRE)					
SR 6.1 – Audit log accessibility	10.3	✓	✓	✓	✓
SR 6.1 RE 1 – Programmatic access to audit logs	10.3.3.1			✓	✓
SR 6.2 – Continuous monitoring	10.4		✓	✓	✓
FR 7 – Resource availability (RA)					
SR 7.1 – Denial of service protection	11.3	✓	✓	✓	✓
SR 7.1 RE 1 – Manage communication loads	11.3.3.1		✓	✓	✓
SR 7.1 RE 2 – Limit DoS effects to other systems or networks	11.3.3.2			✓	✓
SR 7.2 – Resource management	11.4	✓	✓	✓	✓
SR 7.3 – Control system backup	11.5	✓	✓	✓	✓
SR 7.3 RE 1 – Backup verification	11.5.3.1		✓	✓	✓
SR 7.3 RE 2 – Backup automation	11.5.3.2			✓	✓
SR 7.4 – Control system recovery and reconstitution	11.6	✓	✓	✓	✓
SR 7.5 – Emergency power	11.7	✓	✓	✓	✓
SR 7.6 – Network and security configuration settings	11.8	✓	✓	✓	✓
SR 7.6 RE 1 – Machine-readable reporting of current security settings	11.8.3.1			✓	✓
SR 7.7 – Least functionality	11.9	✓	✓	✓	✓
SR 7.8 – Control system component inventory	11.10		✓	✓	✓

Bibliography

NOTE 1 This bibliography includes references to sources used in the creation of this standard as well as references to sources that may aid the reader in developing a greater understanding of cyber security as a whole and of the process of developing a cyber-security management system. Not all references in this bibliography are referred to throughout the text of this standard. The references have been grouped into different categories based on their source.

References to other parts, both existing and in progress, of the IEC 62443 series:

NOTE 2 These references are not all published documents; some of them are in development. They are listed here for completeness of the currently authorized parts of the IEC 62443 series.

[1] IEC/TR 62443-1-2, *Industrial communication networks – Network and system security – Part 1-2: Master glossary of terms and abbreviations*[3]

[2] IEC/TS 62443-1-3, *Industrial communication networks – Network and system security – Part 1-3: System security compliance metrics*[4]

[3] IEC/TR 62443-1-4, *Industrial communication networks – Network and system security – Part 1-4: IACS security lifecycle and use-case*[5]

[4] IEC/TR 62443-2-2, *Industrial communication networks – Network and system security – Part 2-2: Implementation guidance for an IACS security management system*[6]

[5] IEC/TR 62443-2-3, *Industrial communication networks – Network and system security – Part 2-3: Patch management in the IACS environment*[7]

[6] IEC 62443-2-4, *Industrial communication networks – Network and system security – Part 2-4: Installation and maintenance requirements for IACS suppliers*[8]

[7] IEC/TR 62443-3-1, *Industrial communication networks – Network and system security – Part 3-1: Security technologies for industrial automation and control systems*

[8] IEC 62443-3-2, *Industrial communication networks – Network and system security – Part 3-2: Security levels for zones and conduits*[9]

[9] IEC 62443-4-1, *Industrial communication networks – Network and system security – Part 4-1: Product development requirements*[10]

[10] IEC 62443-4-2, *Industrial communication networks – Network and system security – Part 4-2: Technical security requirements for IACS components*[11]

3 Under consideration.

4 To be published.

5 Under consideration.

6 Under consideration.

7 Under consideration.

8 To be published.

9 Under consideration.

10 Under consideration.

11 Under consideration.

Other standards references:

[11] ISO/IEC Directives, Part 2:2011, *Rules for the structure and drafting of International Standards*

[12] ISO/IEC 19790, *Information technology – Security techniques – Security requirements for cryptographic modules*

[13] ISO/IEC 27002, *Information technology – Security techniques – Code of practice for information security management*

[14] NERC CIP-002, *Cyber Security – Critical Cyber Asset Identification*

[15] NERC CIP-003, *Cyber Security – Security Management Controls*

[16] NERC CIP-004, *Cyber Security – Personnel & Training*

[17] NERC CIP-005, *Cyber Security – Electronic Security Perimeter(s)*

[18] NERC CIP-006, *Cyber Security – Physical Security of Critical Cyber Assets*

[19] NERC CIP-007, *Cyber Security – Systems Security Management*

[20] NERC CIP-008, *Cyber Security – Incident Reporting and Response Planning*

[21] NERC CIP-009, *Cyber Security – Recovery Plans for Critical Cyber Assets*

[22] NIST FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*

[23] NIST SP800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*

[24] NIST SP800-53 Rev. 3, *Recommended Security Controls for Federal Information Systems and Organizations*

[25] NIST SP800-57, *Recommendation for Key Management*

[26] NIST SP800-82, *Guide to Industrial Control Systems (ICS) Security*

[27] NIST SP800-92, *Guide to Computer Security Log Management*

Other documents and published resources:

[28] Gilsinn, J.D., Schierholz, R., *Security Assurance Levels: A Vector Approach to Describing Security Requirements*, NIST Publication 906330, October 20, 2010.

[29] IETF RFC 3647, Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework

[30] Digital Bond Bandolier project, available at http://www.digitalbond.com/tools/bandolier/

[31] Open Web Application Security Project (OWASP), available at http://www.owasp.org/

SOMMAIRE

AVANT-PROPOS 89
0 Introduction 91
0.1 Vue d'ensemble 91
0.2 Objectif et public visé 92
0.3 Utilisation dans d'autres parties de la série IEC 62443 93
1 Domaine d'application 95
2 Références normatives 95
3 Termes, définitions, termes abrégés, acronymes et conventions 96
3.1 Termes et définitions 96
3.2 Termes abrégés et acronymes 101
3.3 Conventions 103
4 Contraintes communes de sécurité du système de commande 104
4.1 Présentation 104
4.2 Prise en charge des fonctions essentielles 104
4.3 Contre-mesures compensatoires 105
4.4 Moindre privilège 106
5 FR 1– Commande d'identification et d'authentification 106
5.1 Objectif et descriptions du SL-C(IAC) 106
5.2 Justification 106
5.3 SR 1.1 – Identification et authentification d'utilisateur humain 106
5.3.1 Exigence 106
5.3.2 Justification et recommandations supplémentaires 106
5.3.3 Améliorations d'exigences 107
5.3.4 Niveaux de sécurité 107
5.4 SR 1.2 – Identification et authentification du processus logiciel et de l'appareil 108
5.4.1 Exigence 108
5.4.2 Justification et recommandations supplémentaires 108
5.4.3 Améliorations d'exigences 109
5.4.4 Niveaux de sécurité 109
5.5 SR 1.3 – Gestion des comptes 109
5.5.1 Exigence 109
5.5.2 Justification et recommandations supplémentaires 109
5.5.3 Améliorations d'exigences 109
5.5.4 Niveaux de sécurité 109
5.6 SR 1.4 – Gestion des identificateurs 110
5.6.1 Exigence 110
5.6.2 Justification et recommandations supplémentaires 110
5.6.3 Améliorations d'exigences 110
5.6.4 Niveaux de sécurité 110
5.7 SR 1.5 – Gestion des authentifiants 110
5.7.1 Exigence 110
5.7.2 Justification et recommandations supplémentaires 111
5.7.3 Améliorations d'exigences 112
5.7.4 Niveaux de sécurité 112
5.8 SR 1.6 – Gestion des accès sans fil 112
5.8.1 Exigence 112

5.8.2 Justification et recommandations supplémentaires 112
5.8.3 Améliorations d'exigences 112
5.8.4 Niveaux de sécurité 112
5.9 SR 1.7 – Force de l'authentification basée sur le mot de passe 113
5.9.1 Exigence 113
5.9.2 Justification et recommandations supplémentaires 113
5.9.3 Améliorations d'exigences 113
5.9.4 Niveaux de sécurité 114
5.10 SR 1.8 – Certificats d'infrastructure à clés publiques (ICP) 114
5.10.1 Exigence 114
5.10.2 Justification et recommandations supplémentaires 114
5.10.3 Améliorations d'exigences 114
5.10.4 Niveaux de sécurité 114
5.11 SR 1.9 – Force de l'authentification de clé publique 114
5.11.1 Exigence 114
5.11.2 Justification et recommandations supplémentaires 115
5.11.3 Améliorations d'exigences 115
5.11.4 Niveaux de sécurité 115
5.12 SR 1.10 – Rétroaction de l'authentifiant 116
5.12.1 Exigence 116
5.12.2 Justification et recommandations supplémentaires 116
5.12.3 Améliorations d'exigences 116
5.12.4 Niveaux de sécurité 116
5.13 SR 1.11 – Tentatives d'authentification infructueuses 116
5.13.1 Exigence 116
5.13.2 Justification et recommandations supplémentaires 116
5.13.3 Améliorations d'exigences 117
5.13.4 Niveaux de sécurité 117
5.14 SR 1.12 – Notification d'utilisation du système 117
5.14.1 Exigence 117
5.14.2 Justification et recommandations supplémentaires 117
5.14.3 Améliorations d'exigences 117
5.14.4 Niveaux de sécurité 117
5.15 SR 1.13 – Accès par des réseaux non sécurisés 118
5.15.1 Exigence 118
5.15.2 Justification et recommandations supplémentaires 118
5.15.3 Améliorations d'exigences 118
5.15.4 Niveaux de sécurité 118
6 FR 2 – Commande d'utilisation 118
6.1 Objectif et descriptions du SL-C(UC) 118
6.2 Justification 119
6.3 SR 2.1 – Application de l'autorisation 119
6.3.1 Exigence 119
6.3.2 Justification et recommandations supplémentaires 119
6.3.3 Améliorations d'exigences 120
6.3.4 Niveaux de sécurité 120
6.4 SR 2.2 –Contrôle d'utilisation sans fil 120
6.4.1 Exigence 120
6.4.2 Justification et recommandations supplémentaires 121

6.4.3 Améliorations d'exigences 121
6.4.4 Niveaux de sécurité 121
6.5 SR 2.3 – Contrôle d'utilisation des appareils mobiles et portables 121
6.5.1 Exigence 121
6.5.2 Justification et recommandations supplémentaires 121
6.5.3 Améliorations d'exigences 122
6.5.4 Niveaux de sécurité 122
6.6 SR 2.4 – Code mobile 122
6.6.1 Exigence 122
6.6.2 Justification et recommandations supplémentaires 122
6.6.3 Améliorations d'exigences 122
6.6.4 Niveaux de sécurité 123
6.7 SR 2.5 – Verrouillage de session 123
6.7.1 Exigence 123
6.7.2 Justification et recommandations supplémentaires 123
6.7.3 Améliorations d'exigences 123
6.7.4 Niveaux de sécurité 123
6.8 SR 2.6 – Terminaison de session distante 123
6.8.1 Exigence 123
6.8.2 Justification et recommandations supplémentaires 124
6.8.3 Améliorations d'exigences 124
6.8.4 Niveaux de sécurité 124
6.9 SR 2.7 – Commande de sessions concomitantes 124
6.9.1 Exigence 124
6.9.2 Justification et recommandations supplémentaires 124
6.9.3 Améliorations d'exigences 124
6.9.4 Niveaux de sécurité 124
6.10 SR 2.8 – Événements auditables 125
6.10.1 Exigence 125
6.10.2 Justification et recommandations supplémentaires 125
6.10.3 Améliorations d'exigences 125
6.10.4 Niveaux de sécurité 125
6.11 SR 2.9 – Capacité de stockage de l'audit 126
6.11.1 Exigence 126
6.11.2 Justification et recommandations supplémentaires 126
6.11.3 Améliorations d'exigences 126
6.11.4 Niveaux de sécurité 126
6.12 SR 2.10 – Réponse aux échecs de traitement d'audit 126
6.12.1 Exigence 126
6.12.2 Justification et recommandations supplémentaires 126
6.12.3 Améliorations d'exigences 127
6.12.4 Niveaux de sécurité 127
6.13 SR 2.11– Horodatages 127
6.13.1 Exigence 127
6.13.2 Justification et recommandations supplémentaires 127
6.13.3 Améliorations d'exigences 127
6.13.4 Niveaux de sécurité 127
6.14 SR 2.12 – Non-répudiation 128
6.14.1 Exigence 128

6.14.2 Justification et recommandations supplémentaires 128
6.14.3 Améliorations d'exigences 128
6.14.4 Niveaux de sécurité 128
7 FR 3 – Intégrité du système 128
7.1 Objectif et descriptions du SL-C(SI) 128
7.2 Justification 129
7.3 SR 3.1 – Intégrité de la communication 129
7.3.1 Exigence 129
7.3.2 Justification et recommandations supplémentaires 129
7.3.3 Améliorations d'exigences 130
7.3.4 Niveaux de sécurité 130
7.4 SR 3.2 – Protection contre les programmes malveillants 130
7.4.1 Exigence 130
7.4.2 Justification et recommandations supplémentaires 130
7.4.3 Améliorations d'exigences 131
7.4.4 Niveaux de sécurité 131
7.5 SR 3.3 – Vérification des fonctionnalités de sécurité 131
7.5.1 Exigence 131
7.5.2 Justification et recommandations supplémentaires 131
7.5.3 Améliorations d'exigences 132
7.5.4 Niveaux de sécurité 132
7.6 SR 3.4 – Intégrité du logiciel et des informations 132
7.6.1 Exigence 132
7.6.2 Justification et recommandations supplémentaires 132
7.6.3 Améliorations d'exigences 133
7.6.4 Niveaux de sécurité 133
7.7 SR 3.5 – Validation en entrée 133
7.7.1 Exigence 133
7.7.2 Justification et recommandations supplémentaires 133
7.7.3 Améliorations d'exigences 133
7.7.4 Niveaux de sécurité 134
7.8 SR 3.6 – Sortie déterministe 134
7.8.1 Exigence 134
7.8.2 Justification et recommandations supplémentaires 134
7.8.3 Améliorations d'exigences 134
7.8.4 Niveaux de sécurité 134
7.9 SR 3.7 – Traitement des erreurs 134
7.9.1 Exigence 134
7.9.2 Justification et recommandations supplémentaires 134
7.9.3 Améliorations d'exigences 135
7.9.4 Niveaux de sécurité 135
7.10 SR 3.8 – Intégrité de la session 135
7.10.1 Exigence 135
7.10.2 Justification et recommandations supplémentaires 135
7.10.3 Améliorations d'exigences 135
7.10.4 Niveaux de sécurité 136
7.11 SR 3.9 – Protection des informations d'audit 136
7.11.1 Exigence 136
7.11.2 Justification et recommandations supplémentaires 136

7.11.3 Améliorations d'exigences 136
7.11.4 Niveaux de sécurité 136
8 FR 4 – Confidentialité des données 136
8.1 Objectif et descriptions du SL-C(DC) 136
8.2 Justification 137
8.3 SR 4.1 – Confidentialité des informations 137
8.3.1 Exigence 137
8.3.2 Justification et recommandations supplémentaires 137
8.3.3 Améliorations d'exigences 138
8.3.4 Niveaux de sécurité 138
8.4 SR 4.2 – Persistance des informations 138
8.4.1 Exigence 138
8.4.2 Justification et recommandations supplémentaires 138
8.4.3 Améliorations d'exigences 139
8.4.4 Niveaux de sécurité 139
8.5 SR 4.3 – Utilisation de la cryptographie 139
8.5.1 Exigence 139
8.5.2 Justification et recommandations supplémentaires 139
8.5.3 Améliorations d'exigences 140
8.5.4 Niveaux de sécurité 140
9 FR 5 – Flux de données réduit 140
9.1 Objectif et descriptions du SL-C(RDF) 140
9.2 Justification 140
9.3 SR 5.1 – Segmentation des réseaux 140
9.3.1 Exigence 140
9.3.2 Justification et recommandations supplémentaires 140
9.3.3 Améliorations d'exigences 141
9.3.4 Niveaux de sécurité 141
9.4 SR 5.2 – Protection des limites de zone 142
9.4.1 Exigence 142
9.4.2 Justification et recommandations supplémentaires 142
9.4.3 Améliorations d'exigences 142
9.4.4 Niveaux de sécurité 142
9.5 SR 5.3 – Restrictions de communication de personne à personne à visée générale 143
9.5.1 Exigence 143
9.5.2 Justification et recommandations supplémentaires 143
9.5.3 Améliorations d'exigences 143
9.5.4 Niveaux de sécurité 144
9.6 SR 5.4 – Partitionnement d'application 144
9.6.1 Exigence 144
9.6.2 Justification et recommandations supplémentaires 144
9.6.3 Améliorations d'exigences 144
9.6.4 Niveaux de sécurité 144
10 FR 6 – Réponse rapide aux événements 144
10.1 Objectif et descriptions du SL-C(TRE) 144
10.2 Justification 145
10.3 SR 6.1 – Accessibilité du journal d'audit 145
10.3.1 Exigence 145

10.3.2 Justification et recommandations supplémentaires 145
10.3.3 Améliorations d'exigences 145
10.3.4 Niveaux de sécurité 145
10.4 SR 6.2 – Surveillance permanente 146
10.4.1 Exigence 146
10.4.2 Justification et recommandations supplémentaires 146
10.4.3 Améliorations d'exigences 146
10.4.4 Niveaux de sécurité 146
11 FR 7 – Disponibilité des ressources 146
11.1 Objectif et descriptions du SL-C(RA) 146
11.2 Justification 147
11.3 SR 7.1 – Protection contre le refus de service 147
11.3.1 Exigence 147
11.3.2 Justification et recommandations supplémentaires 147
11.3.3 Améliorations d'exigences 147
11.3.4 Niveaux de sécurité 147
11.4 SR 7.2 – Gestion des ressources 148
11.4.1 Exigence 148
11.4.2 Justification et recommandations supplémentaires 148
11.4.3 Améliorations d'exigences 148
11.4.4 Niveaux de sécurité 148
11.5 SR 7.3 – Sauvegarde du système de commande 148
11.5.1 Exigence 148
11.5.2 Justification et recommandations supplémentaires 148
11.5.3 Améliorations d'exigences 149
11.5.4 Niveaux de sécurité 149
11.6 SR 7.4 – Récupération et reconstitution du système de commande 149
11.6.1 Exigence 149
11.6.2 Justification et recommandations supplémentaires 149
11.6.3 Améliorations d'exigences 149
11.6.4 Niveaux de sécurité 149
11.7 SR 7.5 – Alimentation d'urgence 150
11.7.1 Exigence 150
11.7.2 Justification et recommandations supplémentaires 150
11.7.3 Améliorations d'exigences 150
11.7.4 Niveaux de sécurité 150
11.8 SR 7.6 – Paramètres de configuration de sécurité et de réseau 150
11.8.1 Exigence 150
11.8.2 Justification et recommandations supplémentaires 150
11.8.3 Améliorations d'exigences 150
11.8.4 Niveaux de sécurité 151
11.9 SR 7.7 – Moindre fonctionnalité 151
11.9.1 Exigence 151
11.9.2 Justification et recommandations supplémentaires 151
11.9.3 Améliorations d'exigences 151
11.9.4 Niveaux de sécurité 151
11.10 SR 7.8 – Inventaire de composants du système de commande 151
11.10.1 Exigence 151
11.10.2 Justification et recommandations supplémentaires 151

11.10.3 Améliorations d'exigences 152
11.10.4 Niveaux de sécurité 152
Annexe A (informative) Analyse du vecteur SL 153
A.1 Présentation 153
A.2 Niveaux de sécurité 153
A.2.1 Définition 153
A.2.2 Types de SL 154
A.2.3 Utilisation des SL 154
A.3 Vecteur SL 160
A.3.1 Exigences fondamentales 160
A.3.2 Définitions des niveaux 160
A.3.3 Format du vecteur SL 162
Annexe B (informative) Mapping des SR et RE aux FR SL 1-4 164
B.1 Présentation 164
B.2 Tableau de mapping des SL 164
Bibliographie 168
Références à d'autres parties, existantes et en cours, de la série IEC 62443: 168
Autres normes de référence: 169
Autres documents et ressources publiées: 169

Figure 1 – Structure de la série IEC 62443 93
Figure A.1 – Exemple d'industrie de traitement de haut niveau représentant les zones et conduits 157
Figure A.2 – Exemple de fabrication de haut niveau représentant les zones et conduits 158
Figure A.3 – Schéma de corrélation de l'utilisation de différents types de SL 159

Tableau B.1 – Mapping des SR et RE aux niveaux FR SL 1-4 *(1 sur 4)* 164

COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

_____

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

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

AVANT-PROPOS

1) La Commission Électrotechnique Internationale (IEC) est une organisation mondiale de normalisation composée de l'ensemble des comités électrotechniques nationaux (Comités nationaux de l'IEC). L'IEC a pour objet de favoriser la coopération internationale pour toutes les questions de normalisation dans les domaines de l'électricité et de l'électronique. À cet effet, l'IEC – entre autres activités – publie des Normes internationales, des Spécifications techniques, des Rapports techniques, des Spécifications accessibles au public (PAS) et des Guides (ci-après dénommés "Publication(s) de l'IEC"). Leur élaboration est confiée à des comités d'études, aux travaux desquels tout Comité national intéressé par le sujet traité peut participer. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'IEC, participent également aux travaux. L'IEC collabore étroitement avec l'Organisation Internationale de Normalisation (ISO), selon des conditions fixées par accord entre les deux organisations.
2) Les décisions ou accords officiels de l'IEC concernant les questions techniques représentent, dans la mesure du possible, un accord international sur les sujets étudiés, étant donné que les Comités nationaux de l'IEC intéressés sont représentés dans chaque comité d'études.
3) Les Publications de l'IEC se présentent sous la forme de recommandations internationales et sont agréées comme telles par les Comités nationaux de l'IEC. Tous les efforts raisonnables sont entrepris afin que l'IEC s'assure de l'exactitude du contenu technique de ses publications; l'IEC ne peut pas être tenue responsable de l'éventuelle mauvaise utilisation ou interprétation qui en est faite par un quelconque utilisateur final.
4) Dans le but d'encourager l'uniformité internationale, les Comités nationaux de l'IEC s'engagent, dans toute la mesure possible, à appliquer de façon transparente les Publications de l'IEC dans leurs publications nationales et régionales. Toutes divergences entre toutes Publications de l'IEC et toutes publications nationales ou régionales correspondantes doivent être indiquées en termes clairs dans ces dernières.
5) L'IEC elle-même ne fournit aucune attestation de conformité. Des organismes de certification indépendants fournissent des services d'évaluation de conformité et, dans certains secteurs, accèdent aux marques de conformité de l'IEC. L'IEC n'est responsable d'aucun des services effectués par les organismes de certification indépendants.
6) Tous les utilisateurs doivent s'assurer qu'ils sont en possession de la dernière édition de cette publication.
7) Aucune responsabilité ne doit être imputée à l'IEC, à ses administrateurs, employés, auxiliaires ou mandataires, y compris ses experts particuliers et les membres de ses comités d'études et des Comités nationaux de l'IEC, pour tout préjudice causé en cas de dommages corporels et matériels, ou de tout autre dommage de quelque nature que ce soit, directe ou indirecte, ou pour supporter les coûts (y compris les frais de justice) et les dépenses découlant de la publication ou de l'utilisation de cette Publication de l'IEC ou de toute autre Publication de l'IEC, ou au crédit qui lui est accordé.
8) L'attention est attirée sur les références normatives citées dans cette publication. L'utilisation de publications référencées est obligatoire pour une application correcte de la présente publication.
9) L'attention est attirée sur le fait que certains des éléments de la présente Publication de l'IEC peuvent faire l'objet de droits de brevet. L'IEC ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de brevets et de ne pas avoir signalé leur existence.

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

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

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

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

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

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

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

Le comité a décidé que le contenu de cette publication ne sera pas modifié avant la date de stabilité indiquée sur le site web de l'IEC sous «http://webstore.iec.ch» dans les données relatives à la publication recherchée. À cette date, la publication sera

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

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

IMPORTANT – Le logo «colour inside» qui se trouve sur la page de couverture de cette publication indique qu'elle contient des couleurs qui sont considérées comme utiles à une bonne compréhension de son contenu. Les utilisateurs devraient, par conséquent, imprimer ce document en utilisant une imprimante couleur.

0 Introduction

0.1 Vue d'ensemble

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

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

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

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

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

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

---

1 Les chiffres entre crochets se réfèrent à la Bibliographie.

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

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

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

0.2 Objectif et public visé

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

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

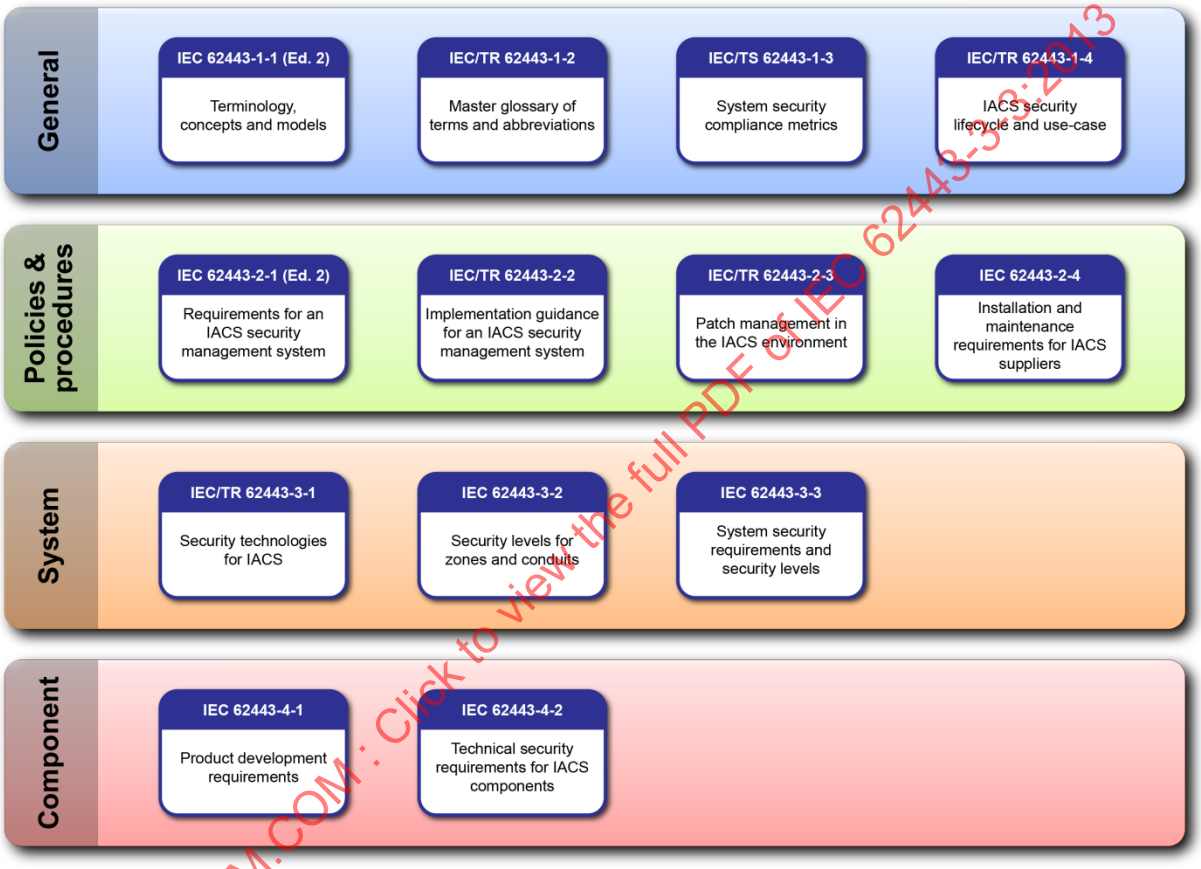
Lors de la conception d'un système de commande conformément à l'ensemble des SR associées aux SL-T spécifiques, il n'est pas nécessaire que chaque composant du système de commande proposé prenne en charge chaque exigence système au niveau imposé dans la présente norme. Des contre-mesures compensatoires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

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

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

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

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



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

Figure 1 – Structure de la série IEC 62443

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

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

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

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

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

1 Domaine d'application

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

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

a) Commande d'identification et d'authentification (IAC - *identification and authentication control*),

b) Commande d'utilisation (UC - *use control*),

c) Intégrité du système (SI - *system integrity*),

d) Confidentialité des données (DC - *data confidentiality*),

e) Flux de données réduit (RDF - *restricted data flow*),

f) Réponse rapide aux événements (TRE - *timely response to events*),

g) Disponibilité des ressources (RA - *ressource availability*).

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

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

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

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

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

3 Termes, définitions, termes abrégés, acronymes et conventions

3.1 Termes et définitions

Pour les besoins du présent document, les termes et définitions donnés dans l'IEC 62443-1-1 et dans l'IEC 62443-2-1, ainsi que les suivants s'appliquent.

NOTE Un grand nombre des termes et définitions suivants sont essentiellement fondés sur des sources appropriées provenant de l'Organisation internationale de normalisation (ISO), de la Commission électrotechnique internationale (IEC) ou de l'Institut national américain de technologie et des normes (NIST), parfois avec des modifications mineures permettant l'adaptation à la définition des exigences de sécurité du système de commande.

3.1.1
actif
objet logique ou physique ayant une valeur perçue ou réelle pour l'IACS

Note 1 à l'article: Dans la présente norme, un actif est n'importe quel élément dont il convient d'assurer la protection en tant que partie du système de gestion de la sécurité de l'IACS.

3.1.2
propriétaire d'actif
individu ou entreprise chargé(e) d'un ou de plusieurs IACS

Note 1 à l'article: Le terme «propriétaire d'actif» est utilisé à la place du terme générique «utilisateur final» pour marquer la distinction.

Note 2 à l'article: Cette définition inclut les composants faisant partie intégrante de l'IACS.

Note 3 à l'article: Dans le contexte de la présente norme, le propriétaire d'actif inclut également l'opérateur de l'IACS.

3.1.3
attaque
offensive sur un système issue d'une menace intelligente

Note 1 à l'article: Par exemple, une action intelligente est une tentative délibérée (plus particulièrement dans le sens d'une méthode ou d'une technique) de contournement des services de sécurité et de violation de la politique de sécurité d'un système

Note 2 à l'article: Il existe différentes classes d'attaques communément admises:

- une «attaque active» tente d'altérer les ressources du système ou de nuire à leur fonctionnement;
- une «attaque passive» tente de dérober ou d'utiliser les informations du système mais sans affecter les ressources;
- une «attaque interne» est une attaque initiée par une entité à l'intérieur du périmètre de sécurité (un «initié»), par exemple, une entité autorisée à accéder aux ressources du système mais qui les utilise de façon non approuvée par ceux qui ont donné l'autorisation;
- une «attaque externe» est initiée à l'extérieur du périmètre, par un utilisateur du système non autorisé ou illégitime (y compris par un initié attaquant depuis l'extérieur du périmètre de sécurité). Les attaquants externes potentiels vont des amateurs aux criminels organisés, aux terroristes internationaux et aux gouvernements hostiles.

3.1.4
authentification
stipulation garantissant qu'une caractéristique revendiquée d'une identité est correcte

Note 1 à l'article: L'authentification est généralement un prérequis permettant l'accès aux ressources d'un système de commande.

3.1.5
authentifiant
moyen utilisé pour confirmer l'identité d'un utilisateur (être humain, processus logiciel ou appareil)

Note 1 à l'article: Par exemple, un mot de passe ou un jeton peuvent être utilisés comme authentifiant.

3.1.6
authenticité
propriété garantissant qu'une entité est bien ce qu'elle revendique être

Note 1 à l'article: L'authenticité est généralement utilisée dans un contexte d'assurance de l'identité d'une entité, ou de validité d'une transmission, d'un message ou d'un émetteur de message.

3.1.7
automatique
processus ou appareil qui, sous des conditions spécifiques, fonctionne sans intervention humaine

3.1.8
disponibilité
propriété garantissant un accès fiable et rapide à l'utilisation des informations et à la fonctionnalité du système de commande

3.1.9
canal de communication
liaison de communication spécifique logique ou physique entre actifs

Note 1 à l'article: Un canal facilite l'établissement d'une connexion.

3.1.10
contre-mesure compensatoire
contre-mesure employée au lieu de ou en plus des capacités de sécurité inhérentes afin de satisfaire à une ou plusieurs exigences de sécurité

Note 1 à l'article: Des exemples comprennent:

- (au niveau du composant): une armoire verrouillée près d'un contrôleur ne comportant pas de contre-mesures de contrôle de cyberaccès suffisantes;
- (au niveau de la zone/du système de commande): un contrôle d'accès physique (protections, grilles et armes) permettant d'assurer la protection d'une pièce de commande et de restreindre l'accès à un groupe de personnel connu afin de compenser l'exigence technique du personnel identifié uniquement par l'IACS; et
- (au niveau du composant): un automate programmable (PLC, *programmable logic controller*) d'un fournisseur ne satisfait pas aux capacités de contrôle d'accès d'un utilisateur final, le fournisseur installe donc un pare-feu devant le PLC et le vend en tant que système.

3.1.11
autorité de conformité
entité ayant la compétence légale de déterminer la pertinence d'une évaluation, d'une mise en œuvre ou de l'efficacité de sécurité, comme cela est spécifié dans un document constitutif

3.1.12
conduit
groupement logique de canaux de communication, reliant deux ou plusieurs zones, qui partagent des exigences de sécurité communes

Note 1 à l'article: Un conduit est autorisé à traverser une zone tant que la sécurité des canaux contenus dans le conduit n'est pas affectée par la zone.

3.1.13
confidentialité
préservation des restrictions autorisées sur l'accès et la divulgation des informations, y compris les moyens de protection de la vie privée et des informations propriétaires

Note 1 à l'article: Lorsque ce terme est utilisé dans le contexte d'un IACS, il se réfère à la protection des données IACS et des informations d'un accès non autorisé.

3.1.14
connexion
association établie entre deux ou plusieurs points d'extrémité qui prend en charge l'établissement d'une session

3.1.15
conséquence
condition ou état qui suit logiquement ou naturellement un événement

3.1.16
système de commande
composants matériels et logiciels d'un IACS

3.1.17
contre-mesure
action, dispositif, procédure ou technique qui réduit une menace, une vulnérabilité ou une attaque en l'éliminant ou l'empêchant, en réduisant le plus possible les dommages qu'elle cause, ou en la découvrant et la consignant afin que des mesures correctives soient prises

Note 1 à l'article: Le terme «commande» est également utilisé pour décrire ce concept dans certains contextes. Le terme «contre-mesure» a été choisi pour la présente norme afin d'éviter la confusion avec le terme «commande» dans le contexte d'une «commande de processus».

3.1.18
mode dégradé
mode de fonctionnement en présence de défaillances anticipées lors de la conception du système de commande

Note 1 à l'article: Les modes dégradés permettent au système de commande de continuer à fournir des fonctions essentielles malgré la déficience d'un ou de plusieurs éléments du système, par exemple dysfonctionnement ou panne de l'appareil de commande, interruption des communications par suite de panne ou isolement intentionnel du système en réponse à un compromis identifié ou suspecté des sous-systèmes.

3.1.19
zone démilitarisée
réseau commun et limité de serveurs joignant deux ou plusieurs zones dans le but de contrôler le flux de donnée entre les zones

Note 1 à l'article: Les zones démilitarisées (DMZ - *demilitarized zone*) sont généralement utilisées afin d'éviter des connexions directes entre des zones différentes.

3.1.20
appareil
actif incorporant un ou plusieurs processeurs ayant la capacité d'envoyer ou de recevoir des données/commandes de ou vers un autre actif

Note 1 à l'article: Des exemples comprennent des contrôleurs, des interfaces homme-machine, des automates programmables, des terminaux à distance, des émetteurs, des actionneurs, des valves, des interrupteurs réseau, etc.

3.1.21
environnement
objets, région ou circonstances environnants pouvant influencer le comportement de l'IACS et/ou pouvant être influencés par l'IACS

3.1.22
fonction essentielle
fonction ou capacité exigée pour maintenir la santé, la sécurité, l'environnement et la disponibilité du matériel sous commande

Note 1 à l'article: Les fonctions essentielles comprennent, entre autres, la fonction instrumentée de sécurité (SIF - *safety instrumented function*), la fonction de commande et la capacité de l'opérateur à voir et manipuler l'appareil

sous commande. La perte de fonctions essentielles est communément appelée «perte de protection», «perte de commande» et «perte de vue» respectivement. Dans certaines industries, des fonctions supplémentaires comme l'historique peuvent être considérées comme essentielles.

3.1.23
événement
occurrence ou modification d'un ensemble particulier de circonstances

Note 1 à l'article: Dans un IACS, il peut s'agir d'une action prise par un individu (autorisé ou non), d'une modification détectée dans le système de commande (normale ou non), ou d'une réponse automatique du système de commande lui-même (normale ou non).

3.1.24
firecall
méthode établie afin de fournir un accès d'urgence à un système de commande sécurisé

Note 1 à l'article: En situation d'urgence, des utilisateurs non autorisés peuvent obtenir l'accès aux systèmes clés afin de corriger le problème. Lorsqu'un firecall est utilisé, un processus de révision intervient généralement pour garantir que l'accès a été correctement utilisé pour corriger un problème. Ces méthodes fournissent généralement un identifiant (ID) utilisateur à usage unique, ou un mot de passe à usage unique.

3.1.25
identificateur
symbole, unique dans son domaine de sécurité, qui identifie, indique ou nomme une entité qui affirme ou revendique une identité

3.1.26
identification
affirmation d'une identité

3.1.27
impact
conséquence évaluée d'un événement particulier

3.1.28
incident
événement ne faisant pas partie du fonctionnement attendu d'un système ou d'un service, qui cause ou peut causer une interruption ou une réduction de la qualité du service fourni par le système de commande

3.1.29
système d'automatisation et de commande industrielles
ensemble des personnes, matériels, logiciels et politiques impliqués dans le processus industriel et qui peuvent affecter ou influencer la sûreté, la sécurité et la fiabilité de son fonctionnement

3.1.30
intégrité
propriété de protection de l'exactitude et de l'exhaustivité des actifs

3.1.31
moindre privilège
principe de base soutenant qu'il convient que soient attribués aux utilisateurs (êtres humains, processus logiciels ou appareils) les privilèges les plus faibles conformément à leurs fonctions et obligations assignées

Note 1 à l'article: Le moindre privilège est communément mis en œuvre en un ensemble de rôles dans un IACS.

3.1.32
code mobile
programme transféré entre un système distant, possiblement «non approuvé», par le biais d'un réseau ou d'un support amovible pouvant être exécuté inchangé sur un système local sans installation ou exécution explicite par le destinataire

Note 1 à l'article: Des exemples de codes mobiles incluent JavaScript, VBScript, les applets Java, les contrôles ActiveX, les animations Flash, les films Shockwave, et les macros Microsoft Office.

3.1.33
non-répudiation
capacité à prouver l'occurrence d'un événement ou d'une action donné(e) et les entités qui en sont à l'origine

Note 1 à l'article: L'objectif d'une non-répudiation est de résoudre les litiges relatifs à l'occurrence ou la non-occurrence de l'événement ou de l'action et à l'implication des entités dans l'événement.

3.1.34
fournisseur de produit
fabricant de produit matériel et/ou logiciel

Note 1 à l'article: Ce terme est utilisé à la place du terme générique «fournisseur» pour marquer la distinction.

3.1.35
accès distant
accès à un système de commande par n'importe quel utilisateur (être humain, processus logiciel ou appareil) communicant de l'extérieur du périmètre de la zone couverte

3.1.36
rôle
ensemble de comportements, privilèges et obligations connectés, associés à tous les utilisateurs (êtres humains, processus logiciel ou appareils) d'un IACS

Note 1 à l'article: Les privilèges à réaliser certaines fonctions sont assignés à des rôles spécifiques.

3.1.37
système équipé pour la sécurité
système utilisé pour la mise en œuvre d'une ou de plusieurs fonctions liées à la sécurité

3.1.38
niveau de sécurité
mesure de confiance qui garantit que l'IACS ne présente pas de vulnérabilités et de fonctions comme prévu

Note 1 à l'article: Les vulnérabilités peuvent être conçues dans l'IACS, insérées à tout moment du cycle de vie, ou être causées par des menaces en évolution. Les vulnérabilités conçues dans l'IACS peuvent être découvertes longtemps après son déploiement initial, par exemple lorsqu'une technique de chiffrement a été interrompue ou par une politique inappropriée de gestion des comptes, comme la non-suppression d'anciens comptes utilisateurs. Les vulnérabilités insérées peuvent être le résultat d'un correctif ou d'une modification de politique qui ouvrent à de nouvelles vulnérabilités.

3.1.39
fournisseur de service
organisation (organisation interne ou externe, fabricant, etc.) qui a accepté de prendre la responsabilité de fournir un service de support donné et d'obtenir, lorsque spécifié, des fournitures conformément à l'accord

Note 1 à l'article: Ce terme est utilisé à la place du terme générique «fournisseur» pour marquer la distinction.

3.1.40
session
échange d'informations semi-permanent, dynamique et interactif entre deux ou plusieurs appareils de communication

Note 1 à l'article: Une session a généralement des processus de début et de fin clairement définis.

3.1.41
ID de session
identificateur utilisé pour indiquer une entrée de session spécifique

3.1.42
point de consigne
valeur cible identifiée dans un système de commande qui commande une ou plusieurs actions au sein du système de commande

3.1.43
intégrateur de système
personne ou entreprise qui se spécialise dans le rassemblement des sous-systèmes de composants en un ensemble et garantit que ces sous-systèmes fonctionnent conformément aux spécifications du projet

3.1.44
menace
circonstance ou événement de nature à compromettre les opérations (y compris la mission, les fonctions, l'image ou la réputation), les atouts, les systèmes de commande ou les individus au moyen d'un accès non autorisé, d'une destruction, d'une divulgation, d'une modification de données et/ou d'un déni de service

3.1.45
confiance
assurance qu'il est possible de compter sur une opération, une source de transaction de données, un réseau ou un processus logiciel pour agir comme prévu

Note 1 à l'article: Généralement, il est possible de dire qu'une entité «a confiance» en une seconde entité lorsque la première présume que la seconde agira comme le prévoit la première.

Note 2 à l'article: Cette confiance ne peut s'appliquer que pour certaines fonctions spécifiques.

3.1.46
non sécurisé
ne satisfait pas aux exigences de confiance prédéfinies

Note 1 à l'article: Une entité peut simplement être déclarée comme non sécurisée.

3.1.47
zone
regroupement d'actifs physiques ou logiques qui partagent des exigences de sécurité communes

Note 1 à l'article: Une zone a un contour bien délimité. La politique de sécurité d'une zone est généralement appliquée par une combinaison de mécanismes se situant au bord et à l'intérieur de la zone.

3.2 Termes abrégés et acronymes

AES	Advanced encryption standard (Norme de chiffrement avancé)
API	Application programming interface (Interface de programmation d'application)
ASLR	Address space layout randomization (Randomisation de l'agencement de l'espace adressable)
BPCS	Basic process control system (Système de commande de processus de base)
CA	Certification authority (Autorité de certification)
CIP	Critical infrastructure protection (Protection des infrastructures essentielles)
COTS	Commercial off the shelf (Disponible dans le commerce)
LCR	Liste des certificats révoqués

DC	Data confidentiality (Confidentialité des données)
DEP	Data execution prevention (Prévention de l'exécution des données)
DHCP	Dynamic host configuration protocol (Protocole de configuration dynamique des hôtes)
DMZ	Demilitarized zone (Zone démilitarisée)
DNS	Domain name service (Système de noms de domaine)
DoS	Denial of service (Refus de service)
EICAR	European Institute for Computer Antivirus Research (Institut européen pour la recherche des virus informatiques)
EMI	Electromagnetic interference (Perturbation électromagnétique)
ERU	Essai de réception en usine
FIPS	[US NIST] Federal Information Processing Standard
FR	Foundational requirement (Exigence fondamentale)
FS-PLC	Functional safety PLC (Automate programmable de sécurité fonctionnelle)
FTP	File transfer protocol (Protocole de transfert de fichier)
GLONASS	Global Navigation Satellite System (Système mondial de satellites de navigation)
GPS	Global Positioning System (Système mondial de localisation)
IHM	Interface homme-machine
HSE	Health, safety and environmental (Santé, sécurité et environnement)
HTTP	Hypertext transfer protocol (Protocole de transfert hypertexte)
HTTPS	HTTP sécurisé
IAC	Identification and authentication control (Commande d'identification et d'authentification)
IACS	Industrial automation and control system(s) (Système(s) d'automatisation et de commande industrielle)
IAMS	Instrument asset management system (Système de gestion d'actif d'instrument)
ID	Identificateur
IDS	Intrusion detection system (Système de détection d'intrusion)
IEC	International Electrotechnical Commission (Commission Electrotechnique Internationale)
IEEE	Institute of Electrical and Electronics Engineers (Institut des ingénieurs électriciens et électroniciens)
IETF	Internet Engineering Task Force (Groupe de travail IETF)
MI	Messagerie instantanée
IP	Internet Protocol (Protocole Internet)
IPS	Intrusion prevention system (Système de prévention d'intrusion)
ISA	International Society of Automation (Société internationale d'automatisation)
ISO	International Organization for Standardization (Organisation internationale de normalisation)
IT	Information technology (Traitement de l'information)
MES	Manufacturing execution system (Système d'exécution de fabrication)
NERC	North American Electric Reliability Council (Conseil nord-américain pour la fiabilité électrique) (concerne les États-Unis et le Canada)
NIST	National Institute of Standards and Technology (Institut national américain de technologie et des normes)
NX	No Execute (Pas d'exécution)

OCSP	Online certificate status protocol (Protocole sur l'état des certificats en ligne)
OWASP	Open Web Application Security Project (Projet de sécurité d'application Web ouvert)
PDF	Portable document format (Format de document portable)
ICP	Infrastructure à clé publique
PLC	Programmable logic controller (Automate programmable)
RA	Ressource availability (Disponibilité des ressources)
RAM	Random access memory (Mémoire à accès aléatoire)
RDF	Restricted data flow (Flux de données réduit)
RE	Requirement enhancement (Amélioration d'exigence)
RFC	[IETF] Request For Comment (Demande de commentaires)
RJ	Registered jack (Prise enregistrée)
RTU	Remote terminal unit (Terminal à distance)
ERS	Essai de réception sur site
SHA	Secure hash algorithm (Algorithme de hachage sécurisé)
SI	System integrity (Intégrité du système)
SIEM	Security Information and Event Management (Gestion des informations et événements de sécurité)
SIF	Safety instrumented function (Fonction équipée pour la sécurité)
SIL	Safety integrity level (Niveau d'intégrité de sécurité)
SIS	Safety instrumented system (Système équipé pour la sécurité)
SL	Security level (Niveau de sécurité)
SL-A	Achieved security level (Niveau de sécurité atteint)
SL-C	Capability security level (Niveau de sécurité de capacité)
SL-T	Target security level (Niveau de sécurité cible)
SP	[US NIST] Special Publication (Publication spéciale)
SR	System requirement (Exigence système)
SSH	Secure socket shell (Session à distance sécurisée)
SuC	System under consideration (Système à l'étude)
TCP	Transmission control protocol (Protocole de contrôle d'émission)
TPM	Trusted platform module
TRE	Timely response to events (Réponse rapide aux événements)
UC	Use control (Commande d'utilisation)
USB	Universal serial bus (Bus série universel)
VoIP	Voice over Internet protocol (Voix par le protocole de l'internet)
WEP	Wired equivalent privacy (Confidentialité équivalente aux transmissions par fil)
WLAN	Wireless local area network (Réseau local sans fil)

3.3 Conventions

La présente norme étend les sept exigences fondamentales définies dans l'IEC 62443-1-1 en une série d'exigences système. Chaque exigence système possède une exigence de base et zéro ou plusieurs améliorations d'exigences (RE) permettant de renforcer la sécurité. Pour la clarté du lecteur, des justifications et des recommandations supplémentaires sont données à chaque exigence de base ainsi que des notes pour toute RE associée, comme jugé nécessaire. Les exigences de base et les RE, si présentes, sont ensuite mappées au niveau de sécurité de capacité du système de commande, SL-C(FR, système de commande) 1 à 4.

Les sept exigences fondamentales comportent toutes un ensemble défini de quatre niveaux de sécurité. Le niveau de capacité 0 d'un système de commande d'une FR particulière est défini implicitement comme sans exigence. Par exemple, la formulation de l'objectif de l'Article 8, FR 4 – Confidentialité des données, est:

> Garantir la confidentialité des informations sur les canaux de communication et dans les dépôts de données afin d'empêcher une divulgation non autorisée.

Les quatre niveaux de sécurité associés sont définis comme suit:

- SL 1 – Empêcher la divulgation non autorisée des informations par écoute illicite ou exposition occasionnelle.
- SL 2 – Empêcher la divulgation non autorisée des informations à une entité cherchant activement par des moyens simples, avec peu de ressources, des compétences génériques et une faible motivation.
- SL 3 – Empêcher la divulgation non autorisée des informations à une entité cherchant activement par des moyens complexes, avec des ressources modérées, des compétences spécifiques à l'IACS et une motivation modérée.
- SL 4 – Empêcher la divulgation non autorisée des informations à une entité cherchant activement par des moyens complexes, avec des ressources étendues, des compétences spécifiques à l'IACS et une motivation élevée.

Les évaluations individuelles des SR et RE sont donc basées sur une augmentation graduelle de la sécurité globale du système de commande pour cette FR particulière.

Le SL-C (système de commande) utilisé tout au long de la présente norme signifie une capacité exigée pour satisfaire à un classement du SL donné pour une FR donnée. Une description complète du concept de vecteur SL est donnée à l'Annexe A.

4 Contraintes communes de sécurité du système de commande

4.1 Présentation

Lors de la lecture, de la spécification et de la mise en œuvre des SR du système de commande détaillées aux Articles 5 à 11 de la présente norme, un certain nombre de contraintes communes doivent être respectées. L'introduction de la présente norme apporte une analyse contextuelle et informative de son objectif. Le présent article ainsi que les articles suivants spécifiques aux FR fournissent le matériel normatif nécessaire à la construction des extensions de la sécurité existante des entreprises, afin de prendre en charge l'intégrité rigoureuse et les exigences de disponibilité nécessaires à l'IACS.

NOTE Le contenu de cet article est incorporé à l'IEC 62443-1-1.

4.2 Prise en charge des fonctions essentielles

Comme cela est documenté en 3.1.22, une fonction essentielle est une «fonction ou capacité exigée pour maintenir la santé, la sécurité, l'environnement et la disponibilité du matériel sous commande».

- Des mesures de sécurité ne doivent pas compromettre les fonctions essentielles d'un IACS à haute disponibilité, à moins qu'elles ne soient prises en charge par une appréciation du risque.

  NOTE Voir l'IEC 62443-2-1 relative aux exigences de documentation associées à l'appréciation du risque exigées pour prendre en charge les cas pour lesquels des mesures de sécurité peuvent affecter les fonctions essentielles.

Lors de la lecture, de la spécification et de la mise en œuvre des SR décrites dans la présente norme, il convient que la mise en œuvre des mesures de sécurité ne cause pas de perte de protection, de perte de commande, de perte de vue ou de perte d'autres fonctions

essentielles. Après une analyse du risque, certaines installations peuvent déterminer que certains types de mesures de sécurité peuvent interrompre des opérations permanentes, mais les mesures de sécurité ne doivent pas causer de perte de protection pouvant induire des conséquences de santé, sécurité et environnement (HSE). Certaines contraintes spécifiques incluent:

- Les contrôles d'accès (IAC et UC) ne doivent pas empêcher le fonctionnement des fonctions essentielles, en particulier:
  - Les comptes utilisés pour des fonctions essentielles ne doivent pas être verrouillés, même temporairement (voir 5.5, SR 1.3 – Gestion des comptes, 5.6, SR 1.4 – Gestion des identificateurs, 5.13, SR 1.11 – Tentatives d'authentification infructueuses et 6.7, SR 2.5 – Verrouillage de session).
  - La vérification et l'enregistrement des actions de l'opérateur afin de faire appliquer la non-répudiation ne doivent pas ajouter de délai significatif au temps de réponse du système (voir 6.14, SR 2.12 – Non-répudiation).
  - Pour les systèmes de commande à haute disponibilité, la défaillance de l'autorité de certification ne doit pas interrompre les fonctions essentielles (voir 5.10, SR 1.8 – Certificats d'infrastructure à clés publiques (ICP)).
  - L'identification et l'authentification ne doivent pas empêcher le démarrage de la SIF (voir 5.3, SR 1.1 – Identification et authentification d'utilisateur humain et 5.4, SR 1.2 – Identification et authentification du processus logiciel et de l'appareil). De même pour l'application de l'autorisation (voir 6.3, SR 2.1 – Application de l'autorisation).
  - Des enregistrements d'audit horodatés incorrects (voir 6.10, SR 2.8 – Événements auditables et 6.13, SR 2.11– Horodatages) ne doivent pas compromettre les fonctions essentielles.
- Les fonctions essentielles d'un IACS doivent être maintenues si la protection des limites de la zone passe en mode défaillance-fermeture et/ou en mode îlot (voir 9.4, SR 5.2 – Protection des limites de zone).
- Un événement de refus de service (DoS) sur le réseau du système de commande ou du système équipé pour la sécurité (SIS) ne doit pas empêcher le fonctionnement de la SIF (voir 11.3, SR 7.1 – Protection contre le refus de service).

4.3 Contre-mesures compensatoires

Les contre-mesures compensatoires, comme utilisées dans la présente norme, doivent respecter les lignes directrices décrites dans l'IEC 62443-3-2.

Tout au long de la présente norme, le langage normatif SR établit que «le système de commande doit permettre de...» prendre en charge certaines exigences de sécurité spécifiques. Le système de commande doit permettre de prendre en charge ces exigences, mais il se peut qu'elles soient prises en charge par un composant externe. Dans ce cas, le système de commande doit fournir une «interface» à ce composant externe. L'identification de l'utilisateur (y compris centralisée v. distribuée), l'application de la sécurité du mot de passe, la vérification de la validité de la signature, la corrélation des événements de sécurité et le démantèlement de l'appareil (persistance des informations) sont des exemples de contre-mesures compensatoires.

NOTE 1 Les exigences de sécurité du système de commande détaillées dans la présente norme se rapportent à toutes les fonctions techniques pertinentes à un système de commande, y compris les outils et applications. Toutefois, comme noté ici, certaines de ces fonctions peuvent être gérées par une ressource externe.

NOTE 2 Dans certaines applications à haute disponibilité de ressource (haut SL-T (RA, système de commande)), des contre-mesures compensatoires externes au système de commande (comme des mesures de sécurité physique supplémentaires et/ou des vérifications améliorées des antécédents du personnel) sont nécessaires. Dans ces cas, il est possible de voir un système de commande à SL à haute disponibilité de ressource avoir un SL IACS 1 ou 2 plus faible, selon les contre-mesures compensatoires. Le verrouillage ou la perte de contrôle causé(e) par les mesures de sécurité est augmenté(e), et non diminué(e) pour les systèmes de commande à SL à très haute disponibilité. Ainsi, des SL plus élevés ne sont pas toujours «mieux», même lorsque le coût ne constitue pas un facteur significatif.

4.4 Moindre privilège

La capacité à appliquer le concept du moindre privilège doit être fournie, avec la granularité des autorisations et la flexibilité de mapper ces autorisations aux rôles suffisants à les prendre en charge. Il convient que la responsabilité individuelle soit disponible lorsque cela est exigé.

5 FR 1– Commande d'identification et d'authentification

5.1 Objectif et descriptions du SL-C(IAC)

Identifier et authentifier tous les utilisateurs (êtres humains, processus logiciels et appareils) avant de leur autoriser l'accès au système de commande.

- SL 1 – Identifier et authentifier tous les utilisateurs (humains, processus logiciels et appareils) par des mécanismes qui protègent contre les accès occasionnels ou fortuits par des entités non authentifiées.
- SL 2 – Identifier et authentifier tous les utilisateurs (êtres humains, processus logiciels et appareils) par des mécanismes qui protègent contre les accès intentionnellement non authentifiés par des entités utilisant des moyens simples avec peu de ressources, des compétences génériques et une motivation faible.
- SL 3 – Identifier et authentifier tous les utilisateurs (êtres humains, processus logiciels et appareils) par des mécanismes qui protègent contre les accès intentionnellement non authentifiés par des entités utilisant des moyens complexes avec des ressources modérées, des compétences spécifiques à l'IACS et une motivation modérée.
- SL 4 – Identifier et authentifier tous les utilisateurs (êtres humains, processus logiciels et appareils) par des mécanismes qui protègent contre les accès intentionnellement non authentifiés par des entités utilisant des moyens complexes avec des ressources étendues, des compétences spécifiques à l'IACS et une motivation élevée.

5.2 Justification

Les propriétaires d'actif doivent établir une liste de tous les utilisateurs (êtres humains, processus logiciels et appareils) afin de déterminer le niveau de protection IAC exigé pour chaque composant du système de commande. Le but de l'IAC est d'assurer la protection du système de commande en vérifiant l'identité de tout utilisateur demandant l'accès au système de commande avant d'activer la communication. Il convient que les recommandations et lignes directrices incluent des mécanismes qui fonctionnent en modes mixtes. Par exemple, certains composants de système de commande exigent une IAC forte, comme des mécanismes d'authentification forts, et d'autres non.

5.3 SR 1-1 – Identification et authentification d'utilisateur humain

5.3.1 Exigence

Le système de commande doit permettre d'identifier et d'authentifier tous les utilisateurs humains. Cette capacité doit faire appliquer l'identification et l'authentification sur toutes les interfaces qui fournissent à l'utilisateur humain un accès au système de commande, afin de prendre en charge la séparation des obligations et le moindre privilège conformément aux politiques de sécurité et aux procédures applicables.

5.3.2 Justification et recommandations supplémentaires

Tous les utilisateurs humains doivent être identifiés et authentifiés pour tous les accès au système de commande. Il convient que l'authentification de l'identité de ces utilisateurs soit réalisée par l'utilisation de méthodes comme des mots de passe, des jetons, la biométrie ou, en cas d'authentification multifactorielle, une combinaison de ces derniers. La localisation géographique des utilisateurs humains peut également être utilisée dans le processus d'authentification. Il convient d'appliquer cette exigence aux accès local et distant du système

de commande. En plus de l'identification et de l'authentification de tous les utilisateurs humains au niveau du système de commande (par exemple, au moment de la connexion au système), des mécanismes d'identification et d'authentification sont souvent employés au niveau de l'application.

Lorsque les utilisateurs humains représentent un groupe unique (comme des opérateurs d'une salle de commande), l'identification et l'authentification de l'utilisateur peuvent être basées sur le rôle ou sur le groupe. Pour certains systèmes de commande, la capacité d'interaction immédiate avec l'opérateur est critique. Il est essentiel que les actions d'urgence locales ainsi que les fonctions essentielles du système de commande ne soient pas gênées par les exigences d'identification et d'authentification (voir l'Article 4 pour une analyse plus complète). L'accès à ces systèmes peut être restreint par des mécanismes de sécurité physique appropriés (voir l'IEC 62443-2-1). Une salle des opérations critiques pour laquelle un contrôle d'accès physique et une surveillance stricts sont en place et pour laquelle une modification des plans attribue la responsabilité à un groupe d'utilisateurs est un exemple de ce type de situation. Ces utilisateurs peuvent alors utiliser la même identité utilisateur. De plus, il convient d'authentifier les clients désignés de la station de travail de l'opérateur (voir 5.4, SR 1.2 – Identification et authentification du processus logiciel et de l'appareil) ou il convient de limiter l'utilisation de ce compte partagé à l'environnement restreint de la salle de commande.

Afin de prendre en charge les politiques d'IACS, comme défini dans l'IEC 62443-2-1, le système de commande vérifie l'identité de tous les utilisateurs dans une première étape. Dans une seconde étape, les autorisations assignées à l'utilisateur humain identifié sont appliquées (voir 6.3, SR 2.1 – Application de l'autorisation).

5.3.3 Améliorations d'exigences

5.3.3.1 SR 1.1 RE 1 – Identification et authentification unique

Le système de commande doit permettre d'identifier et d'authentifier de façon unique tous les utilisateurs humains.

5.3.3.2 SR 1.1 RE 2 – Authentification multifactorielle pour les réseaux non sécurisés

Le système de commande doit permettre d'employer une authentification multifactorielle pour l'accès des utilisateurs humains au système de commande par un réseau non sécurisé (voir 5.15, SR 1.13 – Accès par des réseaux non sécurisés).

NOTE Voir 5.7.3.5.7.3.1,SR 1.5 – Gestion des authentifiants, RE 5.7.3.1 pour la gestion améliorée de l'authentifiant pour les processus logiciels.

5.3.3.3 SR 1.1 RE 3 – Authentification multifactorielle pour tous les réseaux

Le système de commande doit permettre d'employer une authentification multifactorielle pour l'accès de tout utilisateur humain au système de commande.

5.3.4 Niveaux de sécurité

Les exigences des quatre niveaux de sécurité relatifs à la SR 1.1 – Identification et authentification d'utilisateur humain sont:

- SL-C(IAC, système de commande) 1: SR 1.1
- SL-C(IAC, système de commande) 2: SR 1.1 (1)
- SL-C(IAC, système de commande) 3: SR 1.1 (1) (2)
- SL-C(IAC, système de commande) 4: SR 1.1 (1) (2) (3)

5.4 SR 1.2 – Identification et authentification du processus logiciel et de l'appareil

5.4.1 Exigence

Le système de commande doit permettre d'identifier et d'authentifier tous les processus logiciels et appareils. Cette capacité doit faire appliquer l'identification et l'authentification sur toutes les interfaces qui fournissent un accès au système de commande, afin de prendre en charge le moindre privilège conformément aux politiques de sécurité et aux procédures applicables.

5.4.2 Justification et recommandations supplémentaires

La fonction d'identification et d'authentification est de mapper un ID à un processus logiciel ou à un appareil inconnu (dorénavant appelé entité dans le présent paragraphe) afin de le faire connaître avant d'autoriser l'échange de données. Autoriser des entités suspectes à envoyer et recevoir des données spécifiques au système de commande peut causer un comportement nuisible du système de commande légitime.

Toutes les entités doivent être identifiées et authentifiées pour tous les accès au système de commande. Il convient que l'authentification de l'identité de ces entités soit réalisée par l'utilisation de méthodes comme des mots de passe, des jetons ou des localisations (physiques ou logiques). Il convient d'appliquer cette exigence à l'accès local et à l'accès distant du système de commande. Cependant, dans certains scénarios dans lesquels des entités individuelles sont utilisées pour se connecter à des systèmes cibles différents (par exemple, support distant), il peut être techniquement irréalisable qu'une entité ait des identités multiples. Dans ces cas, des contre-mesures compensatoires devraient alors s'appliquer.

Des mécanismes d'identification et d'authentification pour toutes les entités sont nécessaires à la protection contre les attaques, comme l'attaque homme au milieu ou l'usurpation de message. Dans certains cas, ces mécanismes peuvent impliquer de multiples processus logiciels sur le même serveur physique, chacun ayant sa propre identité. Dans d'autres cas, l'identité peut être liée à l'appareil physique, comme tous les processus fonctionnant sur un PLC donné.

Une attention particulière doit être portée lors de l'identification et de l'authentification des appareils portables et mobiles. Ces appareils constituent une méthode connue d'introduction de trafic du réseau non désiré, de logiciel malveillant et/ou d'exposition des informations aux systèmes de commande, y compris les réseaux isolés par ailleurs.

Lorsque les entités fonctionnent comme un groupe unique, l'identification et l'authentification peuvent se baser sur le rôle, sur le groupe ou sur l'entité, et il est essentiel que les actions d'urgence locales ainsi que les fonctions essentielles du système de commande ne soient pas gênées par les exigences d'identification et d'authentification (voir l'Article 4 pour une analyse plus complète). Par exemple, dans des systèmes de commande et de protection communs, un groupe d'appareils exécute les fonctions de protection et communique avec des messages multidiffusions entre les appareils du groupe. Dans ces cas, l'authentification du groupe basée sur des comptes partagés ou sur des clés symétriques partagées est généralement utilisée.

Afin de prendre en charge les politiques de commande d'identification et d'authentification, comme défini dans l'IEC 62443-2-1, le système de commande vérifie l'identité de toutes les entités dans une première étape. Dans une seconde étape, les autorisations assignées à l'entité identifiée sont appliquées (voir 6.3, SR 2.1 – Application de l'autorisation).

5.4.3 Améliorations d'exigences

5.4.3.1 SR 1.2 RE 1 – Identification et authentification unique

Le système de commande doit permettre d'identifier et d'authentifier de façon unique tous les processus logiciels et appareils.

5.4.3.2 Vide

5.4.4 Niveaux de sécurité

Les exigences des quatre niveaux de sécurité relatifs à la SR 1.2 – Identification et authentification du processus logiciel et de l'appareil sont:

- SL-C(IAC, système de commande) 1: Non sélectionné
- SL-C(IAC, système de commande) 2: SR 1.2
- SL-C(IAC, système de commande) 3: SR 1.2 (1)
- SL-C(IAC, système de commande) 4: SR 1.2 (1)

5.5 SR 1.3 – Gestion des comptes

5.5.1 Exigence

Le système de commande doit permettre de prendre en charge la gestion de tous les comptes par les utilisateurs autorisés, y compris l'ajout, l'activation, la modification, la désactivation et la suppression des comptes.

5.5.2 Justification et recommandations supplémentaires

La gestion des comptes peut inclure le groupement des comptes (par exemple, individuel, basé sur le rôle, basé sur l'appareil et système de commande), l'établissement de conditions pour l'adhésion au groupe et l'évaluation des autorisations associées. Dans certains cas d'IACS, lorsque des comptes individuels sont définis comme étant inutiles du point de vue analyse du risque et/ou réglementaire, des comptes partagés sont acceptables tant que des contre-mesures compensatoires appropriées, comme un accès physique limité ou des mesures organisationnelles pour autorisation, sont mises en place et documentées.

Des comptes utilisateur non humains (parfois appelés comptes service) utilisés pour des communications processus à processus logiciel (par exemple, serveur de commande vers l'historique et PLC vers le serveur de commande) exigent généralement des politiques et procédures de sécurité différentes de celles des comptes utilisateur humains. Pour la sécurité améliorée, il convient que la gestion des comptes soit tenue selon des politiques unifiées et déployées localement dans les composants appropriés du système de commande. Il convient que les comptes par défaut du système non utilisés pour la première installation du système puissent être supprimables. L'amélioration de la sécurité repose dans la simplification et dans l'application cohérente de gestion des comptes.

5.5.3 Améliorations d'exigences

5.5.3.1 SR 1.3 RE 1 – Gestion des comptes unifiée

Le système de commande doit permettre de prendre en charge la gestion des comptes unifiés.

5.5.3.2 Vide

5.5.4 Niveaux de sécurité

Les exigences des quatre niveaux de sécurité relatifs à la SR 1.3 – Gestion des comptes sont:

- SL-C(IAC, système de commande) 1: SR 1.3
- SL-C(IAC, système de commande) 2: SR 1.3
- SL-C(IAC, système de commande) 3: SR 1.3 (1)
- SL-C(IAC, système de commande) 4: SR 1.3 (1)

5.6 SR 1.4 – Gestion des identificateurs

5.6.1 Exigence

Le système de commande doit permettre de prendre en charge la gestion des identificateurs par utilisateur, groupe, rôle ou interface du système de commande.

5.6.2 Justification et recommandations supplémentaires

Les identificateurs se distinguent des privilèges qu'ils permettent à une entité d'effectuer dans un domaine ou une zone spécifique de système de commande (voir 6.3, SR 2.1 – Application de l'autorisation). Lorsque les utilisateurs humains représentent un groupe unique (comme des opérateurs d'une salle de commande), l'identification de l'utilisateur peut se baser sur le rôle, sur le groupe ou sur l'appareil. Pour certains systèmes de commande, la capacité d'interaction immédiate avec l'opérateur est critique. Il convient que les actions d'urgence locales pour le système de commande ne soient pas gênées par des exigences d'identification. L'accès à ces systèmes peut être restreint par des contre-mesures compensatoires appropriées. Des identificateurs peuvent être exigés sur des parties du système de commande, mais pas nécessairement sur son ensemble. Par exemple, les appareils sans fil exigent généralement des identificateurs, alors que les appareils câblés peuvent ne pas en exiger.

La gestion des identificateurs est déterminée par des politiques et procédures locales établies conformément à l'IEC 62443-2-1.

5.6.3 Améliorations d'exigences

Aucune.

5.6.4 Niveaux de sécurité

Les exigences des quatre niveaux de sécurité relatifs à la SR 1.4 – Gestion des identificateurs sont:

- SL-C(IAC, système de commande) 1: SR 1.4
- SL-C(IAC, système de commande) 2: SR 1.4
- SL-C(IAC, système de commande) 3: SR 1.4
- SL-C(IAC, système de commande) 4: SR 1.4

5.7 SR 1.5 – Gestion des authentifiants

5.7.1 Exigence

Le système de commande doit permettre de:

h) initialiser le contenu de l'authentifiant;

i) modifier tous les authentifiants par défaut au moment de l'installation du système de commande;

j) modifier/rafraîchir tous les authentifiants; et

k) assurer la protection de tous les authentifiants contre une divulgation non autorisée et une modification lorsqu'ils sont stockés et transmis.

5.7.2 Justification et recommandations supplémentaires

En plus d'un identificateur (voir 5.6, SR 1.4 – Gestion des identificateurs), un authentifiant est exigé pour prouver une identité. Les authentifiants des systèmes de commande incluent, entre autres, les jetons, les clés symétriques, les clés privées (partie d'une paire de clé publique/privée), la biométrie, les mots de passe, les clés physiques et les cartes d'accès. Il convient que les utilisateurs humains prennent des mesures raisonnables de sauvegarde des authentifiants, y compris garder en leur possession leurs authentifiants individuels, ne pas partager ou prêter leurs authentifiants, et signaler immédiatement la perte ou la compromission des authentifiants.

Les authentifiants ont un cycle de vie. Lorsqu'un compte est créé, un nouvel authentifiant doit automatiquement être créé afin que le propriétaire du compte puisse s'authentifier. Par exemple, dans un système basé sur les mots de passe, le compte est associé à un mot de passe. La définition du contenu de l'authentifiant initial peut être interprétée comme l'administrateur qui définit le mot de passe initial paramétré par le système de gestion des comptes pour tous les nouveaux comptes. La capacité à configurer ces valeurs initiales rend plus difficile pour les attaquants de deviner le mot de passe entre la création du compte et sa première utilisation (il convient qu'un nouveau mot de passe soit choisi par le propriétaire du compte lors de la première utilisation). Certains systèmes de commande sont installés par des installateurs automatisés qui créent tous les comptes nécessaires avec des mots de passe par défaut, et des appareils intégrés sont expédiés avec des mots de passe par défaut. Avec le temps, ces mots de passe deviennent connus et sont documentés sur l'Internet. Pouvoir changer les mots de passe par défaut protège le système contre les utilisateurs non autorisés essayant d'obtenir l'accès avec des mots de passe par défaut. Des mots de passe peuvent être obtenus depuis le stockage ou la transmission lors de l'authentification réseau. Cette complexité peut être augmentée par des protections cryptographiques comme le chiffrement ou le hachage, ou par des protocoles CHAP, qui n'exigent pas de transmission du mot de passe. Les mots de passe pourront toujours être soumis à des attaques, comme une force brutale cherchant à deviner ou à décrypter la protection cryptographique des mots de passe en transit ou stockés. Cette occasion peut être réduite en modifiant/rafraîchissant les mots de passe régulièrement. Des considérations similaires s'appliquent aux systèmes d'authentification basés sur des clés cryptographiques. Il est possible d'améliorer la protection en utilisant des mécanismes matériels comme des modules de sécurité matériels tels que des TPM.

Il convient de spécifier la gestion des authentifiants dans des politiques et procédures de sécurité applicables, par exemple des contraintes de modification des authentifiants par défaut, des périodes de rafraîchissement, la spécification de la protection des authentifiants ou des procédures de rappel (voir 3.1.24).

Le verrouillage ou la perte de contrôle par suite de mesures de sécurité n'est pas acceptable. S'il est exigé du système de commande qu'il ait un niveau de disponibilité élevé, il convient que des mesures soient prises afin de maintenir ce niveau (comme des contre-mesures physiques compensatoires, la duplication des clés ou le contournement de la supervision).

Au-delà des capacités de gestion des authentifiants spécifiées dans la présente exigence, la force du mécanisme d'authentification dépend de la force de l'authentifiant choisi (par exemple la complexité du mot de passe ou la longueur de la clé dans l'authentification par clé publique) et des politiques de validation de l'authentifiant lors du processus d'authentification (par exemple, la longueur de validité d'un mot de passe ou les vérifications effectuées par la validation de certificat de clé publique). Pour les mécanismes d'authentification basés sur mot de passe et les authentifications de clés publiques les plus courants, le 5.9, SR 1.7 – Force de l'authentification basée sur le mot de passe, le 5.10, SR 1.8 – Certificats d'infrastructure à clés publiques (ICP) et le 5.11, SR 1.9 – Force de l'authentification de clé publique fournissent des exigences supplémentaires.

5.7.3 Améliorations d'exigences

5.7.3.1 SR 1.5 RE 1 – Sécurité matérielle des identifiants du processus logiciel

Pour les processus logiciels et les utilisateurs d'appareils, le système de commande doit permettre d'assurer la protection des authentifiants pertinents à l'aide de mécanismes matériels.

5.7.3.2 Vide

5.7.4 Niveaux de sécurité

Les exigences des quatre niveaux de sécurité relatifs à la SR 1.5 – Gestion des authentifiants sont:

- SL-C(IAC, système de commande) 1: SR 1.5
- SL-C(IAC, système de commande) 2: SR 1.5
- SL-C(IAC, système de commande) 3: SR 1.5 (1)
- SL-C(IAC, système de commande) 4: SR 1.5 (1)

5.8 SR 1.6 – Gestion des accès sans fil

5.8.1 Exigence

Le système de commande doit permettre d'identifier et d'authentifier tous les utilisateurs (êtres humains, processus logiciels ou appareils) impliqués dans la communication sans fil.

5.8.2 Justification et recommandations supplémentaires

Toute technologie sans fil peut être considérée comme une simple option du protocole de communication, et il convient qu'elle le soit dans la plupart des cas. Ainsi, elle est soumise aux mêmes exigences de sécurité IACS que tout autre type de communication utilisé par l'IACS. Cependant, du point de vue de la sécurité, il existe au moins une différence significative entre les communications sans fil et câblées: les contre-mesures compensatoires de sécurité physique sont généralement moins efficaces avec des communications sans fil. Pour cette raison, et possiblement pour d'autres (par exemple pour des différences réglementaires), une analyse du risque peut légitimement résulter en un SL-T(IAC, système de commande) plus élevé pour des communications sans fil, par rapport à un protocole câblé utilisé dans le même cas.

Les technologies sans fil comprennent, entre autres, les micro-ondes, les satellites, les radiocommunications à commutation de paquets, l'IEEE 802.11x, l'IEEE 802.15.4 (ZigBee, IEC 62591 – *Wireless*HART®, ISA-100.11a), l'IEEE 802.15.1 (Bluetooth), les routeurs mobiles WLAN, les téléphones mobiles avec connexion et différentes technologies infrarouges.

5.8.3 Améliorations d'exigences

5.8.3.1 SR 1.6 RE 1 – Identification et authentification unique

Le système de commande doit permettre d'identifier et d'authentifier de façon unique tous les utilisateurs (êtres humains, processus logiciels ou appareils) impliqués dans la communication sans fil.

5.8.3.2 Vide

5.8.4 Niveaux de sécurité

Les exigences des quatre niveaux de sécurité relatifs à la SR 1.6 – Gestion des accès sans fil sont:

- SL-C(IAC, système de commande) 1: SR 1.6
- SL-C(IAC, système de commande) 2: SR 1.6 (1)
- SL-C(IAC, système de commande) 3: SR 1.6 (1)
- SL-C(IAC, système de commande) 4: SR 1.6 (1)

5.9 SR 1.7 – Force de l'authentification basée sur le mot de passe

5.9.1 Exigence

Pour les systèmes de commande utilisant une authentification basée sur le mot de passe, le système de commande doit permettre de faire appliquer le mot de passe configurable dont la force repose sur une longueur minimale et différents types de caractères.

5.9.2 Justification et recommandations supplémentaires

L'authentification basée sur un nom d'utilisateur et un mot de passe secret est un mécanisme très couramment utilisé. De nombreuses attaques de ces mécanismes se concentrent sur la supposition du mot de passe (par exemple, attaque par dictionnaire ou piratage psychologique ciblé), ou sur le déchiffrement de la protection cryptographique de la représentation du mot de passe stocké (par exemple, en utilisant des tables arc-en-ciel ou en forçant brutalement une collision de fonction de hachage).

Augmenter la taille définie des mots de passe valides en augmentant le nombre de caractères autorisés rend ces attaques plus complexes, mais seulement si la taille définie augmentée est réellement utilisée (généralement, les utilisateurs n'utilisent pas de caractères spéciaux dans leurs mots de passe afin de ne pas les oublier). Limiter la durée de vie d'un mot de passe diminue les occasions d'attaques. Afin d'éviter que les utilisateurs contournent ce contrôle en changeant leur mot de passe pour un nouveau, puis en le changeant immédiatement pour l'ancien, une durée de vie minimale d'un mot de passe est aussi couramment appliquée. Une notification de changement de mot de passe avant son expiration permet à l'utilisateur de changer son mot de passe au moment opportun, selon les conditions de fonctionnement du processus.

Cette protection peut être renforcée ultérieurement en limitant la réutilisation de mots de passe (ce qui empêche d'utiliser en alternance des ensembles de mots de passe), ce qui diminue l'utilité d'un mot de passe déjà enfreint. La protection étendue au-delà des mécanismes basés sur le mot de passe peut être atteinte en utilisant une authentification multifactorielle (voir 5.3 SR 1.1 – Identification et authentification d'utilisateur humain et 5.4, SR 1.2 – Identification et authentification du processus logiciel et de l'appareil).

5.9.3 Améliorations d'exigences

5.9.3.1 SR 1.7 RE 1 – Génération de mot de passe et restrictions de durée de vie pour les utilisateurs humains

Le système de commande doit permettre d'empêcher tout compte utilisateur humain donné de réutiliser un mot de passe pendant un nombre configurable de générations. De plus, le système de commande doit permettre de faire appliquer les restrictions de durée de vie minimale et maximale d'un mot de passe pour les utilisateurs humains. Ces capacités doivent satisfaire aux pratiques de sécurité communément admises dans l'industrie.

NOTE La capacité d'un système de commande à inciter l'utilisateur à changer son mot de passe durant une période configurable avant expiration constitue une bonne pratique communément admise.

5.9.3.2 SR 1.7 RE 2 – Restrictions de durée de vie d'un mot de passe pour tous les utilisateurs

Le système de commande doit permettre de faire appliquer les restrictions de durée de vie minimale et maximale d'un mot de passe pour tous les utilisateurs.

5.9.4 Niveaux de sécurité

Les exigences des quatre niveaux de sécurité relatifs à la SR 1.7 – Force de l'authentification basée sur le mot de passe sont:

- SL-C(IAC, système de commande) 1: SR 1.7
- SL-C(IAC, système de commande) 2: SR 1.7
- SL-C(IAC, système de commande) 3: SR 1.7 (1)
- SL-C(IAC, système de commande) 4: SR 1.7 (1) (2)

5.10 SR 1.8 – Certificats d'infrastructure à clés publiques (ICP)

5.10.1 Exigence

Lorsqu'une ICP est utilisée, le système de commande doit permettre de faire fonctionner l'ICP conformément aux meilleures pratiques communément admises ou d'obtenir des certificats de clé publique d'une ICP existante.

5.10.2 Justification et recommandations supplémentaires

L'enregistrement de la réception d'un certificat de clé publique nécessite l'inclusion d'une autorisation par un superviseur ou d'un officiel responsable et doit être réalisé au moyen d'un processus de sécurité qui vérifie l'identité du détenteur du certificat et garantit que le certificat est émis à la partie prévue. Il convient que toute latence induite par l'utilisation de certificats de clé publique ne dégrade pas la performance fonctionnelle du système de commande.

Il convient que la sélection d'une ICP appropriée tienne compte de la politique de sécurité de l'organisme. Il convient de fonder cette dernière sur le risque associé à la violation de la confidentialité des informations protégées. Des recommandations relatives à la définition de la politique sont données dans les lignes directrices et normes communément admises, comme l'IETF, la RFC 3647 [29] pour les ICP basées sur X.509. Par exemple, il convient que l'emplacement approprié d'une autorité de certification (CA), dans le système de commande ou sur l'Internet, et la liste des CA de confiance soient pris en compte dans la politique et dépendent de l'architecture du réseau (voir également l'IEC 62443-2-1).

5.10.3 Améliorations d'exigences

Aucune.

5.10.4 Niveaux de sécurité

Les exigences des quatre niveaux de sécurité relatifs à la SR 1.8 – Certificats d'infrastructure à clés publiques (ICP) sont:

- SL-C(IAC, système de commande) 1: Non sélectionné
- SL-C(IAC, système de commande) 2: SR 1.8
- SL-C(IAC, système de commande) 3: SR 1.8
- SL-C(IAC, système de commande) 4: SR 1.8

5.11 SR 1.9 – Force de l'authentification de clé publique

5.11.1 Exigence

Pour les systèmes de commande utilisant une authentification de clé publique, le système de commande doit permettre de:

a) valider les certificats en vérifiant la validité de la signature d'un certificat donné;

b) valider les certificats en construisant un chemin de certification vers une CA admise, ou dans le cas de certificats autosignés en déployant des certificats en feuille à tous les hôtes qui communiquent avec le sujet auquel le certificat est émis;

c) valider les certificats en vérifiant le statut de révocation du certificat donné;

d) établir le contrôle de l'utilisateur (être humain, processus logiciel ou appareil) de la clé privée correspondante; et

e) mapper l'identité authentifiée à un utilisateur (être humain, processus logiciel ou appareil).

5.11.2 Justification et recommandations supplémentaires

La cryptographie de la clé publique/privée dépend fortement de la confidentialité d'une clé privée d'un sujet donné et de la bonne gestion des relations de confiance. Lors de la vérification de confiance entre deux entités basée sur l'authentification de clé publique, il est essentiel de tracer le certificat de clé publique vers une entité sécurisée. Une erreur commune de mise en œuvre dans la validation du certificat est de vérifier uniquement la validité d'une signature de certificat sans vérifier la confiance du signataire. Dans les réglages ICP, un signataire est sécurisé s'il est une CA sécurisée ou s'il a un certificat émis par une CA sécurisée. Ainsi tous les vérificateurs doivent tracer les certificats qui leur sont présentés vers une CA sécurisée. Si cette chaîne de CA sécurisées ne peut être établie, il convient que le certificat présenté ne soit pas considéré comme sécurisé.

Si des certificats autosignés sont utilisés à la place d'une ICP, le sujet du certificat a signé lui-même son certificat, il n'y a donc jamais de tierce partie ou de CA sécurisée. Il convient que cela soit compensé par le déploiement de certificats de clés publiques autosignés à tous les pairs qui doivent les valider au moyen d'un autre mécanisme de sécurité (par exemple, configuration de tous les pairs dans un environnement sécurisé). Les certificats sécurisés doivent être distribués aux pairs au moyen de canaux sécurisés. Lors du processus de validation, il convient qu'un certificat autosigné ne soit sécurisé que s'il est déjà présent dans la liste des certificats sécurisés du pair qui valide. Il convient que l'ensemble des certificats sécurisés soit configuré au minimum nécessaire.

Dans les deux cas, la validation doit également tenir compte de la possibilité de révocation d'un certificat. Dans des réglages ICP, ceci est généralement réalisé en tenant à jour des listes des certificats révoqués (LCR) ou en exécutant un serveur OCSP. Lorsque la vérification des révocations n'est pas disponible du fait des contraintes du système de commande, des mécanismes, comme une durée de vie du certificat courte, peuvent compenser le manque d'informations de révocation dans les délais. Il est à noter que des certificats à durée de vie courte peuvent parfois causer des problèmes de fonctionnement significatifs dans un environnement de système de commande.

5.11.3 Améliorations d'exigences

5.11.3.1 SR 1.9 RE 1 – Sécurité matérielle de l'authentification de clé publique

Le système de commande doit permettre d'assurer la protection des clés privées pertinentes au moyen de mécanismes matériels conformément aux pratiques et recommandations de sécurité communément admises dans l'industrie.

5.11.3.2 Vide

5.11.4 Niveaux de sécurité

Les exigences des quatre niveaux de sécurité relatifs à la SR 1.9 – Force de l'authentification de clé publique sont:

- SL-C(IAC, système de commande) 1: Non sélectionné
- SL-C(IAC, système de commande) 2: SR 1.9
- SL-C(IAC, système de commande) 3: SR 1.9 (1)

- SL-C(IAC, système de commande) 4: SR 1.9 (1)

5.12 SR 1.10 – Rétroaction de l'authentifiant

5.12.1 Exigence

Le système de commande doit permettre d'occulter la rétroaction des informations d'authentification lors du processus d'authentification.

5.12.2 Justification et recommandations supplémentaires

Occulter la rétroaction permet d'assurer la protection des informations contre une possible exploitation par des individus non autorisés, par exemple afficher des astérisques ou d'autres caractères aléatoires lorsque l'utilisateur humain entre un mot de passe occulte la rétroaction d'informations d'authentification. D'autres exemples comprennent la saisie de clés WEP, la saisie de jetons SSH et des mots de passe uniques RSA. Il convient que l'entité authentifiante ne fournisse pas d'indice sur la raison de l'échec de l'authentification, comme «nom d'utilisateur inconnu».

5.12.3 Améliorations d'exigences

Aucune.

5.12.4 Niveaux de sécurité

Les exigences des quatre niveaux de sécurité relatifs à la SR 1.10 – Rétroaction de l'authentifiant sont:

- SL-C(IAC, système de commande) 1: SR 1.10
- SL-C(IAC, système de commande) 2: SR 1.10
- SL-C(IAC, système de commande) 3: SR 1.10
- SL-C(IAC, système de commande) 4: SR 1.10

5.13 SR 1.11 – Tentatives d'authentification infructueuses

5.13.1 Exigence

Le système de commande doit permettre d'imposer une limite au nombre configurable de tentatives d'accès invalide par tout utilisateur (être humain, processus logiciel ou appareil) durant une période configurable. Le système de commande doit permettre de refuser l'accès pendant une période spécifiée ou jusqu'à ce qu'il soit déverrouillé par un administrateur lorsque cette limite a été dépassée.

Pour les comptes système au nom desquels les services critiques ou les serveurs sont exécutés, le système de commande doit permettre d'interdire des connexions interactives.

5.13.2 Justification et recommandations supplémentaires

Du fait du refus de service potentiel, le nombre de tentatives d'accès invalide consécutives peut être limité. Si cela est activé, le système de commande peut automatiquement régler sur zéro le nombre de tentatives d'accès après une période prédéterminée établie par les politiques et procédures de sécurité applicables. Régler les tentatives d'accès sur zéro permet aux utilisateurs (être humain, processus logiciel, appareil) d'obtenir l'accès s'ils possèdent l'identifiant de connexion correct. Il convient de ne pas utiliser le refus d'accès automatique pour les stations de travail des opérateurs du système de commande ou les nœuds lorsque des réponses immédiates de l'opérateur sont exigées en situation d'urgence. Il convient que tous les mécanismes de verrouillage tiennent compte des exigences fonctionnelles pour les opérations continues afin d'atténuer le refus des conditions de fonctionnement de service qui peuvent résulter en une défaillance totale du système ou un

préjudice au personnel. Permettre les connexions interactives à un compte utilisé pour des services critiques peut fournir un potentiel refus de service ou d'autres abus.

5.13.3 Améliorations d'exigences

Aucune.

5.13.4 Niveaux de sécurité

Les exigences des quatre niveaux de sécurité relatifs à la SR 1.11 – Tentatives d'authentification infructueuses sont:

- SL-C(IAC, système de commande) 1: SR 1.11
- SL-C(IAC, système de commande) 2: SR 1.11
- SL-C(IAC, système de commande) 3: SR 1.11
- SL-C(IAC, système de commande) 4: SR 1.11

5.14 SR 1.12 – Notification d'utilisation du système

5.14.1 Exigence

Le système de commande doit permettre d'afficher un message de notification d'utilisation du système avant l'authentification. Le message de notification d'utilisation du système doit pouvoir être configuré par le personnel autorisé.

5.14.2 Justification et recommandations supplémentaires

Les politiques et procédures de sécurité et de confidentialité doivent être cohérentes avec les législations, directives, politiques, réglementations, normes et recommandations applicables. Les justifications principales pour cette exigence sont souvent les poursuites pénales des contrevenants, et la preuve de la violation intentionnelle. Cette capacité est donc nécessaire au soutien des exigences de politiques, et n'améliore pas la sécurité de l'IACS. Les messages de notification d'utilisation du système peuvent être mis en œuvre sous forme de bannières d'avertissement affichées lors de la connexion des individus au système de commande. Une bannière d'avertissement mise en œuvre comme une annonce physique dans le système de commande ne protège pas contre les problèmes de connexion à distance.

Des exemples d'éléments pour l'inclusion dans le message de notification d'utilisation du système sont:

a) que l'individu accède à un système de commande spécifique;

b) que l'utilisation du système peut être surveillée, enregistrée et soumise à un audit;

c) que l'utilisation non autorisée du système est interdite et soumise à des sanctions pénales et/ou civiles; et

d) que l'utilisation du système signifie le consentement à la surveillance et à l'enregistrement.

5.14.3 Améliorations d'exigences

Aucune.

5.14.4 Niveaux de sécurité

Les exigences des quatre niveaux de sécurité relatifs à la SR 1.12 – Notification d'utilisation du système sont:

- SL-C(IAC, système de commande) 1: SR 1.12
- SL-C(IAC, système de commande) 2: SR 1.12

- SL-C(IAC, système de commande) 3: SR 1.12
- SL-C(IAC, système de commande) 4: SR 1.12

5.15 SR 1.13 – Accès par des réseaux non sécurisés

5.15.1 Exigence

Le système de commande doit permettre de surveiller et de commander toutes les méthodes d'accès au système de commande par des réseaux non sécurisés.

5.15.2 Justification et recommandations supplémentaires

Des méthodes d'accès distant (comme l'accès par ligne commutée, à large bande et sans fil) ainsi que des connexions provenant du réseau du bureau d'une entreprise (système de non-commande) sont des exemples typiques d'accès au système de commande par des réseaux non sécurisés. Il convient que le système de commande restreigne l'accès obtenu par le biais de connexions par ligne commutée (par exemple, limiter l'accès par ligne commutée à partir de la source de la requête) ou qu'il assure la protection contre les connexions non autorisées ou la subversion de connexions autorisées (par exemple en utilisant des technologies de réseau privé virtuel). Il convient que l'accès par des réseaux non sécurisés à des emplacements de composants du système de commande géographiquement éloignés (par exemple centres de contrôle et sur le terrain) ne soit activé que lorsque cela est nécessaire et authentifié. Les politiques et procédures de sécurité peuvent exiger une authentification multifactorielle pour l'accès distant de l'utilisateur au système de commande.

5.15.3 Améliorations d'exigences

5.15.3.1 SR 1.13 RE 1 – Approbation explicite des demandes d'accès

Le système de commande doit permettre de refuser les demandes d'accès par des réseaux non sécurisés sauf si cela a été approuvé par un rôle assigné.

5.15.3.2 Vide

5.15.4 Niveaux de sécurité

Les exigences des quatre niveaux de sécurité relatifs à la SR 1.13 – Accès par des réseaux non sécurisés sont:

- SL-C(IAC, système de commande) 1: SR 1.13
- SL-C(IAC, système de commande) 2: SR 1.13 (1)
- SL-C(IAC, système de commande) 3: SR 1.13 (1)
- SL-C(IAC, système de commande) 4: SR 1.13 (1)

6 FR 2 – Commande d'utilisation

6.1 Objectif et descriptions du SL-C(UC)

Appliquer les privilèges assignés d'un utilisateur authentifié (être humain, processus logiciel ou appareil) pour effectuer les actions demandées sur l'IACS et surveiller l'utilisation de ces privilèges.

- SL 1 – Utilisation restreinte de l'IACS selon les privilèges spécifiés afin d'assurer la protection contre une mauvaise utilisation occasionnelle ou fortuite.
- SL 2 – Utilisation restreinte de l'IACS selon les privilèges spécifiés afin d'assurer la protection contre les contournements par des entités utilisant des moyens simples avec peu de ressources, des compétences génériques et une motivation faible.

- SL 3 – Utilisation restreinte de l'IACS selon les privilèges spécifiés afin d'assurer la protection contre les contournements par des entités utilisant des moyens complexes avec des ressources modérées, des compétences spécifiques à l'IACS et une motivation modérée.
- SL 4 – Utilisation restreinte de l'IACS selon les privilèges spécifiés afin d'assurer la protection contre les contournements par des entités utilisant des moyens complexes avec des ressources étendues, des compétences spécifiques à l'IACS et une motivation élevée.

6.2 Justification

Une fois l'utilisateur identifié et authentifié, le système de commande doit restreindre les actions permises à l'utilisation autorisée du système de commande. Les propriétaires d'actif et les intégrateurs de système doivent attribuer à chaque utilisateur (être humain, processus logiciel ou appareil), groupe, rôle, etc. (voir 5.6, SR 1.4 – Gestion des identificateurs) les privilèges qui définissent l'utilisation autorisée de l'IACS. La commande d'utilisation a pour objet d'assurer la protection contre les actions non autorisées sur les ressources du système de commande en vérifiant que les privilèges nécessaires ont été octroyés avant d'avoir autorisé à l'utilisateur d'effectuer les actions. La lecture ou l'écriture de données, le téléchargement de programmes et les configurations des paramètres sont des exemples d'actions. Il convient que les recommandations et lignes directrices incluent des mécanismes qui fonctionnent en modes mixtes. Par exemple, certaines ressources du système de commande exigent une protection de commande forte, comme des privilèges restrictifs, et d'autres non. Par extension, les exigences de commande d'utilisation doivent être étendues aux données inactives. Les privilèges utilisateur peuvent varier selon la durée du jour, la date, l'emplacement et les moyens d'accès.

6.3 SR 2.1 – Application de l'autorisation

6.3.1 Exigence

Sur toutes les interfaces, le système de commande doit permettre d'appliquer les autorisations attribuées à tous les utilisateurs humains pour le contrôle de l'utilisation du système de commande afin de prendre en charge la séparation des devoirs et du moindre privilège.

6.3.2 Justification et recommandations supplémentaires

Les politiques de contrôle d'utilisation (par exemple, politiques basées sur l'identité, sur le rôle et sur les réglementations) et les mécanismes d'application d'accès de lecture/d'écriture (par exemple, listes de contrôle d'accès, matrices de contrôle d'accès et cryptographie) sont employés pour contrôler l'utilisation entre les utilisateurs (êtres humains, processus logiciels et appareils) et les actifs (par exemple, appareils, dossiers, enregistrements, processus logiciels, programmes et domaines).

Après que le système de commande a vérifié l'identité d'un utilisateur (être humain, processus logiciel ou appareil) (voir 5.3, SR 1.1 – Identification et authentification d'utilisateur humain et 5.4, SR 1.2 – Identification et authentification du processus logiciel et de l'appareil), il doit également vérifier qu'une opération demandée est réellement autorisée conformément aux politiques et procédures de sécurité définies. Par exemple, dans une politique de contrôle d'accès basée sur le rôle, le système de commande vérifie les rôles attribués à un utilisateur vérifié ou à un actif et les privilèges attribués à ces rôles – si l'opération demandée est couverte par les autorisations, elle est exécutée, sinon elle est rejetée. Cela permet l'application de la séparation des devoirs et des moindres privilèges. Il convient que les mécanismes d'application d'utilisation ne soient pas autorisés à compromettre la performance opérationnelle du système de commande.

Les modifications prévues ou non des composants du système de commande peuvent avoir des effets significatifs sur la sécurité globale du système de commande. En conséquence, il convient que seuls les individus qualifiés et autorisés obtiennent l'utilisation des composants du système de commande afin d'initier des changements, y compris des mises à niveau et des modifications.

6.3.3 Améliorations d'exigences

6.3.3.1 SR 2.1 RE 1 – Application de l'autorisation pour tous les utilisateurs

Sur toutes les interfaces, le système de commande doit permettre d'appliquer les autorisations attribuées à tous les utilisateurs (êtres humains, processus logiciels et appareils) pour le contrôle de l'utilisation du système de commande afin de prendre en charge la séparation des devoirs et du moindre privilège.

6.3.3.2 SR 2.1 RE 2 – Mapping des autorisations aux rôles

Le système de commande doit permettre à un utilisateur ou à un rôle autorisé de définir et de modifier le mapping des autorisations aux rôles pour tous les utilisateurs humains.

NOTE 1 Ne pas limiter les rôles aux hiérarchies imbriquées fixes dans lesquelles un rôle d'un plus haut niveau est un surensemble d'un rôle moins privilégié constitue une bonne pratique communément admise. Par exemple, généralement, un administrateur système ne comprend pas nécessairement de privilèges opérateur.

NOTE 2 Cette RE s'applique aux processus logiciels ainsi qu'aux appareils.

6.3.3.3 SR 2.1 RE 3 – Contournement de la supervision

Le système de commande doit prendre en charge le contournement manuel de la supervision des autorisations des utilisateurs humains actuels pour une durée configurable ou une séquence d'événement.

NOTE La mise en œuvre d'un contournement manuel et audité des mécanismes automatisés dans le cas d'urgences ou d'autres événements importants est souvent nécessaire. Cela permet à un superviseur d'autoriser à un opérateur de réagir rapidement à des conditions inhabituelles sans fermer la session actuelle et sans établir de nouvelle session en tant qu'utilisateur humain à privilège élevé.

6.3.3.4 SR 2.1 RE 4 – Double approbation

Le système de commande doit prendre en charge une double approbation lorsqu'une action peut causer un impact sévère au processus industriel.

NOTE Limiter la double approbation aux actions qui exigent un niveau de confiance très élevé afin qu'elles soient réalisées de façon fiable et correcte constitue une bonne pratique communément admise. Exiger une double approbation met l'accent sur l'importance des conséquences qui résultent d'un échec d'une action correcte. Une modification d'un point de consigne d'un processus industriel critique est un exemple de situation dans laquelle une double approbation est exigée. Ne pas employer de mécanismes de double approbation lorsqu'une réponse immédiate est nécessaire à la sauvegarde des conséquences HSE, par exemple une coupure d'urgence d'un processus industriel, constitue une bonne pratique communément admise.

6.3.4 Niveaux de sécurité

Les exigences des quatre niveaux de sécurité relatifs à la SR 2.1 – Application de l'autorisation sont:

- SL-C(UC, système de commande) 1: SR 2.1
- SL-C(UC, système de commande) 2: SR 2.1 (1) (2)
- SL-C(UC, système de commande) 3: SR 2.1 (1) (2) (3)
- SL-C(UC, système de commande) 4: SR 2.1 (1) (2) (3) (4)

6.4 SR 2.2 –Contrôle d'utilisation sans fil

6.4.1 Exigence

Le système de commande doit permettre d'autoriser, de surveiller et d'appliquer les restrictions d'utilisation pour la connectivité sans fil au système de commande conformément aux pratiques de sécurité communément admises dans l'industrie.

6.4.2 Justification et recommandations supplémentaires

Toute technologie sans fil peut être considérée comme une simple option du protocole de communication, et il convient qu'elle le soit dans la plupart des cas. Ainsi, elle est soumise aux mêmes exigences de sécurité IACS que tout autre type de communication utilisé par l'IACS. Cependant, une analyse du risque peut résulter en une exigence pour les composants IACS sans fil pour la prise en charge des capacités de contrôle d'utilisation plus élevées que ce qui est généralement exigé des systèmes câblés pour la même utilisation et le même SL-T. Des différences de réglementations peuvent également résulter en des capacités différentes exigées entre les communications câblées et sans fil.

Comme indiqué en 5.8, SR 1.6 – Gestion des accès sans fil, les technologies sans fil comprennent, entre autres, les micro-ondes, les satellites, les radiocommunications à commutation de paquets, l'IEEE 802.11x, l'IEEE 802.15.4 (ZigBee, IEC 62591 – *Wireless*HART®, ISA-100.11a), l'IEEE 802.15.1 (Bluetooth), les routeurs mobiles WLAN, les téléphones mobiles avec connexion et différentes technologies infrarouges.

6.4.3 Améliorations d'exigences

6.4.3.1 SR 2.2 RE 1 – Identifier et consigner les appareils sans fil non autorisés

Le système de commande doit permettre d'identifier et de consigner les appareils sans fil non autorisés qui émettent dans l'environnement physique du système de commande.

6.4.3.2 Vide

6.4.4 Niveaux de sécurité

Les exigences des quatre niveaux de sécurité relatifs à la SR 2.2 –Contrôle d'utilisation sans fil sont:

- SL-C(UC, système de commande) 1: SR 2.2
- SL-C(UC, système de commande) 2: SR 2.2
- SL-C(UC, système de commande) 3: SR 2.2 (1)
- SL-C(UC, système de commande) 4: SR 2.2 (1)

6.5 SR 2.3 – Contrôle d'utilisation des appareils mobiles et portables

6.5.1 Exigence

Le système de commande doit permettre d'appliquer automatiquement des restrictions d'usage configurables qui comprennent:

a) l'évitement de l'utilisation d'appareils mobiles et portables;

b) l'exigence d'autorisation spécifique au contexte; et

c) la restriction du transfert du code et des données de/vers les appareils portables et mobiles.

6.5.2 Justification et recommandations supplémentaires

Un appareil portable et mobile peut introduire un trafic réseau, un logiciel malveillant et/ou une visibilité des informations non désirés. Il convient donc qu'un contrôle spécifique soit associé à leur utilisation dans l'environnement typique du système de commande. Les politiques et procédures de sécurité peuvent ne pas autoriser certaines fonctions ou activités exécutées au moyen d'appareils portables et/ou mobiles. Se référer à l'IEC 62443-2-1 pour des recommandations relatives à la permission d'utilisation qu'il convient de donner aux appareils portables et mobiles.

La protection des informations se trouvant dans les appareils portables et mobiles (par exemple, l'emploi de mécanismes cryptographiques pour assurer la confidentialité et l'intégrité lors du stockage et du transport hors des zones sous contrôle) est couverte ailleurs (voir l'Article 8, FR 4 – Confidentialité des données).

6.5.3 Améliorations d'exigences

6.5.3.1 SR 2.3 RE 1 – Application du statut de sécurité des appareils portables et mobiles

Le système de commande doit permettre de vérifier que les appareils portables et mobiles tentant de se connecter à une zone satisfont aux exigences de sécurité de cette zone.

6.5.3.2 Vide

6.5.4 Niveaux de sécurité

Les exigences des quatre niveaux de sécurité relatifs à la SR 2.3 – Contrôle d'utilisation des appareils mobiles et portables sont:

- SL-C(UC, système de commande) 1: SR 2.3
- SL-C(UC, système de commande) 2: SR 2.3
- SL-C(UC, système de commande) 3: SR 2.3 (1)
- SL-C(UC, système de commande) 4: SR 2.3 (1)

6.6 SR 2.4 – Code mobile

6.6.1 Exigence

Le système de commande doit permettre d'appliquer les restrictions d'utilisation des technologies de code mobile basées sur le potentiel à causer des dommages au système de commande qui comprennent:

a) l'évitement de l'exécution du code mobile;

b) l'exigence d'une authentification et d'une autorisation exactes pour l'origine du code;

c) la restriction du transfert du code mobile de/vers le système de commande; et

d) la surveillance de l'utilisation du code mobile.

6.6.2 Justification et recommandations supplémentaires

Les technologies de code mobile comprennent, entre autres, Java, JavaScript, ActiveX, PDF, Postscript, les films Shockwave, les animations Flash et VBScript. Les restrictions d'utilisation s'appliquent à la sélection et à l'utilisation du code mobile installé sur les serveurs et le code mobile téléchargé et exécuté sur des stations de travail individuelles. Il convient que les procédures de contrôle évitent le développement, l'acquisition ou l'introduction d'un code mobile inacceptable dans le système de commande. Par exemple, les échanges de codes mobiles peuvent être refusés directement avec le système de commande, mais peuvent être autorisés dans un environnement contrôlé voisin entretenu par du personnel IACS.

6.6.3 Améliorations d'exigences

6.6.3.1 SR 2.4 RE 1 – Vérification de l'intégrité du code mobile

Le système de commande doit permettre de vérifier l'intégrité du code mobile avant de permettre l'exécution du code.

6.6.3.2 Vide

6.6.4 Niveaux de sécurité

Les exigences des quatre niveaux de sécurité relatifs à la SR 2.4 – Code mobile sont:

- SL-C(UC, système de commande) 1: SR 2.4
- SL-C(UC, système de commande) 2: SR 2.4
- SL-C(UC, système de commande) 3: SR 2.4 (1)
- SL-C(UC, système de commande) 4: SR 2.4 (1)

6.7 SR 2.5 – Verrouillage de session

6.7.1 Exigence

Le système de commande doit permettre d'empêcher un accès ultérieur en initiant un verrouillage de session après une période d'inactivité configurable ou par initiation manuelle. Le verrouillage de session doit rester effectif jusqu'à ce que l'utilisateur humain possédant la session ou un autre être humain autorisé ré-établisse l'accès en utilisant des procédures d'identification et d'authentification appropriées.

6.7.2 Justification et recommandations supplémentaires

Il convient que l'entité responsable d'un système de commande emploie un verrouillage de session afin d'empêcher l'accès à des stations de travail ou à des nœuds spécifiés. Il convient que le système de commande active automatiquement des mécanismes de verrouillage de session après une période configurable pour les stations de travail ou les nœuds désignés. Dans certains cas, le verrouillage de session des stations de travail ou des nœuds de l'opérateur du système de commande n'est pas conseillé (par exemple des sessions exigées pour des réponses immédiates de l'opérateur dans des situations d'urgence). Les verrouillages de session ne remplacent pas la déconnexion du système de commande. Dans les situations où le système de commande ne prend pas en charge le verrouillage de session, il convient que l'entité responsable emploie des contre-mesures compensatoires appropriées (par exemple, en améliorant les mesures de sécurité physique, de sécurité du personnel et d'audit).

6.7.3 Améliorations d'exigences

Aucune.

6.7.4 Niveaux de sécurité

Les exigences des quatre niveaux de sécurité relatifs à la SR 2.5 – Verrouillage de session sont:

- SL-C(UC, système de commande) 1: SR 2.5
- SL-C(UC, système de commande) 2: SR 2.5
- SL-C(UC, système de commande) 3: SR 2.5
- SL-C(UC, système de commande) 4: SR 2.5

6.8 SR 2.6 – Terminaison de session distante

6.8.1 Exigence

Le système de commande doit permettre de terminer une session distante soit automatiquement après une période configurable d'inactivité, soit manuellement par l'utilisateur qui a initié la session.

6.8.2 Justification et recommandations supplémentaires

Une session distante est initiée lorsqu'un système de commande est accessible au-delà des limites d'une zone définies par le propriétaire d'actif, sur la base de l'appréciation du risque. La présente exigence peut être limitée aux sessions utilisées pour la surveillance du système de commande et les activités de maintenance (pas pour les opérations critiques) basées sur l'appréciation du risque du système de commande et sur les politiques et procédures de sécurité. Certains systèmes de commande ou composants peuvent ne pas autoriser la terminaison de sessions.

6.8.3 Améliorations d'exigences

Aucune.

6.8.4 Niveaux de sécurité

Les exigences des quatre niveaux de sécurité relatifs à la SR 2.6 – Terminaison de session distante sont:

- SL-C(UC, système de commande) 1: Non sélectionné
- SL-C(UC, système de commande) 2: SR 2.6
- SL-C(UC, système de commande) 3: SR 2.6
- SL-C(UC, système de commande) 4: SR 2.6

6.9 SR 2.7 – Commande de sessions concomitantes

6.9.1 Exigence

Le système de commande doit permettre de limiter le nombre de sessions concomitantes par interface pour un utilisateur donné (être humain, processus logiciel ou appareil) à un nombre configurable de sessions.

6.9.2 Justification et recommandations supplémentaires

Un DoS de privation de ressource peut se produire si aucune limite n'est imposée. Il existe un compromis entre le verrouillage potentiel d'un utilisateur spécifique et le verrouillage de tous les utilisateurs et services du fait d'un manque de ressources du système de commande. Les recommandations du fournisseur de produit et/ou de l'intégrateur de système sont susceptibles d'exiger la fourniture d'informations suffisantes quant au nombre de sessions qu'il convient d'attribuer.

6.9.3 Améliorations d'exigences

Aucune.

6.9.4 Niveaux de sécurité

Les exigences des quatre niveaux de sécurité relatifs à la SR 2.7 – Commande de sessions concomitantes sont:

- SL-C(UC, système de commande) 1: Non sélectionné
- SL-C(UC, système de commande) 2: Non sélectionné
- SL-C(UC, système de commande) 3: SR 2.7
- SL-C(UC, système de commande) 4: SR 2.7

6.10 SR 2.8 – Événements auditables

6.10.1 Exigence

Le système de commande doit permettre de générer des audits de vérification relatifs à la sécurité pour les catégories suivantes: contrôle d'accès, erreurs de requête, événements du système de fonctionnement, événements du système de commande, événements de sauvegarde et de restauration, modifications de configuration, activité de reconnaissance potentielle et événements de journal d'audit. Les audits de vérification individuels doivent comprendre l'horodatage, la source (appareil d'origine, processus logiciel ou compte utilisateur humain), la catégorie, le type, l'ID événement et le résultat de l'événement.

6.10.2 Justification et recommandations supplémentaires

Le but de la présente exigence est d'enregistrer l'occurrence des événements importants qui doivent être audités comme significatifs et pertinents pour la sécurité du système de commande. L'activité d'audit peut affecter la performance du système de commande. La fonction d'audit de sécurité est généralement coordonnée à la santé du réseau et à la fonction de surveillance du statut qui peut s'effectuer dans une zone différente. Il convient que les listes de vérification et les guides de configuration communément reconnus et admis soient pris en compte lors de l'établissement d'une liste d'événements auditables. Il convient que les politiques et procédures de sécurité définissent les événements auditables adéquats pour prendre en charge les investigations après coup des incidents de sécurité. De plus, il convient que les enregistrements d'audit soient suffisants pour surveiller l'efficacité et le bon fonctionnement des mécanismes de sécurité utilisés pour satisfaire aux exigences de la présente norme.

Il convient de noter que l'exigence d'enregistrement d'événement s'applique dans une fonctionnalité donnée du système, en particulier aux exigences données de sécurité du système à un niveau donné. Par exemple, l'exigence d'enregistrement d'événements d'authentification (dans la catégorie contrôle d'accès) sur un système SL 1 ne s'applique qu'au niveau de la fonctionnalité d'authentification exigé pour le SL 1 conformément aux exigences de l'Article 5. Des événements peuvent se produire dans tout composant du système de commande (par exemple des événements de connexion) ou peuvent s'observer par l'intermédiaire de moniteurs dédiés. Par exemple, le balayage de ports peut être détecté par un système de détection d'intrusion (IDS) ou par un système de prévention d'intrusion (IPS).

6.10.3 Améliorations d'exigences

6.10.3.1 SR 2.8 RE 1 – Trace d'audit au niveau du système et à gestion centralisée

Le système de commande doit permettre de gérer de façon centralisée les événements d'audit et de rassembler les enregistrements d'audit des composants multiples de tout le système de commande dans une trace d'audit au niveau du système (logique ou physique) et corrélée dans le temps. Le système de commande doit permettre d'exporter ces enregistrements d'audit au format normalisé par l'industrie pour l'analyse par des outils commerciaux d'analyse de journal, par exemple, module SIEM (*Security Information and Event Management*).

6.10.3.2 Vide

6.10.4 Niveaux de sécurité

Les exigences des quatre niveaux de sécurité relatifs à la SR 2.8 – Événements auditables sont:

- SL-C(UC, système de commande) 1: SR 2.8
- SL-C(UC, système de commande) 2: SR 2.8
- SL-C(UC, système de commande) 3: SR 2.8 (1)

- SL-C(UC, système de commande) 4: SR 2.8 (1)

6.11 SR 2.9 – Capacité de stockage de l'audit

6.11.1 Exigence

Le système de commande doit allouer une capacité suffisante de stockage d'enregistrement de l'audit conformément aux recommandations relatives à la configuration du système et à la gestion du journal communément reconnues. Le système de commande doit fournir des mécanismes d'audit permettant de réduire la probabilité de dépassement de cette capacité.

6.11.2 Justification et recommandations supplémentaires

Il convient que le système de commande fournisse une capacité de stockage d'audit suffisante, en tenant compte des politiques de rétention, de l'audit à effectuer et des exigences de traitement de l'audit en ligne. Les lignes directrices à prendre en compte peuvent inclure le NIST Special Publication (SP) 800-92 [27]. Il convient que la capacité de stockage d'audit soit suffisante pour conserver les journaux durant une période exigée par les politiques et réglementations applicables ou les exigences commerciales.

6.11.3 Améliorations d'exigences

6.11.3.1 SR 2.9 RE 1 – Avertissement lors du dépassement du seuil de la capacité de stockage d'enregistrement d'audit

Le système de commande doit permettre d'émettre un avertissement lorsque le volume de stockage d'enregistrement d'audit alloué atteint un pourcentage configurable de la capacité maximale de stockage d'enregistrement d'audit.

6.11.3.2 Vide

6.11.4 Niveaux de sécurité

Les exigences des quatre niveaux de sécurité relatifs à la SR 2.9 – Capacité de stockage de l'audit sont:

- SL-C(UC, système de commande) 1: SR 2.9
- SL-C(UC, système de commande) 2: SR 2.9
- SL-C(UC, système de commande) 3: SR 2.9 (1)
- SL-C(UC, système de commande) 4: SR 2.9 (1)

6.12 SR 2.10 – Réponse aux échecs de traitement d'audit

6.12.1 Exigence

Le système de commande doit permettre d'alerter le personnel et d'éviter la perte des services et fonctions essentiels dans le cas d'un échec de traitement d'audit. Le système de commande doit permettre de prendre en charge les actions appropriées en réponse à un échec de traitement d'audit, conformément aux recommandations et pratiques de l'industrie communément admises.

6.12.2 Justification et recommandations supplémentaires

La génération d'audit se produit généralement à la source de l'événement. Le traitement de l'audit implique la transmission, l'augmentation possible (comme l'ajout d'un horodatage) et le stockage permanent des enregistrements d'audit. Les échecs de traitement d'audit comprennent, par exemple, les erreurs logicielles ou matérielles, les échecs des mécanismes de capture de l'audit, et la capacité de stockage d'audit atteinte ou dépassée. Les lignes directrices à prendre en compte lors de la détermination des actions de réponse appropriées peuvent comprendre le NIST SP800-92. Il convient de noter que l'écrasement des enregistrements d'audit les plus anciens ou l'arrêt de la génération du journal d'audit sont des

réponses possibles au dépassement de la capacité de stockage d'audit, mais elles impliquent la perte potentielle d'informations légales et essentielles.

6.12.3 Améliorations d'exigences

Aucune.

6.12.4 Niveaux de sécurité

Les exigences des quatre niveaux de sécurité relatifs à la SR 2.10 – Réponse aux échecs de traitement d'audit sont:

- SL-C(UC, système de commande) 1: SR 2.10
- SL-C(UC, système de commande) 2: SR 2.10
- SL-C(UC, système de commande) 3: SR 2.10
- SL-C(UC, système de commande) 4: SR 2.10

6.13 SR 2.11– Horodatages

6.13.1 Exigence

Le système de commande doit fournir des horodatages pour l'utilisation dans la génération d'enregistrement d'audit.

6.13.2 Justification et recommandations supplémentaires

Il convient de générer les horodatages (comprenant la date et l'heure) en utilisant des horloges internes au système. Si la synchronisation au niveau du système n'est pas présente (ce qui est typique dans beaucoup d'installations), des décalages connus sont nécessaires à la prise en charge de l'analyse d'une séquence d'événements. De plus, la synchronisation des enregistrements d'audit générés en interne avec des événements externes peut exiger la synchronisation avec une source temporelle externe communément reconnue (comme le GPS, GLONASS et Galileo). Il convient d'assurer la protection de la source temporelle contre les modifications non autorisées.

6.13.3 Améliorations d'exigences

6.13.3.1 SR 2.11 RE 1 – Synchronisation temporelle interne

Le système de commande doit permettre de synchroniser les horloges internes au système à une fréquence configurable.

6.13.3.2 SR 2.11 RE 2 – Protection de l'intégrité de la source temporelle

La source temporelle doit être protégée contre des modifications non autorisées et doit engendrer un événement d'audit si tel était le cas.

6.13.4 Niveaux de sécurité

Les exigences des quatre niveaux de sécurité relatifs à la SR 2.11– Horodatages sont:

- SL-C(UC, système de commande) 1: Non sélectionné
- SL-C(UC, système de commande) 2: SR 2.11
- SL-C(UC, système de commande) 3: SR 2.11 (1)
- SL-C(UC, système de commande) 4: SR 2.11 (1) (2)

6.14 SR 2.12 – Non-répudiation

6.14.1 Exigence

Le système de commande doit permettre de déterminer si un utilisateur humain donné prend une mesure particulière.

6.14.2 Justification et recommandations supplémentaires

Les actions effectuées par un opérateur, la modification de la configuration du système de commande, la création d'informations, l'envoi d'un message, l'approbation d'informations (comme l'indication d'accords) et la réception d'un message sont des exemples de mesures particulières prises par un utilisateur. La non-répudiation protège contre les fausses affirmations provenant d'un utilisateur qui indique ne pas avoir pris de mesures spécifiques, d'un auteur qui indique ne pas avoir créé un document particulier, d'un émetteur qui indique ne pas avoir transmis un message, d'un récepteur qui indique ne pas avoir reçu de message ou d'un signataire qui indique ne pas avoir signé un document. Des services de non-répudiation peuvent être utilisés pour déterminer si les informations proviennent d'un utilisateur, si un utilisateur a effectué des actions spécifiques (par exemple, envoyer un courrier électronique et approuver un ordre de travail) ou a reçu des informations spécifiques. Les services de non-répudiation sont obtenus en employant différents techniques ou mécanismes (par exemple signatures numériques, accusés de réception d'un message numérique et horodatages).

6.14.3 Améliorations d'exigences

6.14.3.1 SR 2.12 RE 1 – Non-répudiation pour tous les utilisateurs

Le système de commande doit permettre de déterminer si un utilisateur donné (être humain, processus logiciel ou appareil) prend une mesure particulière.

6.14.3.2 Vide

6.14.4 Niveaux de sécurité

Les exigences des quatre niveaux de sécurité relatifs à la SR 2.12 – Non-répudiation sont:

- SL-C(UC, système de commande) 1: Non sélectionné
- SL-C(UC, système de commande) 2: Non sélectionné
- SL-C(UC, système de commande) 3: SR 2.12
- SL-C(UC, système de commande) 4: SR 2.12 (1)

7 FR 3 – Intégrité du système

7.1 Objectif et descriptions du SL-C(SI)

Garantir l'intégrité de l'IACS afin d'empêcher une manipulation non autorisée.

- SL 1 – Assurer la protection de l'intégrité de l'IACS contre les manipulations occasionnelles ou fortuites.
- SL 2 – Assurer la protection de l'intégrité de l'IACS contre les manipulations par quelqu'un utilisant des moyens simples, avec peu de ressources, des compétences génériques et une faible motivation.
- SL 3 – Assurer la protection de l'intégrité de l'IACS contre les manipulations par quelqu'un utilisant des moyens complexes, avec des ressources modérées, des compétences spécifiques à l'IACS et une motivation modérée.

- SL 4 – Assurer la protection de l'intégrité de l'IACS contre les manipulations par quelqu'un utilisant des moyens complexes, avec des ressources étendues, des compétences spécifiques à l'IACS et une motivation élevée.

7.2 Justification

L'IACS est souvent soumis à de multiples cycles d'essai (essai sur élément, essai de réception en usine, essai de réception sur site, certification, mise en service, etc.) afin d'établir que les systèmes agissent comme prévu avant le début de la production. Une fois fonctionnels, les propriétaires d'actif sont responsables du maintien de l'intégrité de l'IACS. Avec leur méthodologie d'appréciation du risque, les propriétaires d'actif peuvent attribuer différents niveaux de protection de l'intégrité à différents systèmes, canaux de communication et informations dans leur IACS. Il convient que l'intégrité des actifs physiques soit maintenue en état de fonctionnement et en état de non-fonctionnement, comme lors de la production, du stockage ou de la coupure de maintenance. Il convient que l'intégrité des actifs logiques soit maintenue lorsqu'ils sont transmis ou inactifs, comme lors du transfert sur un réseau ou lorsqu'ils demeurent dans un dépôt de données.

7.3 SR 3.1 – Intégrité de la communication

7.3.1 Exigence

Le système de commande doit permettre d'assurer la protection de l'intégrité des informations transmises.

7.3.2 Justification et recommandations supplémentaires

De nombreuses attaques réseau communes sont basées sur la manipulation de données en transmission, comme la manipulation de paquets réseau. Les réseaux commutés ou routés représentent pour les attaquants une plus grande opportunité de manipulation des paquets, puisque les accès non détectés à ces réseaux sont généralement plus simples et les mécanismes de commutation et de routage eux-mêmes peuvent être manipulés afin d'obtenir un plus grand accès aux informations transmises. La manipulation dans le contexte du système de commande peut comprendre le changement des valeurs de mesure transmises d'un capteur à un récepteur, ou l'altération des paramètres de commande envoyés d'une application de commande à un organe de commande.

Selon le contexte (par exemple, la transmission dans un segment de réseau local par rapport à la transmission par des réseaux non sécurisés) et le type de réseau utilisé dans la transmission (par exemple TCP/IP par rapport aux liaisons locales en série), des mécanismes réalisables et appropriés peuvent varier. Dans un petit réseau avec liaisons directes (point à point), la protection de l'accès physique à tous les nœuds peut suffire à des SL inférieurs si l'intégrité des points d'extrémité est également protégée (voir 7.6, SR 3.4 – Intégrité du logiciel et des informations), tandis que dans un réseau distribué dans des zones comportant une présence physique régulière ou du personnel ou dans une grande zone, l'accès physique au réseau est probablement non applicable. Si un service commercial est utilisé pour fournir des services de communication en tant que produit plutôt qu'en tant que service pleinement dédié (par exemple une ligne louée plutôt qu'une liaison T1), il peut être plus difficile d'obtenir les garanties nécessaires en ce qui concerne la mise en œuvre des contrôles de sécurité nécessaires à l'intégrité de la communication (du fait des restrictions légales par exemple). Lorsqu'il s'avère irréalisable ou peu pratique de satisfaire aux exigences de sécurité nécessaires, il peut être approprié de mettre en œuvre des contre-mesures compensatoires appropriées ou d'accepter explicitement le risque supplémentaire.

L'équipement industriel est souvent soumis aux conditions d'environnement pouvant causer des problèmes d'intégrité et/ou d'incidents faux positifs. Souvent, l'environnement contient des particules, des liquides, des vibrations, des gaz, des radiations et des perturbations électromagnétiques pouvant créer des conditions touchant à l'intégrité des câbles et signaux de communication. Il convient de concevoir l'infrastructure du réseau de façon à réduire le plus possible ces effets physiques/environnementaux sur l'intégrité de la communication. Par exemple, lorsque des particules, liquides et/ou gaz constituent un problème, il peut être

nécessaire d'utiliser sur le câble une prise enregistrée scellée (RJ-45) ou un connecteur M12 au lieu d'un connecteur RJ-45 de qualité commerciale. Le câble lui-même peut aussi nécessiter l'utilisation d'une gaine différente pour manipuler les particules, liquides et/ou gaz. Dans le cas où les vibrations sont un problème, les connecteurs M12 peuvent être nécessaires pour empêcher que les broches d'un connecteur RJ-45 ne se déconnectent lors de l'utilisation. Dans le cas où des radiations ou perturbations électromagnétiques sont un problème, il peut être nécessaire d'utiliser des câbles torsadés blindés ou des câbles à fibre optique pour éviter tout effet sur les signaux de communication. Il peut également être nécessaire d'effectuer une analyse spectrale sans fil dans ces zones si le réseau sans fil est prévu pour vérifier qu'il s'agit d'une solution viable.

7.3.3 Améliorations d'exigences

7.3.3.1 SR 3.1 RE 1 – Protection de l'intégrité cryptographique

Le système de commande doit permettre d'employer des mécanismes cryptographiques pour reconnaître les modifications d'informations lors des communications.

NOTE Déterminer l'utilisation appropriée de mécanismes cryptographiques pour l'authentification et l'intégrité des messages après un examen approfondi des besoins de sécurité et des ramifications potentielles de la performance du système et de la capacité à se rétablir d'une défaillance système constitue une bonne pratique communément admise.

7.3.3.2 Vide

7.3.4 Niveaux de sécurité

Les exigences des quatre niveaux de sécurité relatifs à la SR 3.1 – Intégrité de la communication sont:

- SL-C(SI, système de commande) 1: SR 3.1
- SL-C(SI, système de commande) 2: SR 3.1
- SL-C(SI, système de commande) 3: SR 3.1 (1)
- SL-C(SI, système de commande) 4: SR 3.1 (1)

7.4 SR 3.2 – Protection contre les programmes malveillants

7.4.1 Exigence

Le système de commande doit permettre d'employer des mécanismes de protection pour empêcher, détecter, consigner et atténuer les effets des programmes malveillants ou des logiciels non autorisés. Le système de commande doit permettre de mettre à jour les mécanismes de protection.

7.4.2 Justification et recommandations supplémentaires

Il convient que le système de commande utilise des mécanismes de protection pour empêcher, détecter, atténuer et consigner les programmes malveillants détectés (par exemple virus, vers, cheval de Troie et logiciels espions) transmis par courrier électronique, pièces jointes de courriers électroniques, accès Internet, support amovible (par exemple appareils USB, disquettes ou CD), documents PDF, services web, connexions au réseau ou ordinateurs portables infectés, ou par d'autres moyens courants.

Il convient que les mécanismes de détection soient capables de détecter les violations d'intégrité des fichiers binaires d'application et des fichiers de données. Des techniques peuvent comprendre, entre autres, la surveillance de l'intégrité et des attributs binaires, le hachage et les techniques de signature. L'atténuation des techniques peut comprendre, entre autres, le nettoyage de fichiers, la mise en quarantaine, la suppression de fichiers, la restriction de communication hôte et les IPS.

Les techniques de prévention peuvent comprendre, entre autres, les techniques de blocage et d'autorisation d'applications, la commande des supports amovibles, les techniques de bac à sable et les mécanismes spécifiques de plateformes informatiques comme les capacités restreintes de mise à jour du microprogramme, les bits NX, la prévention de l'exécution des données (DEP, *data execution prevention*), la randomisation de l'agencement de l'espace adressable (ASLR, *address space layout randomization*), la détection de corruption de pile et les contrôles d'accès obligatoires. Voir 10.4, SR 6.2 – Surveillance permanente pour une exigence associée impliquant des outils et techniques de surveillance du système de commande.

Les mécanismes de prévention et d'atténuation peuvent comprendre ceux conçus pour les éléments hôtes (comme les ordinateurs et services) et les mécanismes basés sur le réseau (comme les IDS et IPS), et les mécanismes basés sur les composants spécifiques du système de commande (comme les automates programmables et interfaces homme-machine).

7.4.3 Améliorations d'exigences

7.4.3.1 SR 3.2 RE 1 – Points d'entrée et de sortie de la protection contre les programmes malveillants

Le système de commande doit permettre d'employer des mécanismes de protection contre les programmes malveillants à tous les points d'entrée et de sortie.

NOTE Ces mécanismes sont communément fournis dans les supports amovibles, pare-feu, passerelles unidirectionnelles, serveurs web, serveurs proxy ou serveurs à accès distant.

7.4.3.2 SR 3.2 RE 2 – Gestion centralisée et déclaration de protection contre les programmes malveillants

Le système de commande doit permettre de gérer les mécanismes de protection contre les programmes malveillants.

NOTE Ces mécanismes sont généralement fournis par des solutions de gestion centralisée de l'infrastructure du point d'extrémité ou par module SIEM.

7.4.4 Niveaux de sécurité

Les exigences des quatre niveaux de sécurité relatifs à la SR 3.2 – Protection contre les programmes malveillants sont:

- SL-C(SI, système de commande) 1: SR 3.2
- SL-C(SI, système de commande) 2: SR 3.2 (1)
- SL-C(SI, système de commande) 3: SR 3.2 (1) (2)
- SL-C(SI, système de commande) 4: SR 3.2 (1) (2)

7.5 SR 3.3 – Vérification des fonctionnalités de sécurité

7.5.1 Exigence

Le système de commande doit permettre de prendre en charge la vérification des opérations prévues des fonctions de sécurité et la déclaration des découvertes d'anomalies lors des essais de réception en usine, des essais de réception sur site et de l'entretien systématique. Ces fonctions de sécurité doivent comprendre toutes les fonctions nécessaires à la prise en charge des exigences de sécurité spécifiées dans la présente norme.

7.5.2 Justification et recommandations supplémentaires

Il convient que le fournisseur de produit et/ou l'intégrateur de système fournissent des recommandations relatives à la soumission à l'essai des commandes de sécurité conçues. Les propriétaires d'actif doivent être conscients des ramifications possibles de l'exécution de ces essais de vérification lors du fonctionnement normal. Des détails relatifs à l'exécution de

ces vérifications doivent être spécifiés avec un examen approfondi des exigences pour les fonctionnements permanents (par exemple, planification ou notification préalable).

Des exemples de fonctions de vérification de sécurité comprennent:

- Des vérifications des mesures antivirus par l'essai du système de fichier du système de commande de l'Institut européen pour recherche des virus informatiques (EICAR). Il convient que le logiciel antivirus détecte cela, et il convient de mettre en œuvre des procédures de traitement d'incident appropriées.
- La vérification de l'identification, de l'authentification et des mesures de commande d'utilisation en tentant l'accès avec un compte non autorisé (cela peut être automatisé pour certaines fonctionnalités).
- La vérification des IDS comme contrôle de sécurité en incluant une règle dans l'IDS qui se déclenche en cas de trafic irrégulier mais non malveillant. L'essai peut alors être réalisé en introduisant un trafic qui déclenche cette règle et les procédures appropriées de surveillance de l'IDS et de traitement d'incident.
- La confirmation que le journal d'audit se déroule comme il est exigé par les politiques et procédures de sécurité et qu'il n'a pas été désactivé par une entité interne ou externe.

7.5.3 Améliorations d'exigences

7.5.3.1 SR 3.3 RE 1 – Mécanismes automatisés pour la vérification des fonctionnalités de sécurité

Le système de commande doit permettre d'employer des mécanismes automatisés pour prendre en charge la gestion des vérifications de sécurité lors des essais de réception en usine, des essais de réception sur site et d'entretien systématique.

7.5.3.2 SR 3.3 RE 2 – Vérification des fonctionnalités de sécurité en fonctionnement normal

Le système de commande doit permettre de prendre en charge la vérification du fonctionnement prévu des fonctions de sécurité en fonctionnement normal.

NOTE La mise en œuvre attentive de cette exigence constitue une bonne pratique communément admise, puisqu'elle peut causer des effets délétères. Elle n'est souvent pas considérée comme appropriée aux systèmes de sécurité.

7.5.4 Niveaux de sécurité

Les exigences des quatre niveaux de sécurité relatifs à la SR 3.3 – Vérification des fonctionnalités de sécurité sont:

- SL-C(SI, système de commande) 1: SR 3.3
- SL-C(SI, système de commande) 2: SR 3.3
- SL-C(SI, système de commande) 3: SR 3.3 (1)
- SL-C(SI, système de commande) 4: SR 3.3 (1) (2)

7.6 SR 3.4 – Intégrité du logiciel et des informations

7.6.1 Exigence

Le système de commande doit permettre de détecter, d'enregistrer, de déclarer et d'assurer la protection contre les modifications non autorisées des logiciels et informations inactives.

7.6.2 Justification et recommandations supplémentaires

Les modifications non autorisées sont des modifications pour lesquelles l'entité qui tente la modification ne possède pas les privilèges exigés pour cela. Cette exigence système

complète les exigences système relatives des exigences fondamentales 1 et 2. Les exigences fondamentales 1 et 2 impliquent l'application des rôles, privilèges et caractéristiques d'utilisation comme cela a été conçu. Les méthodes de vérification d'intégrité sont employées pour détecter, enregistrer, déclarer et assurer la protection contre les altérations logicielles et d'informations qui peuvent se produire si d'autres mécanismes de protection (comme l'application d'autorisation) ont été contournés. Il convient que le système de commande emploie des mécanismes d'intégrité formels ou recommandés (comme le hachage cryptographique). Par exemple, ces mécanismes pourraient être utilisés pour surveiller que les informations de configuration les plus récentes des appareils de terrain détectent les failles de sécurité (y compris les modifications non autorisées).

7.6.3 Améliorations d'exigences

7.6.3.1 SR 3.4 RE 1 – Notification automatisée relative aux violations d'intégrité

Le système de commande doit permettre d'utiliser des outils automatisés qui fournissent des notifications à un ensemble configurable de receveurs au moment de la découverte d'écarts lors de la vérification de l'intégrité.

7.6.3.2 Vide

7.6.4 Niveaux de sécurité

Les exigences des quatre niveaux de sécurité relatifs à la SR 3.4 – Intégrité du logiciel et des informations sont:

- SL-C(SI, système de commande) 1: Non sélectionné
- SL-C(SI, système de commande) 2: SR 3.4
- SL-C(SI, système de commande) 3: SR 3.4 (1)
- SL-C(SI, système de commande) 4: SR 3.4 (1)

7.7 SR 3.5 – Validation en entrée

7.7.1 Exigence

Le système de commande doit valider la syntaxe et le contenu de chaque entrée utilisée comme entrée de commande de processus industriel, ou comme entrée qui touche directement l'action du système de commande.

7.7.2 Justification et recommandations supplémentaires

Il convient que les règles de vérification de la syntaxe des entrées du système de commande comme les points de consigne soient en place pour vérifier que ces informations n'ont pas été altérées et sont conformes à la spécification. Il convient que les entrées transmises aux interpréteurs soient préexaminées afin d'empêcher le contenu d'être involontairement interprété comme des commandes. Il est à noter qu'il s'agit d'une exigence système de sécurité, par conséquent elle ne traite pas les erreurs humaines, comme par exemple livrer un nombre entier se trouvant hors de la plage attendue.

Les pratiques de l'industrie généralement admises pour la validation des données d'entrée comprennent des valeurs aberrantes pour un type de champ défini, des caractères invalides dans des champs de données, des données manquantes ou incomplètes et la surcharge de la mémoire tampon. Les attaques par injection SQL, XSS ou paquets malformés (comme typiquement générés lors du fuzzing de protocole) sont des exemples supplémentaires de cas où des entrées invalides mènent à des problèmes de sécurité du système. Les lignes directrices à prendre en compte peuvent comprendre le guide du code OWASP [31].

7.7.3 Améliorations d'exigences

Aucune.

7.7.4 Niveaux de sécurité

Les exigences des quatre niveaux de sécurité relatifs à la SR 3.5 – Validation en entrée sont:

- SL-C(SI, système de commande) 1: SR 3.5
- SL-C(SI, système de commande) 2: SR 3.5
- SL-C(SI, système de commande) 3: SR 3.5
- SL-C(SI, système de commande) 4: SR 3.5

7.8 SR 3.6 – Sortie déterministe

7.8.1 Exigence

Le système de commande doit permettre de paramétrer les sorties sur un état prédéterminé si le fonctionnement normal ne peut être maintenu par suite d'une attaque.

7.8.2 Justification et recommandations supplémentaires

Le comportement déterministe des sorties du système de commande par suite de menaces contre le système de commande constitue une caractéristique importante pour la garantie de l'intégrité du fonctionnement normal. Idéalement, le système de commande continue de fonctionner normalement lorsqu'il est attaqué, mais s'il ne peut maintenir un fonctionnement normal, alors ses sorties doivent échouer à un état prédéterminé. L'état prédéterminé approprié des sorties du système de commande dépend de l'application et pourrait être l'une des options utilisateur configurables suivantes:

- Non alimenté – les sorties échouent en état non alimenté
- Maintenu – les sorties échouent à la dernière bonne valeur connue
- Fixe – les sorties échouent à une valeur fixe fixée par le propriétaire d'actif ou par une application

7.8.3 Améliorations d'exigences

Aucune.

7.8.4 Niveaux de sécurité

Les exigences des quatre niveaux de sécurité relatifs à la SR 3.6 – Sortie déterministe sont:

- SR-C(SI, système de commande) 1: SR 3.6
- SR-C(SI, système de commande) 2: SR 3.6
- SR-C(SI, système de commande) 3: SR 3.6
- SR-C(SI, système de commande) 4: SR 3.6

7.9 SR 3.7 – Traitement des erreurs

7.9.1 Exigence

Le système de commande doit identifier et traiter les conditions d'erreur de façon à pouvoir les corriger de manière efficace. Cela doit être réalisé sans fournir des informations susceptibles d'être exploitées par des adversaires afin d'attaquer l'IACS, sauf si la révélation de ces informations est nécessaire au dépannage des problèmes dans les délais.

7.9.2 Justification et recommandations supplémentaires

Il convient que la structure et la teneur des messages d'erreur soient soigneusement prises en compte par le fournisseur de produit et/ou l'intégrateur de système. Il convient que les messages d'erreur générés par le système de commande fournissent des informations utiles et rapides sans toutefois révéler des informations potentiellement dommageables pouvant

être utilisées par des adversaires afin d'exploiter l'IACS. Puisqu'il n'est pas toujours évident de savoir si une condition d'erreur particulière est due à un événement de sécurité, tous les messages d'erreur peuvent nécessiter d'être facilement accessibles lors de la réponse d'incident. Il convient que la divulgation de ces informations soit justifiée par la nécessité d'une résolution des conditions d'erreur dans les délais. Les lignes directrices à prendre en compte pourraient comprendre le guide du code OWASP [31].

7.9.3 Améliorations d'exigences

Aucune.

7.9.4 Niveaux de sécurité

Les exigences des quatre niveaux de sécurité relatifs à la SR 3.7 – Traitement des erreurs sont:

- SL-C(SI, système de commande) 1: Non sélectionné
- SL-C(SI, système de commande) 2: SR 3.7
- SL-C(SI, système de commande) 3: SR 3.7
- SL-C(SI, système de commande) 4: SR 3.7

7.10 SR 3.8 – Intégrité de la session

7.10.1 Exigence

Le système de commande doit permettre d'assurer la protection de l'intégrité de la session. Le système de commande doit rejeter tout usage d'ID de session invalide.

7.10.2 Justification et recommandations supplémentaires

Cette commande se concentre sur la protection des communications au niveau de la session, par rapport aux communications au niveau du paquet. Le but de cette commande est d'instaurer de la confiance à chaque extrémité d'une session de communication, dans l'identité en cours de l'autre partie et dans la validité de l'information transmise. Par exemple, cette commande traite des attaques homme au milieu, comprenant le détournement de session, l'insertion de fausses informations dans une session ou les attaques de rejeu. L'utilisation de mécanismes d'intégrité de session peut avoir un coût important et par conséquent il convient que leur utilisation tienne compte des exigences des communications en temps réel.

7.10.3 Améliorations d'exigences

7.10.3.1 SR 3.8 RE 1 – Invalidation d'ID de session après terminaison de session

Le système de commande doit permettre d'invalider les ID de session au moment de la déconnexion de l'utilisateur ou de la terminaison de session (y compris les séances de navigation).

7.10.3.2 SR 3.8 RE 2 – Génération d'ID de session unique

Le système de commande doit permettre de générer un ID de session unique pour chaque session et doit traiter tous les ID de session non prévus comme invalides.

7.10.3.3 SR 3.8 RE 3 – Caractère aléatoire des ID de session

Le système de commande doit permettre de générer des ID de session uniques avec des sources aléatoires communément admises.

NOTE Le détournement de session et d'autres attaques homme au milieu ou l'injection de fausses informations profitent souvent d'ID de session faciles à deviner (clés ou autres secrets partagés) ou de l'utilisation d'ID de

session qui n'ont pas été correctement invalidés à la terminaison de session. Ainsi, la validité d'un authentifiant de session doit être étroitement lié à la durée de vie d'une session. Utiliser le caractère aléatoire dans la génération d'ID de session uniques aide à assurer la protection contre les attaques de force brute pour la détermination des futurs ID de session.

7.10.4 Niveaux de sécurité

Les exigences des quatre niveaux de sécurité relatifs à la SR 3.8 – Intégrité de la session sont:

- SL-C(SI, système de commande) 1: Non sélectionné
- SL-C(SI, système de commande) 2: SR 3.8
- SL-C(SI, système de commande) 3: SR 3.8 (1) (2)
- SL-C(SI, système de commande) 4: SR 3.8 (1) (2) (3)

7.11 SR 3.9 – Protection des informations d'audit

7.11.1 Exigence

Le système de commande doit assurer la protection des informations et des outils d'audit (si présents) contre un accès, des modifications ou une suppression non autorisés.

7.11.2 Justification et recommandations supplémentaires

Les informations d'audit comprennent toutes les informations (par exemple, les enregistrements, les paramètres et les rapports d'audit) nécessaires à un audit de l'activité du système de commande réussi. Les informations d'audit sont importantes pour la correction d'erreurs, le recouvrement des failles de sécurité, les enquêtes et les efforts relatifs. Les mécanismes de protection améliorée contre les modifications et suppressions comprennent le stockage des informations d'audit sur un support à exécution matérielle à écriture unique.

7.11.3 Améliorations d'exigences

7.11.3.1 SR 3.9 RE 1 – Enregistrements d'audit sur support à écriture unique

Le système de commande doit permettre de produire des enregistrements d'audit sur un support à exécution matérielle à écriture unique.

7.11.3.2 Vide

7.11.4 Niveaux de sécurité

Les exigences des quatre niveaux de sécurité relatifs à la SR 3.9 – Protection des informations d'audit sont:

- SL-C(SI, système de commande) 1: Non sélectionné
- SL-C(SI, système de commande) 2: SR 3.9
- SL-C(SI, système de commande) 3: SR 3.9
- SL-C(SI, système de commande) 4: SR 3.9 (1)

8 FR 4 – Confidentialité des données

8.1 Objectif et descriptions du SL-C(DC)

Garantir la confidentialité des informations sur les canaux de communication et dans les dépôts de données afin d'empêcher une divulgation non autorisée.

- SL 1 – Empêcher la divulgation non autorisée des informations par écoute illicite ou exposition occasionnelle.

- SL 2 – Empêcher la divulgation non autorisée des informations à une entité cherchant activement par des moyens simples, avec peu de ressources, des compétences génériques et une faible motivation.
- SL 3 – Empêcher la divulgation non autorisée des informations à une entité cherchant activement par des moyens complexes, avec des ressources modérées, des compétences spécifiques à l'IACS et une motivation modérée.
- SL 4 – Empêcher la divulgation non autorisée des informations à une entité cherchant activement par des moyens complexes, avec des ressources étendues, des compétences spécifiques à l'IACS et une motivation élevée.

8.2 Justification

Certaines informations générées par le système de commande, qu'elles soient inactives ou en transit, sont de nature confidentielle ou sensible. Cela implique que certains canaux de communication et entrepôts de données exigent une protection contre l'écoute illicite ou l'accès non autorisé.

8.3 SR 4.1 – Confidentialité des informations

8.3.1 Exigence

Le système de commande doit permettre d'assurer la protection de la confidentialité des informations pour lesquelles une autorisation de lecture explicite est prise en charge, qu'elles soient inactives ou en transit.

8.3.2 Justification et recommandations supplémentaires

La protection des informations inactives ou en transit peut être maintenue par des moyens physiques, par compartimentation ou par chiffrement, parmi d'autres techniques. Il est essentiel que la technique choisie tienne compte des ramifications potentielles sur la performance du système de commande et de la capacité à se rétablir d'une défaillance ou d'une attaque du système.

La décision de savoir s'il convient d'assurer ou non la protection de la confidentialité d'une information donnée dépend du contexte et ne peut être établie à la conception du produit. Cependant, le fait qu'une organisation limite l'accès à l'information en configurant des autorisations de lecture explicite dans le système de commande indique que cette information est considérée comme confidentielle par l'organisation. Par conséquent, il convient que toutes les informations pour lesquelles le système de commande prend en charge la capacité à attribuer des autorisations de lecture explicite soient considérées comme potentiellement confidentielles, et ainsi il convient que le système de commande permette également d'en assurer la protection.

Des organisations et industries différentes peuvent exiger des niveaux de force de chiffrement différents pour différentes catégories d'informations, sur la base de la sensibilité des informations ainsi que sur les normes de l'industrie et les exigences relatives à la réglementation (voir 8.5, SR 4.3 – Utilisation de la cryptographie). Dans certaines situations, les informations de configuration réseau stockées et traitées dans les commutateurs et routeurs peuvent être considérées comme confidentielles.

Les communications impliquant des transferts d'informations exposées peuvent être vulnérables à l'écoute illicite ou à l'altération. Si le système de commande dépend d'un fournisseur de service de communications externe, il peut être plus difficile d'obtenir les garanties nécessaires concernant la mise en œuvre des exigences de sécurité nécessaires à la confidentialité de la communication. Dans ces cas, il peut être approprié de mettre en œuvre des contre-mesures compensatoires ou d'accepter ouvertement le risque supplémentaire.