

INTERNATIONAL STANDARD

NORME INTERNATIONALE



HORIZONTAL PUBLICATION
PUBLICATION HORIZONTALE

**Security for industrial automation and control systems –
Part 2-1: Security program requirements for IACS asset owners**

**Sécurité des systèmes d'automatisation et de commande industrielles –
Partie 2-1: Exigences de programme de sécurité pour les propriétaires d'actif
IACS**



THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2024 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester. If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de l'IEC ou du Comité national de l'IEC du pays du demandeur. Si vous avez des questions sur le copyright de l'IEC ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de l'IEC de votre pays de résidence.

IEC Secretariat
3, rue de Varembe
CH-1211 Geneva 20
Switzerland

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

About the IEC

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

About IEC publications

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

IEC publications search - webstore.iec.ch/advsearchform

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 It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

Stay up to date on all new IEC publications. Just Published details all new publications released. Available online and once a month by email.

IEC Customer Service Centre - webstore.iec.ch/csc

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

IEC Products & Services Portal - products.iec.ch

Discover our powerful search engine and read freely all the publications previews, graphical symbols and the glossary. With a subscription you will always have access to up to date content tailored to your needs.

Electropedia - www.electropedia.org

The world's leading online dictionary on electrotechnology, containing more than 22 500 terminological entries in English and French, with equivalent terms in 25 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

A propos de l'IEC

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

A propos des publications IEC

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

Recherche de publications IEC -

webstore.iec.ch/advsearchform

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

IEC Just Published - webstore.iec.ch/justpublished

Restez informé sur les nouvelles publications IEC. Just Published détaille les nouvelles publications parues. Disponible en ligne et une fois par mois par email.

Service Clients - webstore.iec.ch/csc

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

IEC Products & Services Portal - products.iec.ch

Découvrez notre puissant moteur de recherche et consultez gratuitement tous les aperçus des publications, symboles graphiques et le glossaire. Avec un abonnement, vous aurez toujours accès à un contenu à jour adapté à vos besoins.

Electropedia - www.electropedia.org

Le premier dictionnaire d'électrotechnologie en ligne au monde, avec plus de 22 500 articles terminologiques en anglais et en français, ainsi que les termes équivalents dans 25 langues additionnelles. Egalement appelé Vocabulaire Electrotechnique International (IEV) en ligne.

INTERNATIONAL STANDARD

NORME INTERNATIONALE



**Security for industrial automation and control systems –
Part 2-1: Security program requirements for IACS asset owners**

**Sécurité des systèmes d'automatisation et de commande industrielles –
Partie 2-1: Exigences de programme de sécurité pour les propriétaires d'actif
IACS**

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

COMMISSION
ELECTROTECHNIQUE
INTERNATIONALE

ICS 25.040.40, 35.100.05

ISBN 978-2-8322-9459-8

**Warning! Make sure that you obtained this publication from an authorized distributor.
Attention! Veuillez vous assurer que vous avez obtenu cette publication via un distributeur agréé.**

CONTENTS

FOREWORD.....	6
INTRODUCTION.....	8
1 Scope.....	10
2 Normative references	11
3 Terms, definitions, abbreviated terms and conventions	11
3.1 Terms and definitions.....	11
3.2 Abbreviated terms and acronyms	15
3.3 Conventions.....	16
4 Concepts	17
4.1 Use of this document	17
4.1.1 Applicable roles	17
4.1.2 Use of this document by asset owners	17
4.1.3 Use of this document by service providers and product suppliers.....	19
4.2 Maturity level (ML) definitions	20
4.3 Security levels (SLs)	21
4.4 Requirements definitions.....	21
4.4.1 Requirements organization	21
4.4.2 Requirements cross-references	22
4.4.3 Requirement conventions	22
5 Conformance and assessment.....	22
5.1 Overview.....	22
5.2 Conformity evidence	23
5.3 Requirements evaluation and profiles	24
5.3.1 Overview	24
5.3.2 Evaluation of risk to requirements.....	24
5.3.3 Profiles	24
5.3.4 Conformity assessment for the asset owner role.....	25
6 SPE 1 – Organizational security measures	25
6.1 Purpose	25
6.2 ORG 1 – Security related organization and policies.....	25
6.2.1 ORG 1.1: Information security management system (ISMS).....	25
6.2.2 ORG 1.2: Background checks.....	26
6.2.3 ORG 1.3: Security roles and responsibilities	26
6.2.4 ORG 1.4: Security awareness training	27
6.2.5 ORG 1.5: Security responsibilities training.....	27
6.2.6 ORG 1.6: Supply chain security	28
6.3 ORG 2 – Security assessments and reviews	28
6.3.1 ORG 2.1: Security risk mitigation	28
6.3.2 ORG 2.2: Processes for discovery of security anomalies	29
6.3.3 ORG 2.3: Secure development and support	30
6.3.4 ORG 2.4: SP reviews.....	30
6.4 ORG 3 – Security of physical access	30
6.4.1 ORG 3.1: Physical access control.....	30
7 SPE 2 – Configuration management	31
7.1 Purpose	31

7.2	CM 1 – Inventory management of IACS hardware/software components and network communications	31
7.2.1	CM 1.1: Asset inventory baseline	31
7.2.2	CM 1.2: Infrastructure drawings/documentation	32
7.2.3	CM 1.3: Configuration settings	32
7.2.4	CM 1.4: Change control	33
8	SPE 3 – Network and communications security	33
8.1	Purpose	33
8.2	NET 1 – System segmentation	33
8.2.1	NET 1.1: Segmentation from non-IACS zones	33
8.2.2	NET 1.2: Documentation of zones and network zone interconnections	34
8.2.3	NET 1.3: Network segmentation from safety systems	34
8.2.4	NET 1.4: Network autonomy	35
8.2.5	NET 1.5: Network disconnection from external networks	35
8.2.6	NET 1.6: Internal network access control	35
8.2.7	NET 1.7: Network accessible services	36
8.2.8	NET 1.8: User messaging	36
8.2.9	NET 1.9: Network time distribution	36
8.3	NET 2 – Secure wireless access	37
8.3.1	NET 2.1: Wireless protocols	37
8.3.2	NET 2.2: Wireless network segmentation	37
8.3.3	NET 2.3: Wireless properties and addresses	38
8.4	NET 3 – Secure remote access	38
8.4.1	NET 3.1: Remote access applications	38
8.4.2	NET 3.2: Remote access connections	39
8.4.3	NET 3.3: Remote access termination	39
9	SPE 4 – Component security	40
9.1	Purpose	40
9.2	COMP 1 – Components and portable media	40
9.2.1	COMP 1.1: Component hardening	40
9.2.2	COMP 1.2: Dedicated portable media	41
9.3	COMP 2 – Malware protection	41
9.3.1	COMP 2.1: Malware free	41
9.3.2	COMP 2.2: Malware protection	42
9.3.3	COMP 2.3: Malware protection software validation and installation	42
9.4	COMP 3 – Patch management	43
9.4.1	COMP 3.1: Security patch authenticity/integrity	43
9.4.2	COMP 3.2: Security patch validation and installation	43
9.4.3	COMP 3.3: Security patch status	43
9.4.4	COMP 3.4: Security patching retention of security	44
9.4.5	COMP 3.5: Security patch mitigation	44
10	SPE 5 – Protection of data	44
10.1	Purpose	44
10.2	DATA 1 – Protection of data	45
10.2.1	DATA 1.1: Data classification	45
10.2.2	DATA 1.2: Data confidentiality	45
10.2.3	DATA 1.3: Safety system configuration mode	46
10.2.4	DATA 1.4: Data retention policy	46
10.2.5	DATA 1.5: Cryptographic mechanisms	47

10.2.6	DATA 1.6: Key management.....	47
10.2.7	DATA 1.7: Data Integrity	47
11	SPE 6 – User access control	48
11.1	Purpose	48
11.2	USER 1 – Identification and authentication	48
11.2.1	USER 1.1: User identity assignment	48
11.2.2	USER 1.2: User identity removal.....	49
11.2.3	USER 1.3: User identity persistence	49
11.2.4	USER 1.4: Access rights assignment.....	50
11.2.5	USER 1.5: Least privilege.....	50
11.2.6	USER 1.6: Software service authentication.....	50
11.2.7	USER 1.7: Software services interactive login rights.....	51
11.2.8	USER 1.8: Human user authentication	51
11.2.9	USER 1.9: Multifactor authentication (MFA).....	51
11.2.10	USER 1.10: Mutual authentication	52
11.2.11	USER 1.11: Password protection	52
11.2.12	USER 1.12: Shared and disclosed/compromised passwords	53
11.2.13	USER 1.13: User login display information.....	53
11.2.14	USER 1.14: User login failure displays	53
11.2.15	USER 1.15: Consecutive login failures.....	54
11.2.16	USER 1.16: Session integrity.....	54
11.2.17	USER 1.17: Concurrent sessions.....	54
11.2.18	USER 1.18: Screen lock	55
11.2.19	USER 1.19: Component authentication	55
11.3	USER 2 – Authorization and access control	55
11.3.1	USER 2.1: Authorization	55
11.3.2	USER 2.2: Separation of duties	56
11.3.3	USER 2.3: Multiple approvals	56
11.3.4	USER 2.4: Manual elevation of privileges	57
12	SPE 7 – Event and incident management	57
12.1	Purpose	57
12.2	EVENT 1 – Event and incident management	57
12.2.1	EVENT 1.1: Event detection	57
12.2.2	EVENT 1.2: Event reporting.....	58
12.2.3	EVENT 1.3: Event reporting interfaces.....	58
12.2.4	EVENT 1.4: Logging	59
12.2.5	EVENT 1.5: Log entries	59
12.2.6	EVENT 1.6: Log access	59
12.2.7	EVENT 1.7: Event analysis	60
12.2.8	EVENT 1.8: Incident handling and response	60
12.2.9	EVENT 1.9: Vulnerability handling	60
13	SPE 8 – System integrity and availability.....	61
13.1	Purpose	61
13.2	AVAIL 1 – System availability and intended functionality	61
13.2.1	AVAIL 1.1: Continuity management	61
13.2.2	AVAIL 1.2: Resource availability management	62
13.2.3	AVAIL 1.3: Failure-state.....	62
13.3	AVAIL 2 – Backup/restore/archive.....	62
13.3.1	AVAIL 2.1: Backup.....	62

13.3.2	AVAIL 2.2: Backup non-interference	63
13.3.3	AVAIL 2.3: Backup verification.....	63
13.3.4	AVAIL 2.4: Backup media	63
13.3.5	AVAIL 2.5: Backup restoration	64
Annex A (informative) Cross-references to other standards		65
A.1	Requirements relationship to IEC 62443-2-4	65
A.2	Requirements relationship to IEC 62443-3-3	68
A.3	Requirements relationship to IEC 62443-4-2	70
A.4	Requirements relationship to ISO/IEC 27001:2013.....	73
A.5	Requirements relationship to the NIST CSF	77
Annex B (informative) Establishing and maintaining an IACS SP		81
B.1	General.....	81
B.2	Managing cybersecurity risk.....	82
B.2.1	Understanding cybersecurity risk	82
B.2.2	Impacts of cybersecurity compromises.....	82
B.2.3	Risk ranking	82
B.2.4	Cybersecurity attack exposure versus likelihood	83
B.3	Elements of a cybersecurity risk assessment/management process	84
B.4	Elements of a cybersecurity risk assessment/management process	85
Annex C (informative) Evaluating MLs		87
C.1	Approach to evaluating MLs	87
C.2	Examples of how to evaluate MLs	88
Bibliography.....		89
Figure 1 – Roles and responsibilities in the IEC 62443 series		11
Figure B.1 – Example of process flow for cybersecurity risk management.....		85
Figure B.2 – Levels of protection an asset requires.....		86
Table 1 – ML levels and descriptions		20
Table 2 – Typical conformity evidence types		23
Table A.1 – IEC 62443-2-4 cross-references.....		65
Table A.2 – Cross-reference of IEC 62443-2-1 to IEC 62443-2-4		66
Table A.3 – IEC 62443-3-3 cross-references.....		68
Table A.4 – Cross-reference of IEC 62443-2-1 to IEC 62443-3-3		69
Table A.5 – IEC 62443-4-2 cross-references.....		70
Table A.6 – Cross-reference of IEC 62443-2-1 to IEC 62443-4-2		72
Table A.7 – ISO/IEC 27001:2013 cross-references		73
Table A.8 – Cross-reference of IEC 62443-2-1 to ISO/IEC 27001:2013.....		75
Table A.9 – NIST CSF cross-references		77
Table A.10 – Cross-reference of IEC 62443-2-1 to NIST CSF		79
Table B.1 – Example risk levels		83

INTERNATIONAL ELECTROTECHNICAL COMMISSION

SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –**Part 2-1: Security program requirements for IACS asset owners**

FOREWORD

- 1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as “IEC Publication(s)”). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
- 2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
- 3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
- 4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
- 5) IEC itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
- 6) All users should ensure that they have the latest edition of this publication.
- 7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
- 8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
- 9) IEC draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). IEC takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, IEC had not received notice of (a) patent(s), which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at <https://patents.iec.ch>. IEC shall not be held responsible for identifying any or all such patent rights.

IEC 62443-2-1 has been prepared by IEC technical committee 65: Industrial process measurement, control and automation, in collaboration with the liaison ISA99: ISA committee on Security for industrial automation and control systems. It is an International Standard.

This second edition cancels and replaces the first edition published in 2010. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

- a) revised requirement structure into SP elements (SPEs),
- b) revised requirements to eliminate duplication of an information security management system (ISMS), and
- c) defined a maturity model for evaluating requirements.

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

Draft	Report on voting
65/1044/FDIS	65/1053/RVD

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

The language used for the development of this International Standard is English.

This document was drafted in accordance with ISO/IEC Directives, Part 2, and developed in accordance with ISO/IEC Directives, Part 1 and ISO/IEC Directives, IEC Supplement, available at www.iec.ch/members_experts/refdocs. The main document types developed by IEC are described in greater detail at www.iec.ch/publications.

A list of all parts in the IEC 62443 series, published under the general title *Security for industrial automation and control systems*, can be found on the IEC website.

Future standards in this series will carry the new general title as cited above. Titles of existing standards in this series will be updated at the time of the next edition.

The committee has decided that the contents of this document will remain unchanged until the stability date indicated on the IEC website under webstore.iec.ch in the data related to the specific document. At this date, the document will be

- reconfirmed,
- withdrawn, or
- revised.

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

INTRODUCTION

This document is the part of the IEC 62443 series that contains security requirements for industrial automation and control system (IACS) asset owners. In the context of this document, asset owner also includes the operator of the IACS. Its requirements focus on cybersecurity and allow security capabilities that meet them to be provided as a combination of technical, physical, process and compensating security measures.

Cybersecurity is an increasingly important topic in modern organizations. The term cybersecurity is generally used to describe the set of security measures or practices taken to protect a computer or computer system against unauthorized access or attack. In IACS, the most significant concerns include unwanted access or attacks resulting in the IACS not performing the correct functions in the required timeframe.

A very common engineering approach when faced with a challenging problem is to break the problem into smaller pieces and address each piece in a disciplined manner. This approach is a sound one for addressing cybersecurity risks with IACS. However, a frequent mistake is to deal with cybersecurity one system at a time. Cybersecurity is a much larger challenge that should address all IACS components as well as the policies, procedures, practices and personnel that surround and utilize those IACS. Implementing such a wide-ranging management system can require a cultural change within the organization.

Addressing cybersecurity on an organization-wide basis can seem like a daunting task. There is no simple cookbook for security, nor is there a one-size-fits-all set of security practices. Absolute security can be achievable but is probably undesirable because of the loss of functionality that would be necessary to achieve this near perfect state. Security is a balance of risk versus cost.

Each situation will be different. In some situations, the risk can be related to health, safety and environmental (HSE) factors rather than purely economic impact. The risk can have an unrecoverable consequence rather than a temporary financial setback. Therefore, a predetermined set of mandatory security practices can either be overly restrictive and likely quite costly to implement or be insufficient to address the risk.

This document supports the need to address cybersecurity for an IACS in operation by providing requirements for establishing, implementing, maintaining and continually improving an IACS security program (SP). These requirements, when implemented conscientiously, provide security capabilities whose purpose is to reduce IACS security risks to a tolerable level. These requirements are written to be implementation independent, allowing asset owners to select approaches most suitable to their needs. IEC 62443-3-2 [1]¹ describes the methodology for addressing cybersecurity risks in an IACS system design and that assists in the identification of risks and the selection of appropriate security requirements and associated capabilities for an IACS SP.

Commercial-off-the-shelf (COTS) products are often not ruggedized or rigorously engineered enough for IACS environments, where they can introduce additional vulnerabilities and threats to the IACS.

¹ Numbers in square brackets refer to the Bibliography.

When COTS technologies are used in an IACS, they are often configured to meet IACS specific functional needs and operational constraints. For example, security event handling in COTS products may be configured differently for IACS applications than they are for traditional information technology (IT) applications. Typical COTS equipment is designed for environments where the primary objective is the protection of information. In an IACS environment, the primary objectives are the protection of the HSE of the facility and the minimization of the operational and business impact on facility operation. COTS technologies can be applied to IACS applications, but the risks associated with using these technologies need to be understood by the asset owner.

Some organizations can attempt to use pre-existing IT and business cybersecurity solutions to address security for IACS without understanding the consequences. While many of these solutions can be applied to IACS, it is important to apply them correctly to eliminate inadvertent and undesired consequences. For example, in an IACS, availability may have a higher priority than confidentiality, as opposed to typical IT applications.

Asset owners may wish to apply their IACS SP across the organization to address the organization needs and objectives, security requirements, business and work processes, as well as the organization size and structure. All of these influencing factors are dynamic and will likely change over time. Thus, the adoption of an IACS SP is a strategic decision for the organization.

The effectiveness of an IACS SP is often enhanced through coordination or integration with the organization's processes and overall information security management system (ISMS). For example, security can be added to the organization supply chain processes to require security in the design of processes, systems and controls. It is also expected that IACS SP will be scaled in accordance with the needs of the IACS and the organization.

SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –

Part 2-1: Security program requirements for IACS asset owners

1 Scope

This part of IEC 62443 specifies asset owner security program (SP) policy and procedure requirements for an industrial automation and control system (IACS) in operation. This document uses the broad definition and scope of what constitutes an IACS as described in IEC TS 62443-1-1. In the context of this document, asset owner also includes the operator of the IACS.

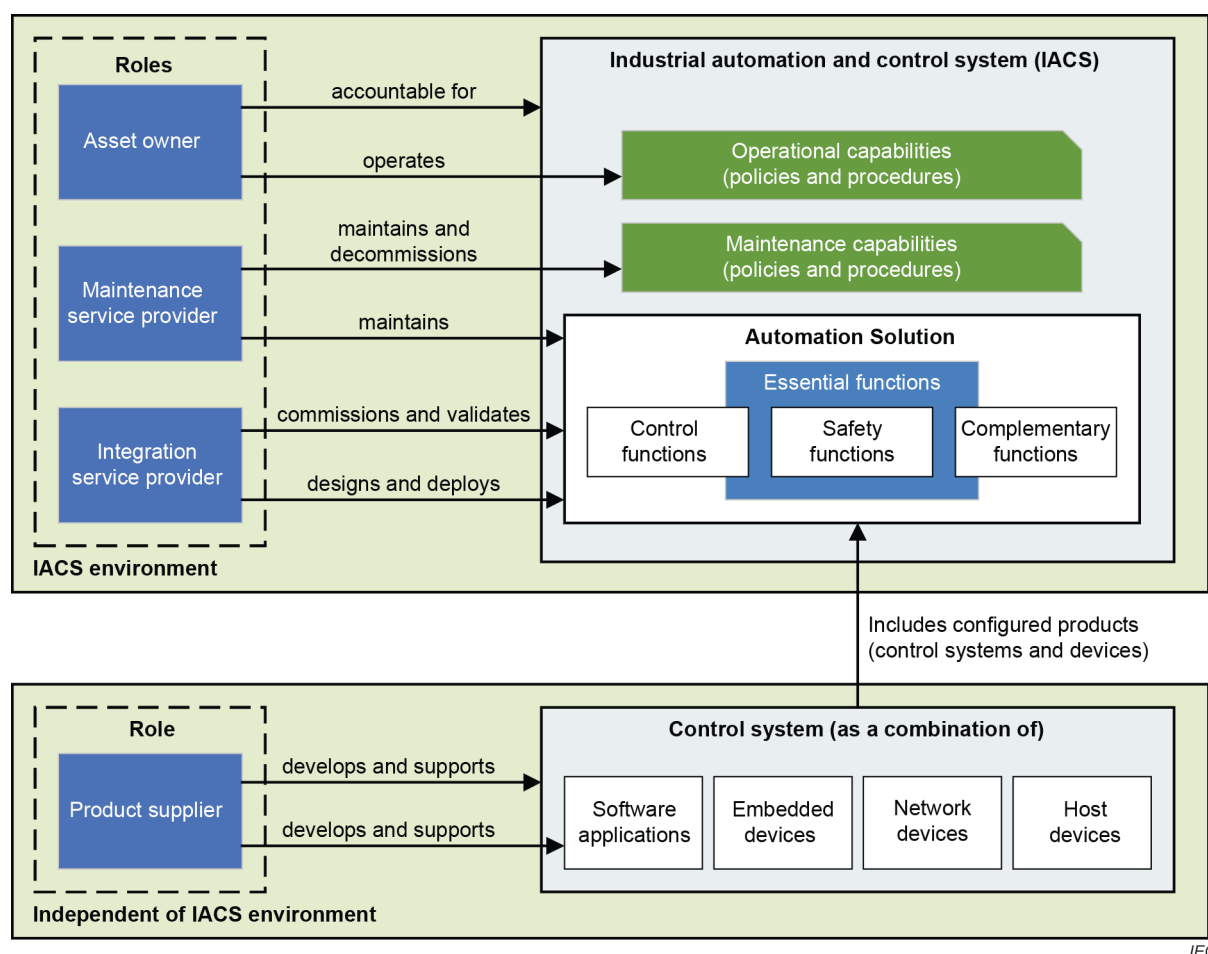
This document recognizes that the lifespan of an IACS can exceed twenty years, and that many legacy systems contain hardware and software that are no longer supported. Therefore, the SP for most legacy systems addresses only a subset of the requirements defined in this document. For example, if IACS or component software is no longer supported, security patching requirements cannot be met. Similarly, backup software for many older systems is not available for all components of the IACS. This document does not specify that an IACS has these technical requirements. This document states that the asset owner needs to have policies and procedures around these types of requirements. In the case where an asset owner has legacy systems that do not have the native technical capabilities, compensating security measures can be part of the policies and procedures specified in this document.

This document also recognizes that not all requirements specified in this document apply to all IACSs. For example, requirements associated with certain technology (such as wireless) or functions (such as remote access) will not apply to IACSs that do not include these technologies or functions. Similarly, not all malware protection requirements apply to systems for which malware protection software is not available for any of their devices. Therefore, this document states that the asset owner needs to identify the IACS security requirements that are applicable to its IACSs in their specific operating environments.

The elements of an IACS SP described in this document define required security capabilities that apply to the secure operation of an IACS. Although the asset owner is ultimately accountable for the secure operation of an IACS, implementation of these security capabilities often includes support from its service providers and product suppliers. For this reason, this document provides guidance for an asset owner when stating security requirements for their service providers and product suppliers, referencing other parts of the IEC 62443 series.

Figure 1 illustrates the roles and responsibilities of the asset owner, service provider(s) and product supplier(s) of an IACS and their relationships to each other and to the Automation Solution. The Automation Solution is a technical solution implementing the control/safety and complementary functions necessary for the IACS. It is composed of hardware and software components that have been installed and configured to operate in the IACS. The IACS is a combination of the Automation Solution and the organizational measures necessary for its design, deployment, operation and maintenance.

Some of these capabilities rely on the appropriate application of integration maintenance capabilities defined in IEC 62443-2-4 [2] and technical security capabilities defined in IEC 62443-3-3 [3] and IEC 62443-4-2 [4].



IEC

Figure 1 – Roles and responsibilities in the IEC 62443 series

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

3 Terms, definitions, abbreviated terms and conventions

3.1 Terms and definitions

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

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at <https://www.electropedia.org/>
- ISO Online browsing platform: available at <https://www.iso.org/obp>

3.1.1

access right

permission to access system resources or privilege to execute system functions

Note 1 to entry: Permissions are generally rights to access resources such as data and executable files, while privileges are generally rights to execute function calls provided by the operating system (OS).

3.1.2

asset owner

organizational role ultimately accountable for one or more IACS

Note 1 to entry: Used in place of the generic word end user to provide differentiation.

Note 2 to entry: In the context of this document, asset owner also includes the operator of the IACS.

[SOURCE IEC 62443-3-3:2013, 3.1.2, modified – Changed in definition "individual or company responsible" into "organizational role ultimately accountable" to reflect role; in Note 1 to entry changed "The term "asset owner" is used" into "Used"; removed Note 2 to entry; in Note 3 to entry changed "this standard, an asset owner" into "this document, asset owner".]

3.1.3

Automation Solution

control system and any complementary hardware and software components that have been installed and configured to operate in an IACS

Note 1 to entry: Automation Solution is used as a proper noun in this document.

Note 2 to entry: The difference between the control system and the Automation Solution is that the control system is incorporated into the Automation Solution design (for example, a specific number of workstations, controllers and devices in a specific configuration), which is then implemented. The resulting configuration is referred to as the Automation Solution.

Note 3 to entry: The Automation Solution can be comprised of components from multiple suppliers, including the product supplier of the control system.

3.1.4

compensating security measure

security measure employed in lieu of or in addition to inherent security capabilities to satisfy one or more security requirements

EXAMPLE 1 (Component-level) A locked cabinet around a controller that does not have sufficient cyber access control security measures.

EXAMPLE 2 (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.

EXAMPLE 3 (Component-level) A product supplier's programmable logic controller (PLC) cannot meet the access control capabilities from an asset owner, so the product supplier puts a firewall in front of the PLC and sells it as a system.

3.1.5

consultant

subcontractor that provides expert advice or guidance to their clients, such as product suppliers, integration and maintenance service providers and asset owners

3.1.6

device

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

EXAMPLES Controllers, human-machine interfaces (HMIs), PLCs, remote terminal units (RTUs), transmitters, actuators, valves, network switches, etc.

3.1.7**maturity level**

qualitative method of characterizing the capability of an organization to implement security requirements according to documented policies and procedures and their historical performance in doing so

3.1.8**portable media**

portable devices that contain data storage capabilities that can be used to physically copy data from one piece of equipment and transfer it to another

Note 1 to entry: Types of portable media include but are not limited to, compact disc (CD) / digital versatile disc (DVD) / Blu-ray media, universal serial bus (USB) memory devices, smart phones, flash memory, solid state disks, hard drives, handhelds and portable computers.

Note 2 to entry: The term "removable media" is another term that is often used for "portable media".

3.1.9**product supplier**

organizational role responsible for the manufacture and support of IACS hardware and/or software products

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

3.1.10**security capability**

technology or procedural measure, feature or mechanism that can be used to provide protection against cyber and physical security attacks

Note 1 to entry: Security capabilities are typically implemented through some combination of technology and procedural means. The term "countermeasure" is often used to describe the implementation of "security capability".

Note 2 to entry: The term "control" is also used to describe this concept in some contexts. The term "security capability" has been chosen for this document to avoid confusion with the word "control" in the context of "process control".

3.1.11**security compromise**

violation of the security of a system such that an unauthorized (1) disclosure or modification of information, (2) action/execution of functions or (3) denial of service (DoS) could possibly have occurred

Note 1 to entry: A security compromise represents a breach of the security of a system or an infraction of its security policies. It is independent of impact or potential impact to the system.

[SOURCE IEC 62443-2-4:2023, 3.1.20, modified – Changed in definition "(2) denial of service could possibly have occurred" into "(2) action/execution of functions or (3) denial of service (DoS) could possibly have occurred".]

3.1.12**security incident**

security compromise that is of some significance to the asset owner or failed attempt to compromise the system whose result could have been of some significance to the asset owner

Note 1 to entry: The term "of some significance" is relative to the environment in which the security compromise is detected. For example, the same compromise can be declared as a security incident in one environment and not in another. Triage activities are often used by asset owners to evaluate security compromises and identify those that are significant enough to be considered incidents.

Note 2 to entry: In some environments, failed attempts to compromise the system, such as failed login attempts, are considered significant enough to be classified as security incidents.

[SOURCE IEC 62443-2-4:2023, 3.1.21]

3.1.13 **security management system** **SMS**

set of interrelated or interacting elements of an organization to establish security policies and objectives and a set of systematic processes to achieve those objectives

Note 1 to entry: This definition is based on the ISO/IEC 27000:2018, 3.41 [5] definition of "management system" and its description.

3.1.14 **security patch**

incremental software change in order to address a security vulnerability, a bug, reliability or operability issue (update) or add a new feature (upgrade)

Note 1 to entry: For the purpose of this definition, firmware is considered software.

Note 2 to entry: Software patches can address known or potential vulnerabilities, or simply improve the security of the software component, including its reliable operation.

3.1.15 **security program** **SP**

portfolio of security services, including integration services and maintenance services, and their associated policies, procedures and products that are applicable to the IACS

Note 1 to entry: The SP for IACS asset owners refers to the policies and procedures defined by them to address cybersecurity concerns of the IACS. This can include technical, process, physical and compensating security measures used to reduce the cybersecurity attack surface.

[SOURCE IEC 62443-2-4:2023, 3.1.23, modified – Added SP; in Note 1 to entry replaced "security program" with SP, replaced "service providers" with "asset owners" and added "This can include technical, process, physical and compensating security measures used to reduce the cybersecurity attack surface."]

3.1.16 **service provider**

organizational role responsible for providing services and associated supplies for the IACS in accordance with an agreement with the asset owner

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

3.1.17 **software service**

software program that is installed and managed by infrastructure software instead of by or on behalf of a logged-on user, typically without a user interface of its own

Note 1 to entry: Some OSs allow logged-on users with elevated privileges to start/stop software services.

3.1.18 **tolerable risk**

level of risk deemed acceptable to an organization

Note 1 to entry: Organizations should include consideration of legal requirements when establishing tolerable risk. Additional guidance on establishing tolerable risk can be found in ISO 31000 [6] and NIST SP 800-39 [7].

Note 2 to entry: IEC 62443-3-2 provides guidance for establishing tolerable risk.

[SOURCE IEC 62443-3-2:2020, 3.1.22, modified – Added Note 2 to entry.]

3.2 Abbreviated terms and acronyms

This subclause defines the abbreviated terms and acronyms used in this document.

ANIMA	autonomic network integrated model and approach ²
ANSI	American National Standards Institute
API	application programming interface
BCP	business continuity plan
BOOTP	bootstrap protocol
BRSKI	bootstrapping of a remote secure key infrastructure ²
C2M2	cybersecurity capability maturity model ³
CD	compact disc
CDA	critical digital asset
CSF	cybersecurity framework ⁴
CIS	center for Internet security
CMMI	capability maturity model integration
CMMI-SVC	CMMI for services
CONOPS	concept of operations
COTS	commercial-off-the-shelf
DA	digital asset
DES	data encryption standard
DHCP	dynamic host configuration protocol
DMZ	demilitarized zone
DOD	Department of Defense ⁵
DOE	Department of Energy ⁵
DoS	denial of service
DRP	disaster recovery plan
DVD	digital versatile disc
EAP	Extensible Authentication Protocol ²
GPS	global positioning system
HMI	human-machine interface
HSE	health, safety and environment
IACS	industrial automation and control system(s)
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IIS	Internet information services ⁶

² IETF

³ US DOE

⁴ NIST

⁵ US

⁶ Microsoft®. This trade name is provided for reasons of public interest or public safety. This information is given for the convenience of users of this document and does not constitute an endorsement by IEC.

IP	Internet protocol
ISA	International Society of Automation
ISMS	information security management system
ISO	International Organization for Standardization
IT	information technology
MFA	multifactor authentication
ML	maturity level
NIST	National Institute of Standards and Technology ⁵
NTP	network time protocol
OPC	open platform communications
OS	operating system
PII	personally identifiable information
PIN	personal identification number
PLC	programmable logic controller
RBAC	role-based access control
RF	radio frequency
RFC	request for comment ²
RFQ	request for quote
RTU	remote terminal unit
SI	international system of units
SL	security level
SL-T	target SL
SP	security program
SPE	SP elements
SPR	security protection rating
SPS	security protection scheme
SSID	service set identifier
TCP	transmission control protocol
UAC	user account control ⁶
UDP	user datagram protocol
USB	universal serial bus
VPN	virtual private network

3.3 Conventions

A requirement without qualifier is the same as that requirement with a BR (Basic Requirement) qualifier; for example, ORG 1.1 and ORG 1.1 BR are the same requirement.

A requirement with a leading 0 in its numerical fields is the same as that requirement without a leading 0 in its numerical fields; for example, SR 2.03 and SR 2.3 are the same requirement.

The above conventions accommodate the different ways the requirements are specified in other IEC 62443 parts.

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

4 Concepts

4.1 Use of this document

4.1.1 Applicable roles

This document primarily applies to the asset owner role, and to a lesser degree, to service provider and product supplier roles (see Figure 1). Organizations who are accountable for the IACS are considered asset owners by the IEC 62443 series. Organizations responsible for the development and support of the hardware and software used in IACS fulfil the product supplier role. Organizations that provide integration services for the IACS fulfil the integration service provider role, while those that provide maintenance services fulfil the maintenance service provider role. These roles and responsibilities are depicted in Figure 1.

It is not uncommon for the organization acting as the asset owner to perform some or all aspects of the integration or maintenance service provider roles, and also perform some or all aspects of the product supplier role for some components of the IACS. In these cases, Subclauses 4.1.2 and 4.1.3 will apply to the asset owner organization.

In other cases, the asset owner may contract with one or more product suppliers and/or service providers to deploy and maintain the IACS. In these cases, these organizations may act as one or more of the integration service providers, maintenance service provider or product supplier roles.

Similarly, part or all of a facility may be operated by an entity other than the asset owner. In all cases, the requirements specified by this document apply to the asset owner. The asset owner may have a supply chain program that contains security requirements derived from this document for product suppliers and service providers.

4.1.2 Use of this document by asset owners

4.1.2.1 Risk mitigation

This document defines requirements for IACS SPs of asset owners. In general, a SP consists of defining, implementing and maintaining process, personnel and technology-based capabilities that are intended to reduce the cybersecurity risk of an IACS.

The primary purpose for each of the SP requirements in this document is to mitigate risk. However, risk reduction can take many forms, such as reduction of the likelihood of an incident, reduction of the impact of an incident, reducing the timeline to recover from an incident, and others. In many cases, an SP requirement reduces the overall risk in multiple ways.

The requirements are specified in an implementation independent manner, allowing a variety of implementations, and allowing users of this document to select a combination of architectural approaches (for example, the use of security zones), policies, procedures and technologies that are most appropriate for their applications.

IEC 62443-3-2 [1], describes a methodology for addressing cybersecurity risks in an IACS Automation Solution design, including the use of security levels (SLs) and security zones.

An IACS SP is typically specific to an individual IACS, of which the facility can have more than one. When there is more than one, it is recommended that a single high-level, facility-level SP be defined whose requirements cascade down as needed to individual IACS SPs. Each IACS SP is dedicated to the availability, integrity and confidentiality of the specific production resources of its IACS, including controllers, field devices and other embedded devices, as well as protecting trade secrets and other confidential information of the IACS.

An IACS SP should be compatible with other IACS SPs at the facility, but this is not always practical or achievable since the technology and risks associated with one IACS can be significantly different than those of another IACS.

IACS SPs are also expected to supplement an asset owner organization's information security management system (ISMS) to provide coordinated operational and information security for the site. ISMS requirements generally do not specifically address all of the security and operational needs of an IACS. This document, along with related parts of IEC 62443 series, define the requirements needed to ensure the operational and informational security of an IACS throughout its lifecycle.

Where practical, IACS SPs should be compatible with the organization's ISMS, but complete consistency with the ISMS is typically not possible due to conflicting objectives of information technology (IT) and IACS systems, and in particular, the essential constraints associated with availability and performance of production facilities. In addition, some of the informational security requirements that apply to protection of the IACS IT aspects can be implemented differently for the IT system and an IACS.

NOTE Alignment of the ISMSs and IACS SPs can be improved by alignment of security goals and objectives between the two systems, and by formally documenting their similarities and differences.

For example, patching policies can be different between IACS SPs and ISMSs as a result of the differences in availability requirements between IACS operator stations and ISMS desktop workstations. Operational constraints, such as this, will typically result in different sets of policies and procedures for IACS SPs and ISMSs.

Since IACSs are a combination of personnel, hardware and software, and processes, SPs of asset owners compliant with this document are composed of:

- a) organizational capabilities that:
 - 1) include an ISMS that typically defines organization-wide policies and practices for IT systems, and
 - 2) support coordination between the IACS and the IT infrastructure in its environment,
- b) technical security capabilities implemented in hardware and software components of the Automation Solution of the IACS (see Figure 1), and
- c) security-related processes, used to securely deploy, configure and operate the IACS, and to maintain its technical security capabilities.

4.1.2.2 SP implementation

This document provides IACS asset owners with a framework to develop and evolve their SPs. Implementing an effective SP for an IACS involves defining and executing comprehensive capabilities that:

- a) address all aspects of security risk management, from identification of programmatic objectives to day-to-day operation, and
- b) include ongoing auditing for program compliance and improvement.

Organizational commitment from top to bottom is essential for IACS SP success. Security of an IACS is a responsibility shared by all members of the organization and their contractors/consultants, and integration of security into their daily activities allows the organization to function more smoothly and succeed in protecting the IACS. SPs based on this document are expected to vary widely depending upon the asset owner's organization and industry. Application of this document to an asset owner's SP begins with determining which of the requirements defined in this document are applicable. Requirements are often determined to be applicable based on the architecture and characteristics of the IACS, the environment in which the IACS operates and the security risks associated with it (see Annex B and IEC 62443-3-2 for more information on management of IACS security risks).

For each applicable requirement, asset owners should implement the appropriate combination of technical and process-oriented capabilities. Technical capabilities are features of the IACS and its components, and process-oriented capabilities are organizational processes used to integrate/deploy the IACS, operate it and maintain it.

Cross-references are provided to IEC 62443-3-3 and IEC 62443-4-2 for technical capabilities and to IEC 62443-2-4 for integration and maintenance capabilities. These cross-referenced capabilities can be used by asset owners when determining the technical and process-oriented capabilities they will implement and for specifying security requirements for their product suppliers and service providers.

It could be impossible or impractical for an asset owner to establish and implement a SP that meets all applicable requirements at once. Therefore, asset owners may, if necessary, develop a phased approach to evolve their SP. In such cases, the initial emphasis should be on effectively managing the highest risks.

This document also recognizes that it can be desirable for asset owners to implement a SP that meets the requirements specified in this document in ways that are consistent with other security specifications. Therefore, Annex A reports cross-references to and from each requirement of this document with requirements in related external references, in particular with ISO/IEC 27001 [8] and the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) [9]. Using these cross-references, the asset owner can harmonize with related external requirements when implementing each of its SP capabilities.

NOTE In the context of an IACS, all references in ISO/IEC 27001 to "information management" refer to the IACS.

Some legacy IACS can preclude direct implementation of specific requirements or subsets of applicable requirements. In these instances, compensating security measures should be implemented where possible.

4.1.2.3 Organizational interfaces

Although the asset owner is ultimately accountable for the operation of the IACS and processes controlled by the IACS, associated responsibilities are often fulfilled with the support of service providers and product suppliers. The respective legal, operational and technical roles and responsibilities for these entities are generally defined in contracts and procurement documents, such as request for quotes (RFQs) and purchase orders. Ideally, security requirements are included in these documents.

When the service provider or product supplier is part of the asset owner's organization, there might not be such a contract, but the security requirements for products and integration/maintenance processes are typically still specified for the IACS.

This document provides in Annex A cross-references to and from each requirement of this document with service provider and product supplier requirements specified in IEC 62443-2-4, IEC 62443-3-3 and IEC 62443-4-2. Asset owners can use these cross-references to assist in the development of security requirements for service provider and product supplier procurement documents. These referenced documents and the requirements cross-references included in Annex A of this document can assist asset owners, service providers and product suppliers to agree on a consistent set of requirements during procurement.

4.1.3 Use of this document by service providers and product suppliers

As described in 4.1.2.3, IEC 62443-2-4, IEC 62443-3-3 and IEC 62443-4-2 define security requirements for products and services procured by asset owners. Since these requirements are cross-referenced to this document's requirements in Annex A, this document can provide a useful context to service providers and product suppliers.

4.2 Maturity level (ML) definitions

The SP requirements defined in this document beginning in 5.3 have been specified to be implementation independent. This is done to allow the asset owner latitude in applying this document while meeting the needs of its organization.

To support implementation independence for process security measures that meet these requirements, a range of MLs from entry level processes to refined and improved processes is defined in Table 1. MLs apply independently to SP requirements, and the asset owner should select the most appropriate ML for a requirement based on risk management goals (see IEC 62443-3-2). While the asset owner can have policies and procedures that satisfy multiple SP requirements, each SP requirement should be evaluated independently. See Annex C for more information about evaluating MLs.

Additionally, since some asset owners could need to use a phased approach to evolve their SPs, a range of program MLs can prove helpful in the planning and scheduling of phases. Note that other parts of IEC 62443 that define requirements for process security measures, such as IEC 62443-2-4 and IEC 62443-4-1 [10], also incorporate ML.

This document's range of MLs is defined by a model that is composed of maturity benchmarks for implementation of process security measures. The benchmarks for each ML are shown in Table 1. The MLs are based on the Capability Maturity Model Integration (CMMI) for Services (CMMI-SVC) model [11]. Table 1 shows the relationship to the CMMI-SVC in the "Description/comparison to CMMI-SVC" column.

Table 1 – ML levels and descriptions

Level	CMMI-SVC	This document	Description/comparison to CMMI-SVC
1	Initial	Initial	At this level, the models are fundamentally the same. Processes are performed in an ad-hoc and often undocumented (or not fully documented) manner. As a result, consistency over time can be difficult to show. NOTE "Documented" in this context refers to the procedure followed in performing this service (for example, detailed instructions to service provider personnel), not to the results of performing the process. In most IACS, changes resulting from the performance of a procedural process are often documented.
2	Managed	Managed	At this level, the models are fundamentally the same, with the exception that this document recognizes that there can be a significant delay between defining a process and executing/practicing it. Therefore, the execution related aspects of the CMMI-SVC Level 2 are deferred to Level 3. At this level, documentation exists that describes how to manage the delivery and performance of the capability. This documentation can be in the form of written procedures or written training programs for performing the capability. The discipline reflected by ML 2 helps to ensure that practices are repeatable, even during times of stress. When these practices are in place, their execution will be performed and managed according to their documented plans.
3	Defined	Defined / Practiced	At this level, the models are fundamentally the same, with the exception that the execution related aspects of the CMMI-SVC Level 2 are included here. Therefore, a process at Level 3 is a Level 2 process that is being practiced on the IACS. The performance of a Level 3 practice can be shown to be repeatable over time within the IACS.

Level	CMMI-SVC	This document	Description/comparison to CMMI-SVC
4	Quantitatively Managed	Improving	At this level, the "Quantitatively Managed" and "Optimizing" CMMI-SVC levels are combined. Using suitable process metrics, the effectiveness or performance improvements of the process or both can be demonstrated. This results in a SP that improves the process through technological/procedural/management changes.
	Optimizing		

Beginning with ML 2, processes are required to be documented. This includes documented policies and procedures as well as documented training for personnel. As a consequence, the SP requirements specified in this document do not state the need for documentation because the ML 2 and above require documentation.

Within this maturity model, each level is progressively more advanced than the previous level and applies independently for each requirement. MLs are a part of the conformance assessment process, so asset owners are required to identify whether they meet each requirement, and if so, the ML associated with their implementation of each requirement or group of requirements.

NOTE It is intended for evolution of a SP, that over time and for a specific requirement, a process will evolve to higher levels as the organization gains proficiency in meeting the requirement.

4.3 Security levels (SLs)

SLs for IACS represent the relative strength of security capabilities defined for the IACS Automation Solution in IEC 62443-3-3 and for components in IEC 62443-4-2.

This document does not describe the methodologies for defining zones and conduits, or determining SLs for zones, conduits and components. Instead, those methodologies are defined in IEC 62443-3-2 for zones and conduits, and IEC 62443-4-2 for components. This document defines the requirements for the overall SP within the organization to manage risk on an ongoing basis, via implementing and maintaining process, personnel and technology-based capabilities.

To correlate SP requirements in this document with target SLs (SL-Ts) for zones, conduits and components, the asset owner can use the cross-references to IEC 62443-3-3 and IEC 62443-4-2 that are provided with the SP requirement to understand the requirements/requirements enhancements associated with the SL-T from those documents.

For example, this document can state a SP should have a process to ensure proper authentication is ensured across the organization. However, to address confidence in the implementation of user authentication capabilities, the asset owner should request its product suppliers to show the product in question was developed using IEC 62443-4-1 compliant processes, and the product capabilities are compliant with relevant IEC 62443-4-2 requirements. Similarly, to address confidence in the installation, configuration and maintenance of these user authentication capabilities, the asset owner would request its service providers to use processes for these capabilities that are compliant to the cross-referenced IEC 62443-2-4 requirement, SP.03.07 RE(1).

4.4 Requirements definitions

4.4.1 Requirements organization

Subclause 5.3 and Clauses 6 through 13 define the selection methodology and individual requirements for asset owner SPs. These requirements have been specified to be implementation independent, allowing the asset owner to select the most suitable implementation for its IACS.

Requirements are organized into SPEs that represent top level activities of the SP, such as organizational security measures, configuration management, network and communications security and component security. SPEs are composed of requirements for a combination of organizational and technical security controls that can be used to implement a defense-in-depth strategy for the IACS.

4.4.2 Requirements cross-references

To aid the asset owner's use of this document, the requirements have been cross-referenced to other parts of the IEC 62443 series and other security specifications that include system and component requirements. This cross-reference is provided to support activities spanning documents in the series, such as the integration of the asset owner's SP with its ISMS and with its supply chain processes as they relate to security.

These cross-references support asset owner efforts to implement the requirements of this document consistently with the other parts of the IEC 62443 series and with the other referenced specifications. Blank entries in these cross-references mean that there is no corresponding requirement in the cross-referenced document. These cross-references are reported in Annex A.

4.4.3 Requirement conventions

Some of the requirement's definitions contain the phrase: "commonly accepted". This phrase is used when the required capability implementation is dependent on the current state of the art, and the state of the art at the time of conformance assessment is used to determine whether the requirement has been met. For example, when the Data Encryption Standard (DES) was developed, it had no known vulnerabilities, but since then vulnerabilities have been discovered and it is no longer appropriate for use in IACSs. The "Rationale and supplemental guidance" subclause of each requirement provides additional explanation of the use of this phrase.

5 Conformance and assessment

5.1 Overview

The formal definitions for terms like conformance, conformity and assessment come from other sources, such as ISO/IEC 17000 [12]. IEC 62443 series provides guidance for conformity and assessments for various roles (see 4.1.1). This guidance is intended to assist the various roles in understanding the conformance and assessment process and is not intended to supersede any of the definitions provided in ISO/IEC 17000.

Conformance or conformity with IEC 62443 series means the affected role has evaluated, and where applicable applied and documented, all methods identified in each requirement of the applicable series part thereby mitigating security risks and identifying the conformity for all identified processes with the necessary supporting evidence.

Assessment means the affected role has performed specific measurement of conformity with the requirements through use of some type of verification process or specific validation process. Those validated processes can be applied through an internal organization process or the use of a third-party identified process compliant with the IEC 62443 series, and also are verified by supplying the necessary supporting evidence.

Conformity assessments can be self-assessments performed by the asset owner, service provider or product supplier roles using internal processes, or assessments can be performed by a qualified, independent third-party. When independent third-party assessments are used, it is important to note that credentialing processes of the third-party are wide and varied and are outside the scope of this document,

Assessment processes themselves are also outside the scope of this document.

Asset owners may have their "as-deployed" control systems, IACS or Automation Solutions assessed for conformance to IEC 62443-3-3 and their "as-provided" integration and maintenance services assessed for conformance to IEC 62443-2-4. These assessments would verify conformance at the time the control system was assessed, or the services were provided. Supplementing these assessments are evaluations that combine security levels and organizational MLs to indicate the composite SP protection provided to the IACS.

Asset owners may assess their IACS and Automation Solutions for conformance to this document, to verify they have a SP in place to sustain a security posture for the IACS which includes all technical components and organizational processes. It is also desirable for the IACS or Automation Solution to use security certified products in the design that are correctly deployed and maintained by certified service providers.

Product suppliers providing products to an asset owner may have their products and development processes assessed for conformance to IEC 62443-3-3, IEC 62443-4-1 and IEC 62443-4-2.

Service providers providing services to an asset owner may have their integration and maintenance services assessed for conformance to IEC 62443-2-4.

5.2 Conformity evidence

Proof of conformity and conformance methods can be provided in many forms as shown in Table 2. Most requirements identify supporting evidence by identifying the specific methods that include, but are not limited to:

- verifying the use,
- capability and configuration of technology,
- their supporting processes, and
- validation through testing of capabilities.

Table 2 – Typical conformity evidence types

Evidence type	Description
Configuration records	Records that show configuration settings, component inventories, patch records, etc.
Legal documents	Contracts and related documents, including subcontractor agreements, signed employee statements, background checks, asset owner approvals, etc.
Organization charts, position descriptions and personnel records	Job related documentation that describes customer roles, including personnel requirements (for example, expertise/experience), job responsibilities and organizational relationships. Also, records that show who was assigned/de-assigned to these positions (for example, to Automation Solution activities).
Product documentation	Internal and external documents that describe the product, such as design documents, product data sheets, knowledge-based articles and network scanning tools.
Screen shots	Screen captures of user interfaces.
Security assessments	Reports that document security-related issues, such as risks, security incidents and vulnerabilities.
Security testing documentation	Internal and external documents that describe the security tests/results used to verify security aspects of the product or installation of the product.
Service policies and procedures	Internal customer documentation that describes policies and procedures used by customer personnel to install, configure, harden and maintain the Automation Solution.
Security-related activity documentation/checklists	Documentation, such as checklists, that records the results of security-related activities, such as risk assessments, threat models, reviews, architecture drawings, test results, spreadsheets, etc.
Automated reports	Reports generated by the IACS.

Evidence type	Description
Training materials/course descriptions	Documents that describe how training is conducted and documents that show the content of the training course, such as a syllabus or course overview.
Training records	Documents that show completion of training. These documents typically show who was trained, when they were trained and the course names. These can take the form of course rosters, course diplomas, human resource records, etc.
User documentation	User manuals, instructions, etc. that describe to the user how to configure, operate, maintain or otherwise interact with the IACS and its products and services.
Testing results	Any and all tests, performed by a qualified person having the appropriate training, on a documented configuration of components, IACS and Automation Solution that verify specifically identified requirements conformance.

5.3 Requirements evaluation and profiles

5.3.1 Overview

In preparation for a conformance assessment, asset owners need to evaluate each requirement in an applicable part of the series for its guidance in mitigating the risk addressed by the requirement.

In the event a role determines through evaluation any requirement may not apply, it is the asset owner's responsibility to justify why a requirement does not apply and provide supporting evidence stating specifically why the requirement does not apply including specifically how that security risk has been otherwise mitigated through other security measures.

5.3.2 Evaluation of risk to requirements

The determination of the cybersecurity risks to be mitigated (see 4.1.2.1 and 6.3.1, ORG 2.1: Security risk mitigation) is typically performed as part of the asset owner's risk management process in IEC 62443-3-2. This process should incorporate "risk response" activities as described in IEC TS 62443-1-1 and IEC 62443-3-2, which are responsible for identifying and dispositioning risks. Completing the risk management process in IEC 62443-3-2 is critical to the security of the IACS even if a conformance assessment is not performed.

Requirements then are applied based on risk mitigation and apply to all circumstances where identified risks need to be mitigated to a tolerable level, and conversely, if requirements may not apply where risks have evidence to prove the risk can be at a tolerable level.

Each requirement is selected based on risk mitigation and interpreted in the context of tolerable risk; that is, meeting the requirement means that the asset owner has either mitigated or accepted the risks associated with the requirement with supporting evidence.

If the asset owner is not prepared to accept the risks, then the requirement is not met.

5.3.3 Profiles

It can be necessary for some industries and verticals to align the requirements in this and other IEC 62443 documents to industry/vertical-specific concepts and terminology. In order to provide additional flexibility in the application of the standards series, IEC TS 62443-1-5 [13] describes a method for one or more organizations to create a common profile of IEC 62443 (all parts). A profile allows an interested party (organization, group, sector, conformity assessment body, etc.) to select a subset of requirements from one or more standards in IEC 62443 (all parts), provide a contextual mapping for those requirements (for example to an industry/vertical) and specify a minimum security or maturity level for selected requirements.

Published profiles can be used as a common basis of assessment against a subset or industry/vertical-specific mapping of the requirements in the IEC 62443 series. They support interested parties during conformity assessment activities, to achieve comparability of assessed IEC 62443 requirements.

5.3.4 Conformity assessment for the asset owner role

In preparation for a conformity assessment, asset owners can select the requirements that are to be assessed based on:

- a) a security profile to which the asset owner claims conformance; or
- b) the outcome of an IACS specific cyber security risk assessment and identification of applicable requirements necessary to reduce risks to a tolerable level.

A requirement might not be applicable because, for example, the IACS does not contain components/technology, such as wireless and safety systems addressed by the requirement.

Risk management is critical to the security of the IACS even if a conformity assessment is not performed.

6 SPE 1 – Organizational security measures

6.1 Purpose

The requirements in this SPE are defined to ensure that the organization is prepared to adequately address IACS security. It focuses on organizational policies and procedures for applying security practices and ensuring that its personnel are security aware and trained for their security responsibilities.

6.2 ORG 1 – Security related organization and policies

6.2.1 ORG 1.1: Information security management system (ISMS)

6.2.1.1 Requirement

If the asset owner has an ISMS, the asset owner shall coordinate the IACS SP with the ISMS. If the asset owner does not have an ISMS, the asset owner shall incorporate the appropriate management processes into the IACS SP.

6.2.1.2 Rationale and supplemental guidance

A formal ISMS is often employed by the asset owner organization to protect its IT system. When employed, the ISMS and the IACS SP should be coordinated to provide an integrated defense-in-depth strategy for the IACS, thereby avoiding duplication of effort and providing an efficient security interface between IT and IACS.

Requirements and recommendations for a formal ISMS can be found in ISO/IEC 27001 [8], ISO/IEC 27002 [14], the NIST CSF [9], NIST SP 800-53 [15], NIST SP 800-82 [16] as well as others. ISMS requirements and recommendations that are applicable to an IACS should be selected based on risk mitigation (see 4.1.2.1), and their implementation should be synchronized, to the greatest degree possible, with the ISMS to minimize differences and discord between the two.

Coordination between the IACS SP and the ISMS involves cooperation between security administrators, design and management of shared IACS network interfaces (for example, firewalls, demilitarized zones (DMZs) and remote access) and management of user access across those interfaces. The formal ISMS can be implemented for IT systems of the organization or for the IACS itself.

Areas of potential conflicts should be identified, examined and addressed, such as policies and practices for patch management (see also IEC TR 62443-2-3 [17]) and anti-malware updates, to prevent them from interfering with each other or opening vulnerabilities between the IACS and facility systems.

6.2.2 ORG 1.2: Background checks

6.2.2.1 Requirement

The asset owner shall have policies and procedures about performing background checks on all personnel who require access to the IACS (including employees, contractors, subcontractors, consultants, product suppliers and service providers) prior to granting them access to the IACS. Where feasible and allowed by applicable law, such background checks shall include identity verification and criminal records checks.

6.2.2.2 Rationale and supplemental guidance

Background checks are used to protect the IACS from being staffed with personnel whose integrity and trustworthiness can be questionable, including, but is not limited to, employees, contractors, subcontractors, consultants, products suppliers and service providers.

While the background check cannot guarantee these qualities, it can identify personnel who have had trouble with them. Examples of background checks include identity verification and criminal record checks.

This requirement recognizes that the ability to perform background checks is not always possible because of applicable laws or because of lack of support by local authorities, service organizations or both. Some countries prohibit background checks; while other countries do not. Of those that allow them, some provide no support for conducting them, making it infeasible or impractical for background checks to be performed.

When background checks are possible, the asset owner should have a policy for how and how often they are performed.

6.2.3 ORG 1.3: Security roles and responsibilities

6.2.3.1 Requirement

The asset owner shall have policies and procedures around defining and assigning security roles and responsibilities to qualified personnel, including employees, contractors, subcontractors and consultants.

6.2.3.2 Rationale and supplemental guidance

Security roles, such as security administrators, security leads and security contact points, are necessary to establish/maintain the security of the IACS. Further, the personnel in those roles need to be qualified to perform their security-related tasks to ensure that they are performed appropriately. The asset owner needs to define qualification requirements, which typically consist of varying levels of education, experience and training. Some things, like facility-specific technical training, are often provided by the asset owner and are not usually included in prior experience requirements.

The organization should determine the organizational processes required to establish/maintain the security of the IACS and identify the personnel who will be responsible for managing and implementing these processes. They should also determine a base level of expertise necessary to perform these tasks, and ensure the identified personnel have this expertise. Expertise can be demonstrated through related experience, training or both.

6.2.4 ORG 1.4: Security awareness training

6.2.4.1 Requirement

The asset owner shall have policies and procedures requiring all personnel (including employees, contractors, subcontractors, consultants, product suppliers and service providers) who interact with the IACS receive formal cybersecurity awareness training that is updated on a regular basis.

6.2.4.2 Rationale and supplemental guidance

Security awareness training is necessary to ensure personnel who have physical contact with or access to the IACS understand that their behaviour has the potential for impacting the security of the IACS. Maintaining security awareness is instrumental in establishing an organizational culture that recognizes that its personnel play an important role in the security of the IACS.

Physical contact with the IACS includes contact with IACS components (for example, displays and embedded devices), communications media, portable media, cabinets and all other equipment whose compromise can impact the IACS. Access to the IACS includes user interfaces, communications interfaces and local device interfaces through which access to the IACS can be gained.

Security awareness training is used to inform personnel of basic security principles that they are to apply to their daily behaviour. This training should be customized or related to the specific security policies and requirements of the IACS. Sources of these policies and requirements include this document and other parts of the IEC 62443 series that are applicable to the IACS. The asset owner should also have a policy that specifies how often its security awareness training program is to be reviewed to keep it current and relevant.

Regular review and update of training content and plans is necessary to respond to changes to the threat landscape, the vulnerability landscape and technology associated with the IACS.

6.2.5 ORG 1.5: Security responsibilities training

6.2.5.1 Requirement

The asset owner shall have policies and procedures requiring all personnel (including employees, contractors, subcontractors, consultants, product suppliers and service providers) who interact with the IACS receive formal cybersecurity training that is relevant to their IACS cybersecurity responsibilities. Such training shall either be accepted or provided by the asset owner.

6.2.5.2 Rationale and supplemental guidance

Security responsibility training serves two purposes:

- a) to ensure that personnel who are responsible for some aspect of the cybersecurity of the IACS understand what their responsibilities are and how their performance will be measured, and
- b) to ensure that they understand the processes and procedures necessary to meet those responsibilities.

NOTE Personnel to receive security training include, but are not limited to employees, contractors, subcontractors, consultants, product suppliers and service providers.

Security responsibility training will typically be provided to personnel on a recurring basis that includes the security objectives to be met along with related job performance criteria. It is important that each person understands what is expected in the meeting of his/her security responsibilities.

Security responsibility training should also describe how to meet security responsibilities. These descriptions can include classroom/online instructions, references to manuals or written policies and procedures. When training is completed, an individual should clearly understand his/her objectives and how their job performance will be evaluated with respect to his/her security responsibilities.

6.2.6 ORG 1.6: Supply chain security

6.2.6.1 Requirement

The asset owner shall have policies and procedures that specify requirements for suppliers of products and services addressing cybersecurity risks to the IACS. The asset owner policies and procedures shall consider recursive requirements on the suppliers, where feasible.

6.2.6.2 Rationale and supplemental guidance

IACSs are typically composed of products and services integrated and tested to work together. Each of these products and services is provided to the asset owner by an organization (which can include the asset owner) that is generally referred to as a supplier. Each supplier often has suppliers of its own, and each of these second level suppliers can have suppliers of their own. This cascading of suppliers is referred to as the supply chain.

To construct an effective supply chain process, the asset owner should identify each technical and process security measure incorporated into the IACS, and then define appropriate security requirements for those that are directly or indirectly provided by product suppliers or service providers. The objective is for products to have appropriate security measures built into them and for services to include appropriate security processes.

For a product or service to meet IACS security requirements, the supplier is responsible for ensuring that components and services of the product or service are themselves assessed for risk in the context of their use and should have security requirements specified for them. This process of risk determination and security requirement definition should occur recursively along the supply chain, thus creating a formal process for addressing security in the supply chain.

6.3 ORG 2 – Security assessments and reviews

6.3.1 ORG 2.1: Security risk mitigation

6.3.1.1 Requirement

The asset owner shall have policies and procedures around identifying, documenting, and mitigating or otherwise managing IACS cybersecurity risks, including determining a tolerable risk level and responding to risks outside that tolerable risk level.

6.3.1.2 Rationale and supplemental guidance

Security risks represent the potential for loss as a result of a security compromise. The higher the risk, the greater the potential for loss. Risk management involves understanding the IACS operational environment, identifying, assessing and quantifying risks within this environment, determining which risks cannot be tolerated by the organization and mitigating them to reduce their level of risk to a tolerable level. Risks that have been mitigated to a tolerable level means that the organization is willing to "live with" or is prepared to manage the mitigated risk. See IEC 62443-3-2 for more information about risk assessments and risk tolerance. See IEC 62443-3-3 for more information about applying technical security measures to mitigate the risks outside the tolerable risk level.

Risk mitigation involves developing attack scenarios, assessing and ranking associated potential consequences and implementing security measures in response to risks that are deemed intolerable. Security measures typically include a combination of architectural, technical mechanisms, vulnerability closures and process security measures. Risk mitigation also includes activities to ensure that risks are maintained at a tolerable level, such as periodic or event-driven (for example, changes in the threat landscape and discovery of new vulnerabilities) reassessments, internal or external audits that ensure technical and process security measures are in place and applied appropriately and conformity certifications to applicable cybersecurity standards.

The requirements in this document describe capabilities that, when appropriately implemented, provide security measures for the IACS. The asset owner should select requirements from this document that are applicable for the IACS and implement them accordingly. For those requirements not selected, the asset owner should document why they are not applicable or were not selected. For example, they do not address a security risk or the risk that they address is tolerable without mitigation. When documenting the risks, desired capabilities, requirements (both selected and not) and security measures, it is preferable to collect these in a document sometimes called a security protection scheme (SPS) or concept of operations (CONOPS). The SPS should include both technical and process security measures and should discuss how each of the principal roles are involved with the IACS.

Developing attack scenarios typically involves identifying threats and known vulnerabilities that are applicable to the system. Known vulnerabilities are those that have been discovered and, in many cases, reported within the industry. Known vulnerabilities are often related to OS, open-source software and control system software; however, they can be associated with any element of the IACS. See 12.2.9, EVENT 1.9: Vulnerability handling, for more information about addressing newly discovered vulnerabilities.

6.3.2 ORG 2.2: Processes for discovery of security anomalies

6.3.2.1 Requirement

The asset owner shall have policies and procedures related to periodically discovering and addressing, through manual or automated processes:

- a) undocumented and unauthorized components/software connected to or communicating within the IACS,
- b) undocumented and/or unauthorized network traffic,
- c) new and/or known but undocumented vulnerabilities in the IACS, and
- d) other security anomalies and non-conformities.

6.3.2.2 Rationale and supplemental guidance

Security anomalies, non-conformities and undocumented/unauthorized components, software and network traffic represent potential threats to the IACS and new or known but undocumented vulnerabilities provide potential entry points to attackers.

Discovering and assessing their potential impact to the IACS is a necessary part of risk management. Using manual processes or automated tools on a regular basis limits the exposure to these threats and exploitation of vulnerabilities, allowing them to be detected and subsequently addressed.

For example, the network should be regularly probed or examined to discover unauthorized components and network accessible services. Other processes/tools should then be used to identify the software that is associated with these transmission control protocol (TCP) / internet protocol (IP) ports.

Care should be taken when using automated tools to ensure that they do not hinder or impact the operation, performance and availability of the IACS.

6.3.3 ORG 2.3: Secure development and support

6.3.3.1 Requirement

The asset owner shall have policies and procedures addressing the use of a secure development lifecycle process for the development and support of systems and components used in the IACS.

6.3.3.2 Rationale and supplemental guidance

Secure development and testing of systems and components prior to incorporating them into the IACS provides assurance that they will not allow the compromise of the integrity or availability of the IACS, or the disclosure of IACS confidential data. Secure support processes ensure that the security of systems and components is maintained throughout their lifecycle. See IEC 62443-4-1 for secure product development and support requirements.

Requiring secure development and support processes for systems and components for an IACS ensures that system and component security will be developed and tested prior to inclusion in the operational IACS, supported once operational, and managed throughout all phases of the lifecycle, including decommissioning at end-of-life and/or operational use.

6.3.4 ORG 2.4: SP reviews

6.3.4.1 Requirement

The asset owner shall have policies and procedures related to periodically reviewing the SP to:

- a) verify that it is being properly applied,
- b) validate that the technical and process security measures continue to meet the system security requirements,
- c) address changes in the organization and its processes, technical changes in the Automation Solution and changes in the threat environment, and
- d) make improvements, as appropriate.

6.3.4.2 Rationale and supplemental guidance

Regular assessments are used to verify compliance to the SP, validate that the SP meets the desired system security requirements and ensure that changes to the organization, its policies, the Automation Solution and threats to the IACS are being addressed by the SP. Such assessments are typically used to evolve the SP in terms of the requirements it meets and the ML at which they are met.

It is not uncommon for an asset owner to develop a long-term plan, referred to as a road map, for implementing requirements over a period of time. Regular assessments can then be used to monitor:

- the road map and adjust it as necessary, and
- its progress.

6.4 ORG 3 – Security of physical access

6.4.1 ORG 3.1: Physical access control

6.4.1.1 Requirement

The asset owner shall have policies and procedures around physical access to the IACS, including access to facilities, equipment and cabling, so that the physical access is controlled to meet risk targets.

6.4.1.2 Rationale and supplemental guidance

Physical access controls protect the IACS from personnel and equipment gaining unwanted physical proximity to the IACS. Physical proximity can allow connection of wired or wireless equipment to the IACS and use of IACS resources, such as workstations or surveillance (for example, cameras). In general, organizations will restrict physical access to systems, structures and components associated with the IACS, and permit access to only authorized personnel, including employees, contractors, consultants, product suppliers and service providers.

A variety of mechanisms can be used to provide physical access controls such as fences, guards, badges, locked doors, cameras and conduits for wiring.

7 SPE 2 – Configuration management

7.1 Purpose

The requirements in this SPE are defined to ensure that the asset owner documents the IACS architecture, maintains an inventory of its hardware and software components and controls changes to them.

7.2 CM 1 – Inventory management of IACS hardware/software components and network communications

7.2.1 CM 1.1: Asset inventory baseline

7.2.1.1 Requirement

The asset owner shall have policies and procedures to document, verify and maintain, throughout the full life cycle of the IACS, the inventory baseline of all devices, hardware components, software components, communications protocols and open communications ports used in the IACS including but not limited to:

- a) organizational responsibilities,
- b) manufacturer,
- c) model,
- d) version numbers,
- e) serial numbers,
- f) network interfaces,
- g) communication addresses,
- h) revision/patch levels, and
- i) history.

7.2.1.2 Rationale and supplemental guidance

Having and maintaining a verified inventory baseline is necessary to validate that all devices, hardware components, software components and communications protocols/ports/endpoints are known to the asset owner, and consequently authorized and configured to meet security requirements. Maintaining the IACS inventory baseline confirms that the current implementation of the system matches the approved design. The inventory baseline should reflect the implemented system through all of the IACS life cycle phases, including design, specification, implementation, verification and validation, operations, maintenance and decommissioning.

In order to identify and manage supply chain cybersecurity risks, the inventory baseline should account for third-party assets that are part of the IACS.

Having and maintaining an inventory baseline also provides the ability for the asset owner to review the properties of components and communications paths. This helps establish the basis for managing changes to components and communications paths, including additions, deletions and updates.

Configuration baselines are normally maintained in a database that contains component and protocol properties. These properties should include information that identifies and describes the component/protocol, and its use, current state and history.

7.2.2 CM 1.2: Infrastructure drawings/documentation

7.2.2.1 Requirement

The asset owner shall have policies and procedures to verify and maintain the current baseline of drawings/documentation showing the physical and logical connectivity of all IACS devices and software components.

7.2.2.2 Rationale and supplemental guidance

Having and maintaining verified architecture drawings and descriptions provides the basis for conducting security assessments, including the identification of trust boundaries. Verifying that the drawings match the implementation is necessary to verify that unauthorized devices are not connected to the system.

Configuration baselines as described in 7.2.1, CM 1.1: Asset inventory baseline, should be supplemented by architecture drawings and descriptions. Architectural relationships should include network connectivity, communications protocols/ports and data/control flows between components.

Infrastructure drawings and documentation should be classified and protected in accordance with 10.2.1, DATA 1.1: Data classification, and 10.2.2, DATA 1.2: Data confidentiality.

Examples of documentation often used include line drawings, functional drawings, elevations and rack layouts, room layouts, security perimeter drawings (electronic and physical) and communication path protocol and endpoint information.

7.2.3 CM 1.3: Configuration settings

7.2.3.1 Requirement

The asset owner shall have policies and procedures to document the configuration settings of all IACS devices and software applications and to verify their operational compliance with the documented configuration.

7.2.3.2 Rationale and supplemental guidance

The configuration of IACS components will often change during the life cycle of the system to meet the goals and objectives of its operation through different stages including installation, deployment, maintenance, repair, and upgrades. Documenting approved configuration settings and having a means of verifying that they are applied or written correctly to components is essential to the security and operation of the system.

It is important to have accurate records of the IACS configurations to assure that a system performs as intended and that it is identified and documented in sufficient detail to support its projected life cycle.

7.2.4 CM 1.4: Change control

7.2.4.1 Requirement

The asset owner shall have policies and procedures to authorize, validate and approve changes to the current configuration baseline and infrastructure drawings/documentation, including revision and patch levels.

7.2.4.2 Rationale and supplemental guidance

Validating the implemented system against the configuration baseline and controlling changes are primary mechanisms for protecting against the unauthorized addition or removal of hardware, software and communications to the IACS, including substitutions, software updates and the addition of communications paths.

When combined with 7.2.1, CM 1.1: Asset inventory baseline, 7.2.2, CM 1.2: Infrastructure drawings/documentation and 7.2.3, CM 1.3: Configuration settings, asset owners are able to support forensics by inspecting components/communications and determining when they were added to the system, when they were updated, who authorized the updates and who performed the updates.

A formal process for documenting, submitting and approving change requests is necessary. This process should identify the organization roles and personnel who are responsible for these activities.

In addition, a good practice to follow is "separation of duty", in which the people implementing the change, validating the change and approving the change are different people.

8 SPE 3 – Network and communications security

8.1 Purpose

The requirements in this SPE are defined to ensure that the IACS is protected from attacks conducted through the network and through communications capabilities. These attacks can originate external to the IACS, across security zone boundaries within the IACS and from unauthorized or compromised systems or devices connected to IACS networks. See IEC 62443-3-2 for guidance on assessing risk and partitioning systems into security zones.

8.2 NET 1 – System segmentation

8.2.1 NET 1.1: Segmentation from non-IACS zones

8.2.1.1 Requirement

The asset owner shall have policies and procedures segmenting IACS from non-IACS zones and limiting any interconnections to the minimum necessary for IACS operations and within tolerable risk.

8.2.1.2 Rationale and supplemental guidance

Remote/external networks provide access to the IACS from potentially unknown sources, and consequently pose a threat to the IACS. Network segmentation provides the means for restricting traffic (data and control flows) and limiting visibility between the IACS and external systems.

Traffic between the IACS and external systems should be identified, managed, authorized and documented. Authorization and management are a typically part of policies that define the technical and process aspects of secure remote access. In addition, this traffic should be characterized by their endpoints (for example, device and software application) and by their communications protocol.

Network security devices at the boundaries between IACS and non-IACS segments are used to enforce, authorize and monitor data flows, and their configurations should be appropriate, documented and kept current. They should be configured to limit access to only those access paths that are necessary and for which the level of trust associated with their external endpoint and the associated risk is tolerable.

Based on the tolerable risks, the asset owner should determine the SL-Ts for the IACS. IEC 62443-3-2 provides a description of the process steps to partition the Automation Solution into zones and conduits. It also describes how to identify the SL-T for each zone and conduit.

See 12.2.1, EVENT 1.1: Event detection, for more information about monitoring. See 8.2.6, NET 1.6: Internal network access control, for more information about zone-to-zone segmentation within the IACS environment.

8.2.2 NET 1.2: Documentation of zones and network zone interconnections

8.2.2.1 Requirement

The asset owner shall have policies and procedures for documenting and maintaining a baseline of all IACS zones and network zone interconnections and/or conduits, the security risks associated with each, and their designation as trusted or untrusted.

8.2.2.2 Rationale and supplemental guidance

As part of the network segmentation process, or after the network has been segmented, interconnections between zones and/or conduits should be evaluated for threats and associated risks. Interconnections are typically implemented by network devices, such as routers, firewalls and data diodes, that permit network traffic to flow between segments.

Understanding which interconnections are trusted or untrusted is an essential part of determining where network access controls are required (see 8.2.3, NET 1.3: Network segmentation from safety systems, and 8.2.4, NET 1.4: Network autonomy). Untrusted interconnections should be subject to a higher degree of protection.

NOTE Zones and conduits (see IEC TS 62443-1-1 and IEC 62443-3-2) are used to represent logical partitions of the system and communications channels between them whose implementation can be supported by network segmentation and network devices.

8.2.3 NET 1.3: Network segmentation from safety systems

8.2.3.1 Requirement

If the IACS contains a safety system network, the asset owner shall have policies and procedures related to protecting the safety system from interference by non-safety system networks and their devices.

8.2.3.2 Rationale and supplemental guidance

Safety systems should be operationally independent from control systems and other networks, including both wired and wireless networks. While it is often necessary for the safety system to be connected to the IACS for operator, engineering and administrator access, the safety system should not be connected to the control system networks in a manner that safety system functions and communications can be disrupted or otherwise compromised by the control system. Therefore, the safety system should be protected from interference from applications outside the safety system.

NOTE IEC 62443-3-2 recommends giving special attention to safety systems when creating zones and conduits.

Firewalls, gateways and other methods of managing access to the safety system can be provided to implement a degree of separation between the control system and the safety system. Other mechanisms or design strategies that protect the safety system from interference can also be used.

8.2.4 NET 1.4: Network autonomy

8.2.4.1 Requirement

The asset owner shall have policies and procedures around the ability to operate the IACS as designed when disconnected from external networks (for example, fail-safe operation, safe shut down, restricted operation and normal operation).

8.2.4.2 Rationale and supplemental guidance

The IACS should be capable of operating as designed when communication with non-IACS systems is lost. That is, failure of network communications with external systems should not cause the IACS to fail. The IACS may operate in a degraded mode or less optimized way, but, at a minimum, it should be possible to continue essential functions.

There can be cases, such as the Industrial Internet of Things and/or Industry 4.0, where there are external connections to the IACS. In cases such as these, the IACS should be designed so that essential functions continue to operate when external connections are disconnected.

8.2.5 NET 1.5: Network disconnection from external networks

8.2.5.1 Requirement

The asset owner shall have policies and procedures around the ability to disconnect the IACS from external networks to protect itself or the external networks from actual or suspected threats.

8.2.5.2 Rationale and supplemental guidance

The IACS should be able to be disconnected, either logically or physically, from external networks in response to adverse security-related conditions (see 8.2.4, NET 1.4: Network autonomy) originating from either the IACS or the external networks. However, the asset owner should determine when such disconnection is advised to ensure that disconnection does not create a higher risk than the actual or suspected threats.

Disconnection techniques can include manual or automatic disconnection. Network devices that allow traffic flow to/from external networks to be disabled or blocked can be used for this purpose.

8.2.6 NET 1.6: Internal network access control

8.2.6.1 Requirement

The asset owner shall have policies and procedures around identifying, documenting, and mitigating or otherwise managing security risks associated with communications between internal IACS network segments, including determining a tolerable risk level and responding to risks outside that tolerable risk level.

8.2.6.2 Rationale and supplemental guidance

When analysing the risks between internal IACS network zones in 8.2.2, NET 1.2: Documentation of zones and network zone interconnections, it is important to consider the potential for disruption to essential functions by disconnecting or restricting network communications between those zones. Communications between internal IACS network zones can also present risks, such as those associated with untrusted interfaces that need mitigation. When they do, these risks can be mitigated by restricting traffic between them and allowing only those data and control flows that are necessary and have been authorized.

Communications between internal IACS network segments that were identified in 8.2.2, NET 1.2: Documentation of zones and network zone interconnections, to have tolerable risks should be authorized and allowed if they are essential. All traffic that presents intolerable risks should be blocked and reported. This can be accomplished by using network segmentation devices that inspect all traffic and block all unauthorized traffic, also called default deny.

8.2.7 NET 1.7: Network accessible services

8.2.7.1 Requirement

The asset owner shall have policies and procedures around protecting network accessible services from unauthorized network access.

8.2.7.2 Rationale and supplemental guidance

Application services accessible through the network generally provide access to IACS resources. They should be accessed only by devices, applications and users and from network segments that are authorized to do so. This will protect the IACS against unauthorized access and against probes that attempt to discover and exploit application service vulnerabilities, thus reducing the attack surface of the IACS.

Network access control mechanisms, including but not limited to managed switches, routers with access control lists and firewalls should be configured to allow access to application services only from authorized client network addresses and ports and protocols. In addition, application services should be configured to allow only authorized users to establish sessions with them, thus providing an additional layer of protection.

8.2.8 NET 1.8: User messaging

8.2.8.1 Requirement

The asset owner shall have policies and procedures around restricting the capability of user-to-user messages transferred on IACS networks from containing payloads, such as attachments, network links or scripts, that can be used to support attacks against the IACS.

8.2.8.2 Rationale and supplemental guidance

Attachments, network links to remote applications and scripts have the potential to introduce malware into the IACS.

Email, instant messaging and other mechanisms that can be used to transfer files or establish links to unknown destinations should be excluded from use in the IACS.

8.2.9 NET 1.9: Network time distribution

8.2.9.1 Requirement

The asset owner shall have policies and procedures around securely distributing and synchronizing time within the IACS.

8.2.9.2 Rationale and supplemental guidance

Accurate, system-wide time is used to timestamp events when they occur. Therefore, time needs to be distributed throughout the IACS using a protocol that provides for synchronization across devices and preferably provides some level of protection against tampering.

It is important to verify that the time distribution protocol used is commonly accepted for industrial uses and has the granularity needed for the IACS. At the time of publication of this document, the IEEE 1588 [18] standard provides finer granularity than the network time protocol (NTP) and is more cost effective than Global Positioning System (GPS) technologies. Secure versions of some of the common time synchronization protocols can be used to provide additional authentication and validation to aid in protecting against the potential for tampering.

8.3 NET 2 – Secure wireless access

8.3.1 NET 2.1: Wireless protocols

8.3.1.1 Requirement

The asset owner shall have policies and procedures about the use of wireless communications within the IACS and which industry accepted protocols are authorized for use, if any. Any wireless protocol(s) shall be documented, and this documentation maintained to include:

- a) a current baseline configuration of each,
- b) data exchanges with other network segments, and
- c) security capabilities and features employed by each wireless network.

8.3.1.2 Rationale and supplemental guidance

Wireless networks are not restricted by physical boundaries, allowing devices outside the physical perimeter of the IACS to access it. Therefore, it is important for the asset owner to use proven wireless protocols. It is also important for the asset owner to know how they are used, the data that is transferred over them and their security capabilities, including their strengths and limitations. Wireless and radio frequency (RF) surveys and security assessments can be used to gain understanding of their capabilities. Without this knowledge, the asset owner could not be able to make security-related decisions regarding their use.

The asset owner should ensure that it has identified and documented, as part of the IACS baseline, all wireless networks used by the IACS and their data flows. The asset owner should also be aware of the security features provided by them and make all of this information available for security assessments performed on the IACS. As part of a wireless and RF survey, asset owners should also consider looking for potential unknown and/or unauthorized wireless networks within their environment as these can represent a potential attack vector for their IACS.

8.3.2 NET 2.2: Wireless network segmentation

8.3.2.1 Requirement

If wireless communications are authorized for use in the IACS, the asset owner shall have policies and procedures around segmenting wireless networks from other IACS network segments.

8.3.2.2 Rationale and supplemental guidance

Wireless networks are not restricted by physical boundaries, allowing devices outside the physical perimeter of the IACS to access and transfer data to/from them. Therefore, it is important for the asset owner to control/manage all access, including data flows, within and from wireless networks. Subclause 8.3.1, NET 2.1: Wireless protocols, specifies the requirement for describing security-related characteristics for accessing the IACS from wireless networks.

Access controls, such as those provided by network segmentation devices and wireless gateways, should be configured to allow only necessary communications to/from wireless networks. Those devices should be used at the interface(s) between the IACS and the wireless network.

8.3.3 NET 2.3: Wireless properties and addresses

8.3.3.1 Requirement

If wireless communications are authorized for use in the IACS, the asset owner shall have policies and procedures around configuring wireless networks with properties and network addresses that minimize information useful to attackers.

8.3.3.2 Rationale and supplemental guidance

Network visible properties, such as network names and service set identifiers (SSIDs), that are too descriptive can give attackers information they can use to refine their attack. Network addresses can be statically configured, or they can be automatically assigned using the dynamic host control protocol (DHCP) or bootstrap protocol (BOOTP). Unfortunately, both DHCP and BOOTP have known vulnerabilities that can be exploited by attackers. Therefore, approaches for assigning SSIDs and network addresses should follow commonly accepted industry security practices.

Commonly accepted practices for network names at the time of publication of this document are to use descriptive names that keep confusion for administrators to a minimum, but that do not provide location, ownership, function detail or other information that could be useful to attackers.

8.4 NET 3 – Secure remote access

8.4.1 NET 3.1: Remote access applications

8.4.1.1 Requirement

If remote access is authorized for use in the IACS, the asset owner shall have policies and procedures around the use of commonly accepted remote access applications in the IACS.

8.4.1.2 Rationale and supplemental guidance

Remote access applications, such as remote desktop applications, allow remote login to workstations and devices. Other remote access applications, like Open Platform Communications (OPC), provide remote connections into the IACS. In the past, many remote access applications were not developed with adequate security and were breached. Therefore, remote access applications used in the IACS should be properly vetted prior to use.

Remote access connections should be investigated to ensure that the version and configuration settings for the application(s) used do not have any known vulnerabilities. New remote access products should not be used until carefully evaluated and tested by reputable and well-known third parties for security weaknesses.

8.4.2 NET 3.2: Remote access connections

8.4.2.1 Requirement

If remote access is authorized for use in the IACS, the asset owner shall have policies and procedures around authorizing, authenticating, encrypting, documenting, logging and monitoring all interactive remote access connections. Documentation for each connection shall include, but not be limited to:

- a) its purpose,
- b) the remote access application to be used,
- c) encryption and authentication technologies used,
- d) how the connection will be established (for example, via the Internet through a virtual private network (VPN) through a DMZ) with instructions, as necessary,
- e) the circumstances requiring the connection,
- f) the length of time the connection needs to be open, including expected inactivity periods,
- g) the location and identity of the remote client device, application and user, and
- h) any compliance requirements that need to be met prior to establishing the connection.

8.4.2.2 Rationale and supplemental guidance

Interactive remote access applications, such as remote desktop applications, allow remote login to workstations and devices. Other remote access applications, like OPC, provide remote connections into the IACS. In both cases, they provide the potential for a remote computer, like a workstation or laptop, that has potentially been infected with malware to infect or attack the IACS. For example, a laptop with remote access privileges might be taken offsite, be connected to the Internet and then be infected. From the same laptop, the user might then create a VPN connection and establish a remote desktop connection over a corporate VPN to the IACS. If written with sufficient intelligence, the malware will then have direct access to the IACS.

The asset owner should have a process for documenting and authorizing all remote access connections before they can be used. This typically includes a process for requesting a remote access connection between a client and a server, a validation and approval process for the connection based on its expected use and a process to prepare for the connection for use, such as creating firewall rules, configuring VPNs and the DMZ and granting the client user access to the server application.

This should be documented along with any instructions that are needed to prepare and use the connection(s). The documentation should indicate why the connection is needed, how long it needs to be open, if there are any expected inactivity periods and the condition/circumstance that causes the connection to be needed. This documentation should be adequate to evaluate and approve the request, and, if approved, to authenticate the client device and user.

8.4.3 NET 3.3: Remote access termination

8.4.3.1 Requirement

If remote access is authorized for use in the IACS, the asset owner shall have policies and procedures around terminating all interactive remote access connections after a configured inactivity period.

8.4.3.2 Rationale and supplemental guidance

Leaving remote access connections open, when not in use, creates an unnecessary risk for the connection to be used inappropriately, or for attackers to attempt to take control of them, thus increasing the attack surface.

Remote access connections should be approved for use for a specific period of time or while actively being used and configured for automatic termination after a specified period of inactivity.

9 SPE 4 – Component security

9.1 Purpose

The requirements in this SPE are defined to ensure that the IACS and its components (for example, devices and software) are appropriately protected from attacks. These attacks can originate through component interfaces, both external and internal. Examples of external interfaces include network interfaces, USB interfaces and configuration ports. Examples of internal interfaces include inter-process communications interfaces and application programming interfaces (APIs).

Subclause 9.4, COMP 3 – Patch management, addresses the application of security patches to close known security vulnerabilities in IACS components. For more details on patch management, see IEC TR 62443-2-3.

9.2 COMP 1 – Components and portable media

9.2.1 COMP 1.1: Component hardening

9.2.1.1 Requirement

The asset owner shall have policies and procedures to harden components prior to their use in the IACS to protect their software and hardware features, to maintain the hardened state during the lifetime of the components and to maintain the documentation of hardening items, means and procedures of the components.

9.2.1.2 Rationale and supplemental guidance

The purpose of hardening is to reduce the attack surface of the device. Hardening a device involves removing or disabling features that are not needed for operation within the IACS, protecting the device interfaces from unauthorized physical and logical access and ensuring that maintenance processes do not cause the hardened state of the device to be compromised or degraded.

Hardening is often accomplished prior to or during installation of a device into the IACS. Security templates, such as those specified by the Center for Internet Security (CIS), define security settings that can be applied to restrict use of the device and protect it against attack. In addition, unnecessary applications, such as games, protocols and digital certificates, shipped with commercial-off-the-shelf (COTS) OSs and other infrastructure software, along with unnecessary communications ports and associated communication access services, should be removed or disabled to prevent them from being used to intentionally or unintentionally interfere with device operations or infect the device with malware.

Hardening measures are specific to each component. Examples of hardening measures include, but are not limited to:

- removing/disabling unnecessary software applications and services (for example, email, office applications and games) and their associated communication access points (for example, TCP / user datagram protocol (UDP) ports);
- enabling interfaces for portable media when authorized for use and disabling them when not authorized for use;
- removing/disabling wireless communications that are not required by the IACS;
- removing/disabling network addresses that are not authorized for use;

- protecting physical and logical access to diagnostic and configuration ports from unauthorized access and use;
- configuring unused ports on network devices (for example, switches and routers) to protect against unauthorized access to the IACS network infrastructure; and
- ensuring maintenance processes maintain the hardened state of the IACS during its lifetime.

During operation, it will often be necessary to change the configuration of components due to operational conditions. For example, a third-party organization may require the asset owner to open ports in order to perform maintenance activities on assets in the IACS. Procedures need to be defined to ensure that the hardened state of both the IACS and its components are recovered after the configuration changes.

9.2.2 COMP 1.2: Dedicated portable media

9.2.2.1 Requirement

The asset owner shall have policies and procedures related to the approved or disapproved use or functions of portable media within the IACS.

9.2.2.2 Rationale and supplemental guidance

Portable media is media that is removable and can be taken offsite to other locations where it can be infected. Dedicating portable media, such as USB memory sticks, to the IACS and to specific use within the IACS can minimize the potential for it becoming infected with malware.

Policies and procedures should be in place that

- define the portable media that can be used and the functions within the IACS for which it can be used, and
- restrict its usage to the approved functions within the IACS and only by approved devices.

In addition, technical measures can be taken to authenticate media to ensure they have been authorized for use within the IACS. For example, if portable media is authorized for use to perform an essential function, such as a safety function, the asset owner needs to ensure that the portable media used is only dedicated to that purpose and not used elsewhere.

9.3 COMP 2 – Malware protection

9.3.1 COMP 2.1: Malware free

9.3.1.1 Requirement

The asset owner shall have policies and procedures to verify that all components and portable media (if portable media is authorized for use in the IACS) are free of known malware before being used in the IACS.

9.3.1.2 Rationale and supplemental guidance

Devices and portable media can be infected prior to or during shipment. This provides a method of attack that does not require network connectivity or physical presence of the attacker. Ensuring that malware is not present in devices and portable media installed into the IACS minimizes this avenue of attack. For encrypted media, the asset owner should obtain assurances from the supplier that procedures are in place to verify the data contained on the encrypted media is free of malware.

Mechanisms used to ensure malware is not present in devices and portable media include scanning and authenticity checks, such as digital signatures. Authenticity checks can determine if software images in the device have not been modified. Scanning is used to detect known malware and is useful, in particular when authenticity checks are not supported. Further, distribution path protections, such as anti-tampering seals can also be used to support this requirement.

9.3.2 COMP 2.2: Malware protection

9.3.2.1 Requirement

The asset owner shall have policies and procedures related to the installation, functioning, and maintenance of malware protection mechanisms, where feasible.

9.3.2.2 Rationale and supplemental guidance

Mechanisms that provide protection against known malware are used to detect malware and also to prevent it from executing. These need to be verified to prevent the infection of the system with malware. These mechanisms also need to be tested for compatibility with the component, meaning that they have been tested to verify that they do not interfere with the function and operation of the component.

Malware protection software is often not available for all IACS components. Components for which malware protection software is not available should be documented and protected by compensating security measures in the IACS that are appropriate for the assessed level of risk.

Three primary methods for protecting a component against malware are antivirus, allow-listing and digital signature verification. Antivirus software is used to examine files and data entering the device and compare it to known bit-patterns, called a malware signature, often called deny-listing. The malware signatures need to be kept up to date to cover all known malware. When malware is detected, it is normally quarantined, and the user is notified to take the appropriate action. Allow-listing, on the other hand, is configured to allow only authorized software to execute. Thus, allow-listing does not require updates to malware signatures and also provides protection against previously unknown malware. Digital signature verification can be considered a form of allow-listing, since it authenticates software based on its digital signature (usually a form of a secure hash) prior to allowing it to run.

9.3.3 COMP 2.3: Malware protection software validation and installation

9.3.3.1 Requirement

The asset owner shall have policies and procedures related to the testing for compatibility, approval and installation of malware protection software and any related malware signature files in a timely manner after their release.

9.3.3.2 Rationale and supplemental guidance

Anti-malware mechanisms are often integrated into OS routines, and therefore, have the potential for affecting how the system operates. In addition, because malware protection software examines files and data for predefined bit-patterns, it could be that legitimate device software or data has the same bit patterns. This is unlikely, but it has occurred. Therefore, all anti-malware software should be checked for compatibility with device software to ensure that it does not interfere with the function and operation of the device.

Testing of anti-malware software should be performed prior to its use in a device. This is generally done by the service provider or the product supplier.

Because the IACS is vulnerable to known malware until malware protection software and its malware signature files are installed, timely installation is important. Timeliness, therefore, is a factor in reducing risks to a tolerable level.

9.4 COMP 3 – Patch management

9.4.1 COMP 3.1: Security patch authenticity/integrity

9.4.1.1 Requirement

The asset owner shall have policies and procedures related to verifying the authenticity and integrity of all patches prior to installation.

9.4.1.2 Rationale and supplemental guidance

Patches are typically distributed by the product supplier using a variety of delivery mechanisms, including network transfers, CDs/DVDs and USB memory sticks. During the transfer, it is possible that the patches are intercepted and infected with malware. Therefore, verifying their integrity and authenticity is necessary.

Asset owners should verify that all patches are received directly from the patch developer, that the distribution path is protected and that support for authenticity and integrity checking is provided, such as digital signatures, or that compensating security measures are applied when digital authenticity and integrity checking is not feasible. In addition, asset owners should verify that patches have not been infected at the product supplier's site. For distribution media, such as CDs/DVDs/USB, tamperproof seals should also be used. See IEC TR 62443-2-3 for additional guidance.

9.4.2 COMP 3.2: Security patch validation and installation

9.4.2.1 Requirement

The asset owner shall have policies and procedures related to the testing for compatibility, approval and installation of security patches applicable to components in a timely manner after their release.

9.4.2.2 Rationale and supplemental guidance

Security patches are often provided for OS and infrastructure software that is developed independently from IACS software. As a result, the IACS software can be affected by these patches. Therefore, it is necessary to test security patches with the IACS prior to using them.

Testing of security patches should be performed prior to its use in a device. This is generally done by the service provider or the product supplier.

Because patches close vulnerabilities, the IACS is vulnerable to associated attacks until the patches are installed. Therefore, timely installation is important and is a factor in reducing risks to a tolerable level.

9.4.3 COMP 3.3: Security patch status

9.4.3.1 Requirement

The asset owner shall have policies and procedures related to the documentation and maintenance of the security patch status of all components.

9.4.3.2 Rationale and supplemental guidance

When troubleshooting or when performing diagnostics or forensics, it is necessary to know the software configuration, including patch status, of a device. In addition, when assessing device vulnerabilities, it is essential to know which security patches have been applied.

Security patch status should be maintained to indicate, at a minimum:

- the patch identifier,
- the applicable software that is being patched,
- the date of patch release, and
- the date of patch installation (planned or actual).

Refer to IEC TR 62443-2-3 for supplemental guidance.

9.4.4 COMP 3.4: Security patching retention of security

9.4.4.1 Requirement

The asset owner shall have policies and procedures to verify that security patch installation does not cause a reduction in the security of the component.

9.4.4.2 Rationale and supplemental guidance

In some cases, installation of patches can introduce known vulnerabilities, cause the removal of configuration settings, change the way the software handles configuration settings or change the function of the software. If the installation is not properly managed, installation can also result in loss of integrity of device contents, where some elements of the device have been removed as part of the installation process. In addition, patches can be installed that are not authenticated as part of the installation process, potentially resulting in the installation of patches that have been the subject of tampering.

Maintenance procedures should include verification that the state of a device's contents and configuration have not been degraded by patch installation. Refer to IEC TR 62443-2-3 for supplemental guidance.

9.4.5 COMP 3.5: Security patch mitigation

9.4.5.1 Requirement

The asset owner shall have policies and procedures related to assessing the risk of not installing any applicable security patches, and if the risk is not tolerable, addressing the risk and documenting the resolution.

9.4.5.2 Rationale and supplemental guidance

When security patches are not installed, for example because they failed testing, were not approved for installation or were not made available in time, their associated vulnerabilities remain. Therefore, workarounds or other compensating security measures should be used.

The asset owner should ensure that all security patches that are applicable to the device, but that were not installed, are assessed for risk(s) and addressed through workarounds or compensating security measures if the associated risks are unacceptable. Risks and resolutions should be documented. Refer to IEC TR 62443-2-3 for supplemental guidance.

10 SPE 5 – Protection of data

10.1 Purpose

The requirements in this SPE are defined to ensure that data is protected from disclosure (confidentiality) and tampering (integrity).

10.2 DATA 1 – Protection of data

10.2.1 DATA 1.1: Data classification

10.2.1.1 Requirement

The asset owner shall have policies and procedures related to identifying and classifying all IACS data requiring safeguarding according to their protection requirements.

10.2.1.2 Rationale and supplemental guidance

To protect data from disclosure and tampering, it is necessary to understand which data needs to be protected and whether it needs to be protected from disclosure, tampering, loss, loss of use or some other compromise. The risk value to the organization of compromise is also necessary and is used to determine the degree to which it needs to be protected.

A risk assessment generally is used to identify data and the risk/impact to the organization associated with its compromise, including disclosure, tampering, loss or loss of use.

The following are examples of types of IACS data that should be identified and classified:

- a) user authentication and authorization information,
- b) audit and security log information, including audit history,
- c) test data,
- d) configuration data,
- e) cryptographic keys,
- f) backup data,
- g) control action transfers, including direction of transfer,
- h) proprietary and trade secret data, and
- i) any personally identifiable information (PII) collected or processed in the IACS.

10.2.2 DATA 1.2: Data confidentiality

10.2.2.1 Requirement

The asset owner shall have policies and procedures related to the confidentiality of IACS data taking into account risks to compromise of the data according to their classification.

10.2.2.2 Rationale and supplemental guidance

Confidentiality of data needs to be protected whether at rest or in motion. Failure to protect the confidentiality of the data can result in a compromise to it. Data at rest is generally considered to be data held in volatile memory (for example, computer memory) or in non-volatile memory (for example, disk, CD/DVD/USB or flash memory). Data in motion is generally considered to be data being moved between two or more locations, either electronically via some form of communication link or physically.

Data can be protected from unauthorized access via a number of mechanisms. Which mechanism is used and in which combination depends on the classification of data and its value to the organization. Generally, user access controls provide the first level of defence for data at rest, allowing only those authorized to access the data or the software using the data to access it.

Approvals for the transfer of data can be used to restrict which data is transferred.

Encryption can be used to protect data from disclosure. It can be used for data at rest when intruders have somehow defeated access controls. It is often used for data in motion to prevent anyone who is able to intercept or monitor data transmissions from being able to retrieve the original information.

When these capabilities are not feasible or when additional protection is desired, access controls that restrict physical and network access to computers and communications links allow data to be isolated from attackers.

10.2.3 DATA 1.3: Safety system configuration mode

10.2.3.1 Requirement

If safety systems are authorized for use in the IACS, the asset owner shall have policies and procedures related to:

- a) updating the safety system configuration only when configuration mode is enabled, and
- b) only enabling configuration mode when configuration changes are necessary.

10.2.3.2 Rationale and supplemental guidance

The safety system, like a control system, operates according to configuration parameters written or downloaded to it. Typically, the configuration is static, changing only when necessary. To protect against unauthorized changes to the safety system configuration, the safety system configuration should be updated at approved times only, and configuration changes should be allowed only for a finite duration. Such an approach is often referred to as configuration mode for the safety system. Configuration mode can be enabled using explicit actions of the safety system administrator and disabled for normal operation of the safety system once the configuration update has been completed.

A safety system configuration mode should be supported by a software, hardware or mechanical interface that is available only to authorized safety system administrators. The default should always be "disabled".

10.2.4 DATA 1.4: Data retention policy

10.2.4.1 Requirement

The asset owner shall have policies and procedures related to data retention during the entire IACS lifecycle, including purging.

10.2.4.2 Rationale and supplemental guidance

Data retention refers to keeping data values and events, such as logs, histories and backups, for a specified period of time. This also includes ensuring that data requiring safeguarding is purged when the device is decommissioned or otherwise removed from the IACS. Data retention policies, such as the length of time to keep the values, and associated capabilities should be established to support security operations, such as recovery and forensics, and control operations, such as trend analysis. These policies and capabilities should be specified to minimize risks to the organization and be documented.

Data retention policies generally include length of time to keep data values and events for runtime copies, locally accessible copies (for example, logs and historians) and archived copies. Capabilities include capacities to support the policies and the timeliness of being able to retrieve desired copies.

Confidential data in devices should be purged from memory when the device is decommissioned or otherwise removed from service. This prevents disclosure of that data to those who can subsequently have access to the device. For example, a device's memory should be purged when returning a failed board/device to the supplier for repair under a support service contract. See 10.2.2, DATA 1.2: Data confidentiality, for more information on protecting the confidentiality of IACS data.

In some situations, read-only memory should be preserved to allow the product supplier to troubleshoot the problem. To support these cases, the agreements with the supplier should include protection of asset owner data.

Devices used in the IACS should have mechanisms or documented procedures for purging confidential, non-volatile data from them. Non-volatile data media includes disks and flash memory.

10.2.5 DATA 1.5: Cryptographic mechanisms

10.2.5.1 Requirement

The asset owner shall have policies and procedures related to utilizing commonly accepted cryptographic mechanisms in the IACS.

10.2.5.2 Rationale and supplemental guidance

The IACS should use cryptographic mechanisms that are in current use by IT, as well as industrial applications, and are regarded as free of publicly known vulnerabilities and weaknesses.

10.2.6 DATA 1.6: Key management

10.2.6.1 Requirement

If cryptographic mechanisms utilizing keys are approved for use in the IACS, the asset owner shall have policies and procedures around using, protecting and enforcing the lifetime of cryptographic keys, following practices and recommendations commonly accepted by both the industrial and security communities.

10.2.6.2 Rationale and supplemental guidance

Key management is an important component for the use of cryptographic mechanisms, such as data encryption, digital signatures and authentication. Poor key management can result in the compromise of keys that can result in cryptographic failure.

Handling of expiration of certificates needs to be taken into account to avoid risks to the operations of the IACS in the event of an expired certificate.

10.2.7 DATA 1.7: Data Integrity

10.2.7.1 Requirement

The asset owner shall have policies and procedures related to data integrity protection from compromise, whether at rest or in motion (electronically or physically), that take into account applicable risks.

10.2.7.2 Rationale and supplemental guidance

Data needing integrity protection needs to be protected whether at rest or in motion. Failure to protect the integrity of the data can result in a compromise that can impact the industrial process.

Approvals for the transfer of data can be used to restrict which data is transferred, and data/parameter validation can be used to determine if it has been changed in transit or whether invalid values are being transmitted.

Digital signatures can be used to protect data at rest or in motion from tampering. They provide a secure checksum that allows authentication and detection of changes.

When these capabilities are not feasible or when additional protection is desired, access controls that restrict physical and network access to computers and communications links allow data to be isolated from attackers.

11 SPE 6 – User access control

11.1 Purpose

The requirements in this SPE are defined to ensure that users (human users, software processes and devices) are assigned accounts that are used to control access to the IACS and its resources and commands. Access control involves identification, authentication and authorization in order to assign and enforce access rights as well as the control of user sessions. IACS human users include, but are not limited to, engineers, operators, administrators and support personnel.

OS and control system access rights grant users' permission to use IACS resources and issue commands. Typical access rights include read, write and execute; however, others are possible. Sessions are user connections to the system established as a result of successful identification and authentication.

In general, user account management policies should be defined to provide consistency across user accounts that meet the requirements of Clause 11. Such policies will typically be formally documented and provide a framework for creating and maintaining user accounts.

11.2 USER 1 – Identification and authentication

11.2.1 USER 1.1: User identity assignment

11.2.1.1 Requirement

The asset owner shall have policies and procedures for assigning IACS-specific identifiers, authenticators and roles to users (human users, software processes and devices).

11.2.1.2 Rationale and supplemental guidance

User accounts are digital representations of users. Identifiers relate users to accounts and authenticators, such as passwords, give human users, software processes and devices permission to use their associated account. Human users are authenticated during login and are granted access to run programs under the account used to login. Software processes are authenticated when they are started automatically by the OS and run under the account used to start them.

For devices, the account management system is configured with an account that is used to verify a device's identity during device connection to the system. This capability verifies that devices are authorized to participate in system operations and complements network device authentication (see 11.2.19, USER 1.19: Component authentication), which is used to prevent unauthenticated devices from transmitting or receiving on the network.

Human users and software processes can also be authenticated when they establish a communications connection with another software process, typically referred to as a server. In these cases, the server process determines whether it will use the account under which it is running or the account of the user or software process that was authenticated.