IEC 62443-3-3

Edition 1.0 2013-08

INTERNATIONAL STANDARD

colour inside

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

IEC 62443-3-3:2013(E)

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

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
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 corrigenda or an amendment might have been published.

Useful links:

IEC publications search - www.iec.ch/searchpub

The advanced search enables you 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It also gives information on projects, replaced and withdrawn publications.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 on-line and also once a month by email.

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary (IEV) on-line.

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: csc@iec.ch.

IEC 62443-3-3

Edition 1.0 2013-08

INTERNATIONAL STANDARD

colour inside

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

PRICE CODE XC

ICS 25.040.40; 35.110

ISBN 978-2-8322-1036-9

Warning! Make sure that you obtained this publication from an authorized distributor.

CONTENTS

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.

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.

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.

A bilingual version of this publication may be issued at a later date.

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.

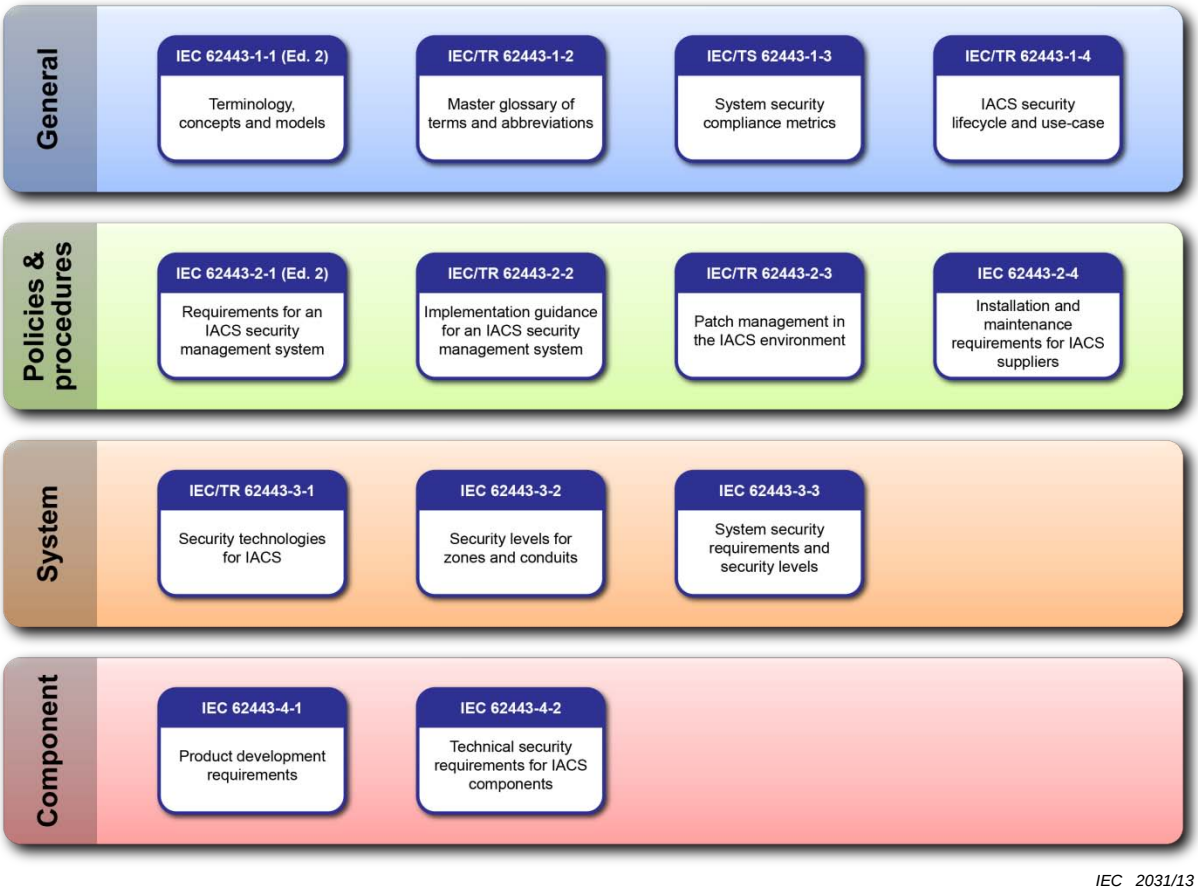

Figure 1 – Structure of the IEC 62443 series

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:

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

b) 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;

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

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

e) 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: SR 3.4
- 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.

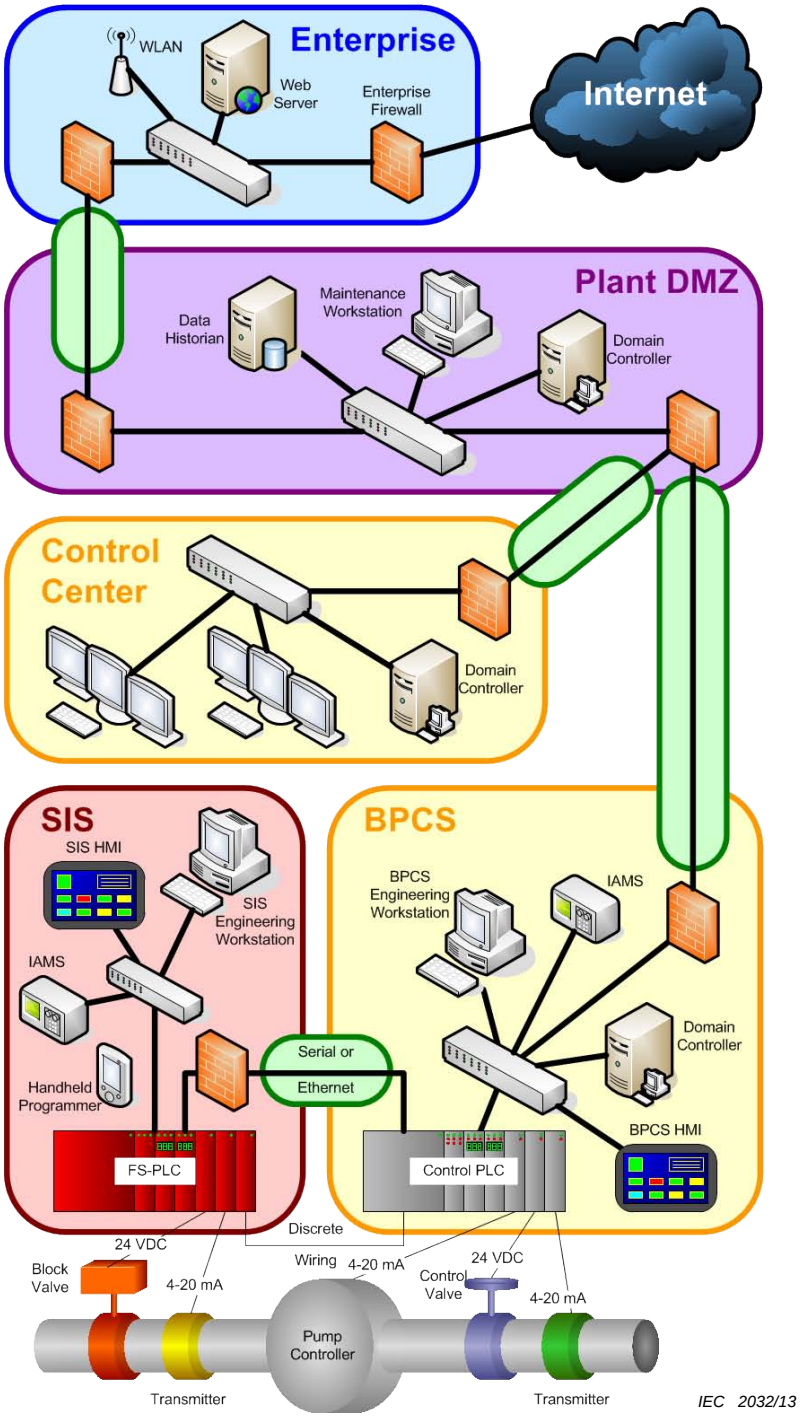

Figure A.1 – High-level process-industry example showing zones and conduits

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.

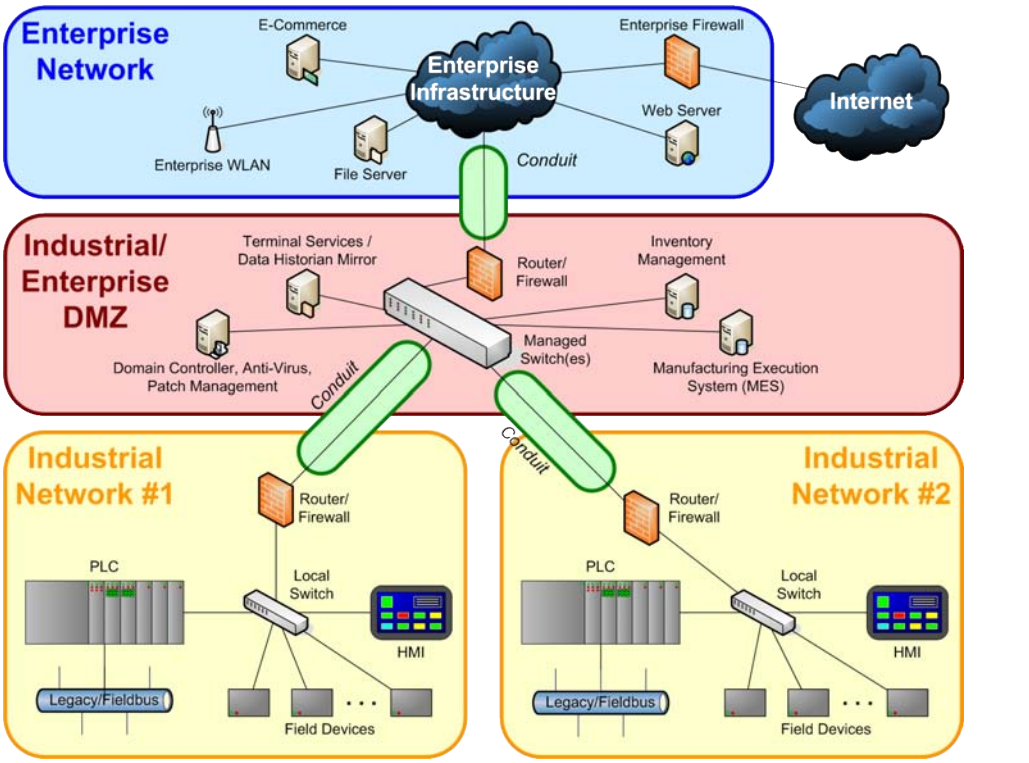

Figure A.2 – High-level manufacturing example showing zones and conduits

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).

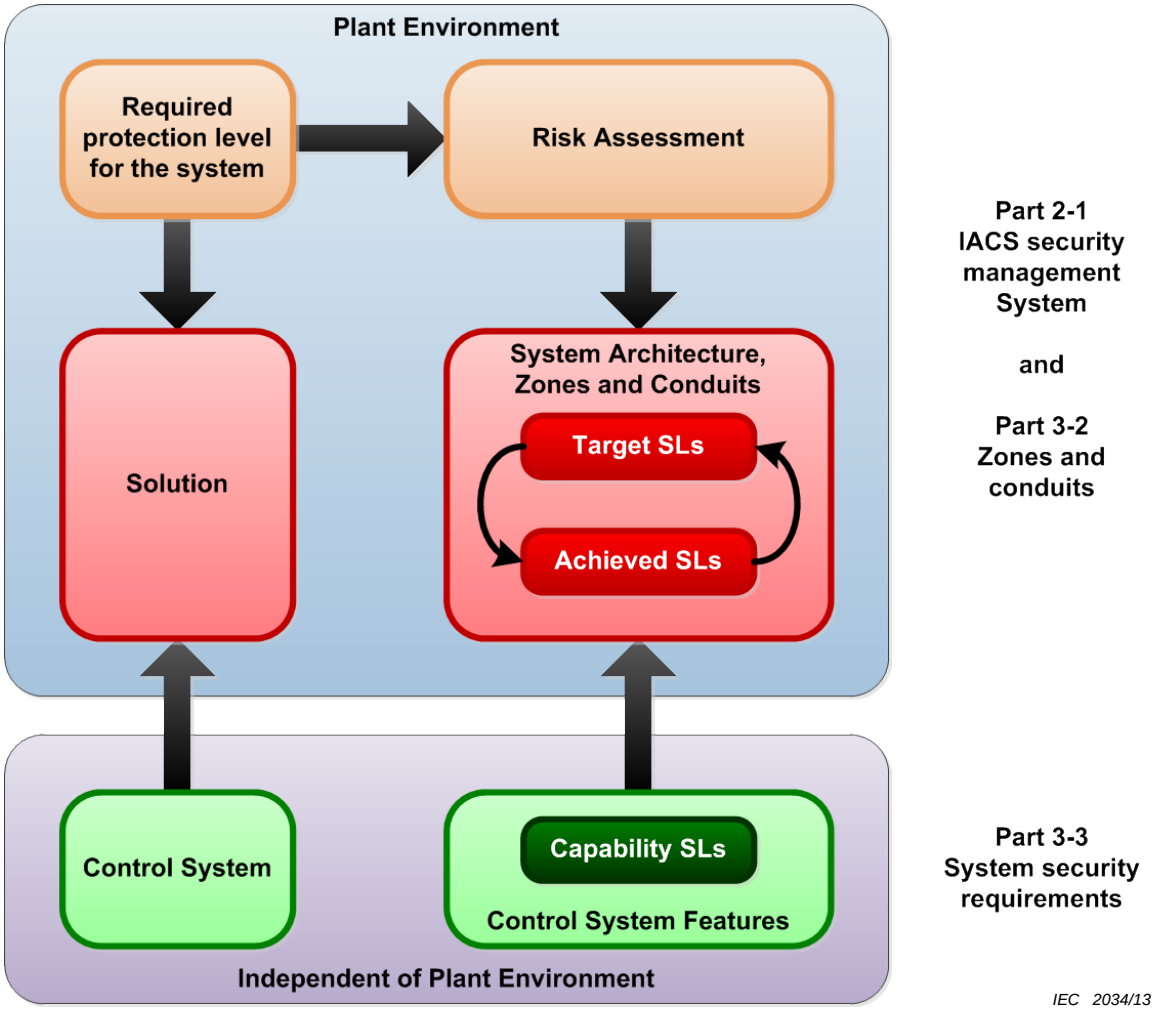

Figure A.3 – Schematic of correlation of the use of different SL types

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/

_____

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

3, rue de Varembé
PO Box 131
CH-1211 Geneva 20
Switzerland

Tel: + 41 22 919 02 11
Fax: + 41 22 919 03 00
info@iec.ch
www.iec.ch