



DPC: 20/30392160 DC

BSI Group Headquarters

389 Chiswick High Road London W4 4AL

Tel: +44 (0)20 8996 9000

Fax: +44 (0)20 8996 7400

www.bsigroup.com

Date: 01 April 2020

Origin: International

Latest date for receipt of comments: 20 May 2020

Project No. 2019/00520

Responsible committee: GEL/65 Measurement and control

Interested committees:

Title: Draft BS IEC 62443-2-2 Ed.1.0 Security for industrial automation and control systems. Part 2-2: IACS Security Program Ratings.

Please notify the secretary if you are aware of any keywords that might assist in classifying or identifying the standard or if the content of this standard

- i) has any issues related to 3rd party IPR, patent or copyright
- ii) affects other national standard(s)
- iii) requires additional national guidance or information

WARNING: THIS IS A DRAFT AND MUST NOT BE REGARDED OR USED AS A BRITISH STANDARD. THIS DRAFT IS NOT CURRENT BEYOND 20 May 2020

This draft is issued to allow comments from interested parties; all comments will be given consideration prior to publication. No acknowledgement will normally be sent. **See overleaf for information on the submission of comments.**

No copying is allowed, in any form, without prior written permission from BSI except as permitted under the Copyright, Designs and Patent Act 1988 or for circulation within a nominating organization for briefing purposes. Electronic circulation is limited to dissemination by e-mail within such an organization by committee members.

Further copies of this draft may be purchased from BSI Shop <http://shop.bsigroup.com> or from BSI Customer Services, Tel: +44(0) 20 8996 9001 or email cservices@bsigroup.com. British, International and foreign standards are also available from BSI Customer Services.

Information on the co-operating organizations represented on the committees referenced above may be obtained from <https://standardsdevelopment.bsigroup.com/>.

Responsible Committee Secretary: Jasnam Channe (BSI)

Direct tel:

E-mail: jasnam.channe@bsigroup.com

Full document details: 20/30392160 DC

Introduction

This draft standard is based on national and international discussions. Your comments on this draft are invited and will assist in the preparation of the consequent standard.

For international standards, comments will be reviewed by the relevant UK national committee before sending the consensus UK vote and comments to the international committee, which will then decide appropriate action. If the international standard is approved, it is usual for the text to be published as a British Standard.

For national standards, comments will be reviewed by the relevant UK national committee and the resulting standards published as a British Standard.

UK Vote

Please indicate whether you consider the UK should submit a negative (with supporting technical reasons) or positive vote on this draft. Please indicate if you are aware of any reason why this draft standard should not be published as a British Standard.

Submission of Comments

- **Annotated drafts are not acceptable and will be rejected.**
- All comments should be submitted online at <https://standardsdevelopment.bsigroup.com/>. You will need to register in order to comment.

Template for comments and secretariat observations

Date: xx/xx/20xx	Document: ISO/DIS xxxx
------------------	------------------------

1	2	(3)	4	5	(6)	7
MB	Clause No./ Subclause No./Annex (e.g. 3.1)	Paragraph/Figure/ Table/Note	Type of comment	Commend (justification for change) by the MB	Proposed change by the MB	Secretariat observations on each comment submitted
	3.1	Definition 1	ed	Definition is ambiguous and needs clarifying.	Amend to read '...so that the mains connector to which no connection...'	
	6.4	Paragraph 2	te	The use of the UV photometer as an alternative cannot be supported as serious problems have been encountered in its use in the UK.	Delete reference to UV photometer.	



65/797/CD

COMMITTEE DRAFT (CD)

PROJECT NUMBER:

IEC 62443-2-2 ED1

DATE OF CIRCULATION:

2020-03-27

CLOSING DATE FOR COMMENTS:

2020-06-19

SUPERSEDES DOCUMENTS:

65/717/NP, 65/741A/RVN

IEC TC 65 : INDUSTRIAL-PROCESS MEASUREMENT, CONTROL AND AUTOMATION

SECRETARIAT:

France

SECRETARY:

Mr Rudy BELLIARDI

OF INTEREST TO THE FOLLOWING COMMITTEES:

TC 44, SC 45A, TC 57, SC 62A, ISO/IEC JTC 1/SC 41

PROPOSED HORIZONTAL STANDARD:



Other TC/SCs are requested to indicate their interest, if any, in this CD to the secretary.

FUNCTIONS CONCERNED:

☐ EMC

☐ ENVIRONMENT

☐ QUALITY ASSURANCE

☐ SAFETY

This document is still under study and subject to change. It should not be used for reference purposes.

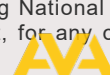
Recipients of this document are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

TITLE:

Security for industrial automation and control systems – Part 2-2: IACS Security Program Ratings

NOTE FROM TC/SC OFFICERS:

Copyright © 2020 International Electrotechnical Commission, IEC. All rights reserved. It is permitted to download this electronic file, to make a copy and to print out the content for the sole purpose of preparing National Committee positions. You may not copy or "mirror" the file or printed version of the document, or any part of it, for any other purpose without permission in writing from IEC.



Documents

Document Sharing Hub

FOREWORD	Error! Bookmark not defined.
INTRODUCTION	6
1 Scope	7
2 Normative references	7
3 Terms, definitions, abbreviated terms, acronyms, and conventions	8
3.1 Terms and definitions	8
3.2 Abbreviations	9
3.3 Conventions	9
4 Roles and responsibilities	9
5 Holistic protection scheme	11
5.1 Overview	11
5.2 Holistic protection scheme in the IACS life cycle	12
5.3 Organizational structure and OE	13
6 Security Program Rating	15
6.1 Overview	15
6.2 2.2-SM-001 – Application of security program ratings to zones	16
6.2.1 Requirement	16
6.2.2 Rationale and supplemental guidance	16
6.3 2.2-SM-002 – Application of security program ratings per OE	17
6.3.1 Requirement	17
6.3.2 Rationale and supplemental guidance	17
6.4 2.2-SM-003 – Combined evaluation of technical and organizational measures	17
6.4.1 Requirement	17
6.4.2 Rationale and supplemental guidance	17
6.5 2.2-SM-004 - Rating of security levels of the zones of the automation	17
6.5.1 Requirement	17
6.5.2 Rationale and supplemental guidance	17
6.6 2.2-SM-004 - Rating of organizational security measures for operation	18
6.6.1 Requirement	18
6.6.2 Rationale and supplemental guidance	18
6.7 2.2-SM-005 - Determination of SPR values	18
6.7.1 Requirement	18
6.7.2 Rationale and supplemental guidance	18
7 Use of security program ratings	20
7.1 Use of SPR in risk-reduction	20
7.2 SPR types	21
7.3 Use of SPR in the IACS life cycle	22
Annex A (informative) Role-based activities in the development, operation and maintenance of a holistic protection scheme	24
A.1 Overview	24
A.2 Specification	24
A.3 Design	27
A.4 Implementation	32
A.5 Verification and Validation	34
A.6 Operation	35

48	A.7	Maintenance	36
49	A.8	Decommissioning	37
50	Annex B (informative)	Views	38
51	Annex C (informative)	Use of this international standard	41
52	C.1	Use of ISA-62443-2-2 by external parties	41
53	C.2	Use of ISA-62443-2-2 by IACS asset owners	41
54	C.3	Use of ISA-62443-2-2 by IACS service providers	41
55	C.4	Use of ISA-62443-2-2 by IACS product suppliers	41
56	C.5	Use of ISA-62443-2-2 by independent evaluation organizations	42
57	Annex D (informative)	Evaluation methodologies	43
58	D.1	Overview	43
59	D.2	Detailed assessment, requirements-based	43
60	D.3	Detailed assessment, risk based	43
61	D.4	Simplified evaluation, questions-based	43

62

63

INTERNATIONAL ELECTROTECHNICAL COMMISSION

IEC 62443-2-2 Ed. 1.0

Industrial communication networks - Security for industrial automation and control systems**Part 2-2: IACS security program ratings**

FOREWORD

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

International Standard IEC 62443-2-2 has been prepared under the auspices of IEC technical committee 65 by working group 3 task group 3 of the ISA99 committee.

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

FDIS	Report on voting
65/XX/FDIS	65/XX/RVD

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

This document has been drafted in accordance with the ISO/IEC Directives, Part 2.

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

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

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

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

The National Committees are requested to note that for this document the stability date is 2023.

This text is included for the information of the national committees and will be deleted at the publication stage.

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

INTRODUCTION

Note: The format of this document follows the ISO/IEC requirements discussed in ISO/IEC Directives, Part 2.¹ The ISO/IEC Directives specify the format of this document as well as the use of terms like “shall”, “should”, and “may”. The use of those terms for the requirements specified in Clauses 4 through 14 of this document use the conventions discussed in the ISO/IEC Directives, Part 2, Clause 7.

This standard is part of the ISA/IEC-63443 series and specifies a methodology for the evaluation of the protection of Industrial Automation and Control Systems (IACS) in operation by combining the evaluation of organizational and technical measures in a single values called security program ratings (SPR). It has been developed by Working Group 3 Task Group 3 of the ISA99 committee.

The figure 1 illustrates the different parts of ISA/IEC-63443 being developed. Those that are normatively referenced are included in the list of normative references in Clause 2, and those that are referenced for informational purposes or that are in development are listed in the Bibliography.

EDITOR's NOTE: the figure 1 will be actualized before final adoption of this part.

IEC 62443					
Industrial communication networks – Network and system security					
General		Policies & Procedures		System	
1-1	Concepts and models	2-1	Security program requirements for IACS asset owners	3-1	Secure product development lifecycle requirements
1-2	Master glossary of terms and abbreviations	2-2	IACS security program ratings	3-2	Technical security requirements for IACS components
1-3	System security conformance metrics	2-3	Patch management in the IACS environment	3-3	
1-4	IACS security lifecycle and use-cases	2-4	Security program requirements for IACS service providers		
		2-5	Implementation guidance for IACS asset owners		

Figure 1 - Parts of the ISA/IEC-63443 Series

¹ Numbers in square brackets refer to the Bibliography.

1 Scope

This part of the ISA/IEC-62443 series addresses the evaluation of the cybersecurity protection which can be reasonably expected from a holistic protection scheme for an IACS in operation. It includes a methodology for combining the evaluation of organizational and technical security measures based on a defense-in-depth strategy. The result will be expressed in numerical values called security program ratings (SPR). The term is derived from the term “security program” used in ISA/IEC-63443-2-1 for specifying the security measures an asset owner shall establish as part of the operation activities of the IACS. The methodology is based on the fulfillment of technical and organizational requirements specified in relevant documents of the ISA/IEC-62443 series. Organizational security measures of a holistic protection scheme are included in the security program of the organizations responsible for operation of the IACS. Technical measures include both cybersecurity and physical security measures applied to the automation solution which is used in the IACS.

Developing, operating and maintaining a holistic protection scheme requires the contribution of the asset owners / operators, service providers for integration and maintenance and product suppliers in the various phases of an IACS life cycle. This document describes the contributions of these actors in each phase of the IACS life cycle and the use of SPR to support the evaluation of the results of the activities.

The purpose of the document is to provide a consistent and repeatable way for evaluating the protection of the IACS in operation based on a defense-in-depth strategy. It is not in the scope of this document to prescribe how the evaluation should be performed. Annex C provides guidelines for developing evaluation methodologies. As there is not yet a consensus for mathematical measurements of security, most methodologies are currently based on qualitative evaluation based on the auditor's expertise on the known threat situation at the point of time when the evaluation has been made.

2 Normative references

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

ISA/IEC-TS62443-1-1: 2009 – *Security for industrial automation and control systems: Terminology, concepts and models*

EDITOR'S NOTE: at date of publication of this document ISA/IEC-TS62443-1-1: 2009 is under review. Some contents of ISA/IEC-TS62443-1-1: 2009 referred in this document may evolve. This document will be adapted accordingly.

ISA/IEC-TR62443-2-3:2015– *Security for industrial automation and control systems –Part 2-3: Patch management in the IACS environment*

ISA/IEC-62443-2-4:2017 – *Security for industrial automation and control systems –Part 2-4: Security program requirements for IACS service providers*

ISA/IEC-62443-3-3:2013 – *Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels*

EDITOR'S NOTE: at date of publication of this document ISA/IEC 62443-3-3:2013 is under review. Some contents of ISA/IEC 62443-3-3:2013 will be harmonized with contents of this document. This document will be adapted accordingly.

ISA/IEC-62443-4-1:2018 – *Security for industrial automation and control systems – Part 4-1: Secure product development lifecycle requirements*

ISA/IEC-62443-4-2:2019 – *Security for industrial automation and control systems – Part 4-1: Technical security requirements for IACS components*

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

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in the normative references specified in Clause 2 and the following apply.

EDITOR'S NOTE: at date of publication of this document some definitions are under review. The definitions in this document will be adapted accordingly when evolving to an international standard.

3.1.1

asset

physical or logical object owned by or under the custodial duties of an organization, having either a perceived or actual value to the organization

3.1.2

security measures applied to the automation solution

measures implemented in the automation solution with the goal to achieve a desired security level. These are basically technical measures and eventually technical and/or organizational compensating countermeasures for enhancing technical capabilities of products used in the automation solution

Note to entry: if compensating countermeasures are of organizational nature these must be added as part of the organizational security measures for operation.

3.1.3

holistic protection scheme

set of technical and organizational security measures with the aim to protect an IACS in operation against cyberthreats

3.1.4

Industrial Automation and Control System (IACS)

collection of personnel, hardware, and software that can affect or influence the safe, secure, and reliable operation of an industrial process

Note 1 to entry: in the context of an IACS, all references in ISO/IEC 27001 to "information" refer to the IACS.

Note 2 to entry: In the context of an IACS, all references in ISO/IEC 27001 to an information security system refer to cyber security.

3.1.5

maturity level

degree to which a procedural capability (a process) is performed, formalized, practiced, and optimized

3.1.6

organizational security measures for operation

organizational security measures to be practiced during operation of the automation solution in order to achieve and keep the desired security program ratings. It includes to keep the information used in the security measures up to date.

Note to entry: examples of data used in security measures include but are not limited to virus patterns, firewall rules, active accounts list, backup and restore data.

3.1.7

product

hardware and/or software entity which has been developed to be used in various applications, independently of a specific IACS environment.

Note 1 to entry: examples of products include but are not limited to components and control systems.

Note 2 to entry: definition of component in [ISA/IEC 62443-4-2]: entity belonging to an IACS that exhibits the characteristics of one or more of a host device, network device, software application, or embedded device.

Note 3 to entry: definition of control system in [ISA/IEC 62443-3-3]: hardware and software components of an IACS.

3.1.8

security program rating (SPR)

rating of the protection provided by the holistic protection scheme based on the evaluation of:

- a) the capabilities of the security measures applied to the automation solution; and

b) the maturity to practice the organizational security measures for operation.

3.1.9

security objective

security subdomain which is considered when evaluating the protection provided by a set of technical and organizational measures. Security program ratings can be rated in each security objective so that the protection of the IACS in operation can be represented in the SPR values of the security objective.

3.1.10

security level

level corresponding to the required effectiveness of countermeasures and inherent security properties of components and systems of an automation solution.

Note to entry: definition of security level in [ISA/IEC 62443-3-3]: measure of confidence that the IACS is free from vulnerabilities and functions in the intended manner.

EDITOR'S NOTE: at date of publication of this document ISA/IEC -62443-3-3:2013 is under review. The definition in ISA/IEC -62443-3-3 and the definition in this document will be harmonized. This document will be adapted accordingly.

3.1.11

view

simplified representation of the protection of the IACS in operation in SPR values structured in elements of the view instead of security objective. Compared to the number of security objectives, the views have less elements thus showing a higher level of abstraction in each SPR value.

3.2 Abbreviations

ISA	American National Standards Institute
AO	Asset Owner
IACS	Industrial automation and control system(s)
IEC	International Electrotechnical Commission
ISA	International Society of Automation
ML	Maturity Level
PIN	Personal Identification Number
PS	Product Supplier
SM	Maintenance Service Provider
SI	Integration Service Provider
SL	Security Level
SO	Security Objective
SPR	Security Program Rating

3.3 Conventions

[Describe all conventions used in this document, if any.]

4 Roles and responsibilities

An IACS is defined as a collection of personnel, hardware, and software involved in the operation of an industrial process. Applied to cybersecurity the IACS model includes a technical solution – the automation solution - as well as the organizational security measures for operation according to security policies and procedures. This clause describes the roles involved in the protection of an IACS in operation against cyberthreats.

A role is defined by responsibilities and/or accountabilities as well as associated activities to be fulfilled by an organization. An organization can be an individual, a legal entity, such as a company or government agency, or a subdivision of the legal entity, such as a department.

An organization can fulfill one or multiple roles. For example, it is not unusual that the same company is responsible for the operation of an IACS as well as for the design, implementation and validation of the automation solution. On the other hand, a role can be fulfilled by one or several organizations. For example, the maintenance activities can be performed by different organizations.

The development, operation and maintenance of a holistic protection scheme for an IACS in operation requires the contribution and collaboration of all involved actors according to their designated role. The figure 2 gives an overview of the roles and their distinct activities, duties and responsibilities.

Note: The terms “Asset Owner”, “Maintenance Service Provider”, “Integration Service Provider” and “Product Supplier” are defined in the documents of the ISA / IEC 62443 series as organizations. For the description of the contributions of the various actors in this document these terms are used for activities, duties and responsibilities of the roles associated with them.

The role asset owner (AO) includes two parts. The first role is the accountability for the IACS including the protection of the IACS in operation and the associated risks throughout the life cycle. The role AO defines the tolerable cybersecurity risk as an input requirement for all cybersecurity activities along the IACS life cycle. Whilst remaining accountable, the organization fulfilling this role delegates the responsibilities and the associated activities to organizations fulfilling other roles described in this clause. The second part assigned to the role AO is the responsibility to operate the automation solution according to defined security policies and procedures. It includes to keep information used in security measures like virus patterns, firewall rules, active accounts list, or backup and restore data up to date. The inclusion of these two parts in the role AO considers that in many cases the organization which operates the IACS is also the legal owner and therefore accountable for the IACS.

The role maintenance service provider (SM) is responsible for the maintenance and decommissioning of the automation solution. Compared to the actualization of the information used in the security measures, which is included in the role AO, the maintenance activities have the purpose to upgrade and eventually complement the measures of the holistic protection scheme to follow a change in the threat situation or a modification of the automation solution. A maintenance phase is triggered by the result of a cybersecurity risk assessment showing that the measures of the holistic protection scheme no more provide the desired level of protection. In general, the upgrade includes technical security measures applied to the automation solution as well as the organizational security measures for operation of the holistic protection scheme to keep the desired protection of the IACS in operation. The role SM includes the responsibility for decommissioning parts or the whole automation solution and ensuring that the tolerable residual cybersecurity risk is still matched during or after decommissioning.

The role integration service provider (SI) is responsible for the design and implementation as well as commissioning and validation of the security measures applied to the automation solution. The activities cover the development and validation of a holistic protection scheme for the IACS in operation with the goal to match the tolerable cybersecurity risk. These include the development of technical security measures applied to the automation solution as well as guidelines for organizational measures to be implemented during operation. The base for the guidelines are often given by guidelines provided by the role product supplier. It is not unusual that one or several organizations design and deploy parts or the whole automation solution while another organization is responsible for the commissioning and validation of the automation solution.

The role product supplier (PS) is responsible for the development and support of products used in the automation solution. The activities include the development of product security capabilities to be used in the automation solution following an established product development life cycle process, including incident handling and vulnerability management processes. The role PS has the responsibility for the provision of product specific integration, hardening and operational guidelines for the product(s) they supply to the asset owner.

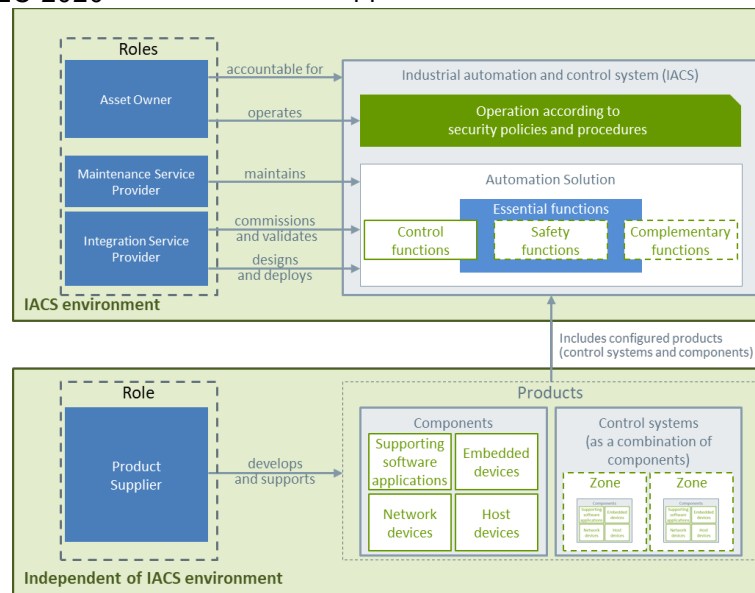


Figure 2 - Principal roles in the ISA / IEC 62443 series

Note: The organizations fulfilling the roles described in this clause can vary from one project to another, and the terms used for naming these organizations may vary heavily in various market sectors, branches or countries, including but not limited to:

Role AO: plant owner, regulator organization, operations department, operation service provider;

Role SM: maintenance department, technical service;

Role SI: plant setup and commissioning department, integrator, EPC company, machine builder; and

Role PS: manufacturer, producer, OEM.

5 Holistic protection scheme

5.1 Overview

The concept of holistic protection scheme recognizes that the protection of an IACS in operation includes a combination of technology, processes, and people. Weaknesses in the protection concept can have their origin in each of these areas. Consequently, all these parts must be included during the evaluation of the protection provided by a holistic protection scheme in a project specific IACS environment. Furthermore, all roles (AO, SI, SM, PS) must contribute to the development, operation and maintenance of a holistic protection scheme.

The technology part consists of cyber/electronic security measures (for example an industrial firewall that controls the communication between network segments) and physical security measures (for example a lock that controls the physical access to a cabinet housing an industrial firewall and its cabling). These are technical security measures applied to the automation solution. They are based on the technical security capabilities of products and include measures resulting from the design of the automation solution itself, for example the protection measures provided by the network architecture. Most of the security measures applied to the automation solution are of technical nature based on the capabilities of products used in the automation solution. Compensating countermeasures may be necessary to reach a desired security level in order to enhance the technical capabilities of the products. These can be additional technical measures and/or organizational measures.

The process and people legs cover operation activities which are relevant for the protection of the IACS against cyberthreats. These are of organizational nature and must be practiced by the personnel in charge during operation of the IACS. The effectiveness of organizational measures relies on the ability of skilled personnel in charge to act reliably over time according to documented security policies in procedures. This is reflected in the maturity level of the responsible organization. The maturity aspect is particularly important as the operation phase often lasts many years.

In many cases, organizational and technical measures are related, and the protection against cyber threats requires the alignment between the security measures applied to the automation solution and the related organizational measures. For example, identification and authentication are a prerequisite to restrict access to the automation solution to authorized human users according to their respective roles. This can be achieved for example with usernames and associated passwords.

The technology part of the protection scheme is that the automation solution provides the technical capabilities for username / password-based identification and authentication mechanisms. The related organizational measures require a password policy specifying length and complexity, expiration conditions, change, reuse, handling, sharing, and disclosure of passwords. The same security issue of identification and authentication can be addressed by a stronger mechanism using multifactor authentication, for example using a smart card and a PIN (Personal Identification Number). This would lead to a higher security level rating of the capabilities provided by the technical security measures applied to the automation solution. In this case the related organizational measures are different and must address the handling of the smart card, the management of the key material as well as setting / changing the PIN.

5.2 Holistic protection scheme in the IACS life cycle

The development, operation and maintenance of a holistic protection scheme should be included in all activities along the IACS life cycle, see figure 3. Starting with a tolerable cybersecurity risk, the desired protection for the IACS in operation should be determined. A design of security measures applied to the automation solution along with guidelines for the related organizational measures must be developed to meet those protection targets. This is usually an iterative process where after each iteration it must be evaluated if the proposed set of technical and organizational measures are able to achieve the desired protection. As part of the design process, the products with the necessary security capabilities will be selected. Where such products are not available, compensating technical or organizational security countermeasures should be developed.

Before starting the operation phase the achieved protection provided by the set of technical and organizational measures should be validated. It is highly desirable to develop documented security policies and procedures for the organizational measures as those must be performed by the personnel in charge during operation of the IACS. The review and actualization of the information used in the security measures like virus patterns, firewall rules, active accounts list, backup and restore data are part of the organizational measures for operation. The validation is often concluded with a dry run involving the organization responsible for operation. The effectiveness of the holistic protection scheme during operation is validated if the technical security measures applied to the automation solution are operated by skilled personnel reliably according to security policies and procedures. This is reflected by the maturity of the organization in charge of operation of the IACS.

As the threat situation may evolve over time, it is necessary to re-assess periodically if the cybersecurity protection is still satisfying the target protection that has been defined in the specification phase. The trigger for a revalidation is given by a defined interval (for example regulatory process, safety management requirement, scheduled maintenance) or by a change in the threat environment or operational conditions, whichever occurs first. A maintenance phase will be started if there is the necessity to improve the set of technical and/or organizational measures in order to adapt to changes in the IACS operating conditions or the threat environment.

The activities of the decommissioning phase have the objective to avoid that information stored in decommissioned assets can be misused and threaten the IACS in operation. Decommissioning portions of a network can have significant repercussions to the remaining parts of the IACS, thus requiring a revalidation of what is left.

Note: In figure 3 the IACS life cycle phases are mapped to the stages of the general representative system life cycle model of IEC 24748 "Systems and software engineering - Life cycle management."