



DPC: 21 / 30445886 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: 27 October 2021
Origin: International**Latest date for receipt of comments: 11 November 2021**

Project No. 2019/00520

Responsible committee: GEL/65 Measurement and control

Interested committees:

Title: Draft BS EN 62443-2-2 Security for industrial automation and control systems. Part 2-2: IACS Security Protection

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 11 November 2021

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 <http://standardsdevelopment.bsigroup.com>

Responsible Committee Secretary: **Jasnam Channe (BSI)**
Direct tel:
E-mail: jasnam.channe@bsigroup.com

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.	

PROJECT NUMBER: IEC 62443-2-2 ED1	
DATE OF CIRCULATION: 2021-10-15	CLOSING DATE FOR COMMENTS: 2021-12-10
SUPERSEDES DOCUMENTS: 65/797/CD, 65/821B/CC	

IEC TC 65 : INDUSTRIAL-PROCESS MEASUREMENT, CONTROL AND AUTOMATION	
SECRETARIAT: France	SECRETARY: Mr Didier GIARRATANO
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 Protection

NOTE FROM TC/SC OFFICERS:
The part title has changed based on comments received and their resolution, from:
"Security for industrial automation and control systems – Part 2-2: IACS Security Program Ratings"
into:
"Security for industrial automation and control systems – Part 2-2: IACS Security Protection"

Copyright © 2021 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.

CONTENTS

FOREWORD	4
INTRODUCTION	6
1 Scope	7
2 Normative references	8
3 Terms, definitions, abbreviated terms, acronyms, and conventions	8
3.1 Terms and definitions	8
3.2 Abbreviated terms and acronyms.....	12
3.3 Conventions	13
4 Security Protection Scheme	14
4.1 Overview	14
4.2 Cybersecurity Requirement Specification.....	14
4.3 Technical and process security measures.....	15
5 Security Protection Ratings	16
5.1 Overview	16
5.2 Determination of the SPR values	17
5.3 Use of the maturity model defined in IEC 62443-2-1 Ed.2	19
5.4 Use of the methodology	21
6 Principal Roles	22
6.1 General	22
6.2 Asset Owner (role AO).....	22
6.3 Integration Service Provider (role SI).....	23
6.4 Maintenance Service Provider (role MS).....	23
6.5 Product Supplier (role PS)	23
7 Roles and activities for the generation of the CRS.....	24
8 Roles and activities for the design and implementation of the security measures applied to the Automation Solution	24
9 Roles and activities for the documentation of the process security measures	27
10 Initial validation of the Security Protection Scheme	27
10.1 General	27
10.2 Validation of the security measures applied to the Automation Solution	27
10.3 Validation of the process security measures	28
10.4 Prediction of the SPR values	28
11 Periodic revalidation of the SPS during operation.....	29
BIBLIOGRAPHY	31

FIGURES

Figure 1 – Simplified Asset Owner Security Protection Scheme (SPS) Lifecycle	7
Figure 2 – Security Protection Scheme	14
Figure 3 – Structure of the CRS.....	15
Figure 4 – Categories of the security measures according to their purpose	16
Figure 5 – Step 1 for the determination of SPR value	17
Figure 6 – Step 2 for the determination of the SPR value	18
Figure 7 – Example of the determination of an SPR value	19

Figure 8 – Maturity model	20
Figure 9 – Example of the determination of the SPR value by using the maturity model of IEC 62443-2-1 Ed.2	21
Figure 10 – Example of a matrix to show progress steps in the implementation of an SPS21	
Figure 11 – Principal roles in the IEC 62443 series	23
Figure 12 – Activities and responsibilities for the generation of the CRS (simplified view)	24
Figure 13 – Activities and responsibilities for the design and implementation of the technical security measures applied to the Automation Solution (simplified view)	25
Figure 14 – Activities and responsibilities for the documentation of process security measures (simplified view)	27
Figure 15 – Example of the determination of the SL value which can be met with capabilities provided by the technical security measures	28
Figure 16 – Example of the prediction of the SPR value	29

INTERNATIONAL ELECTROTECHNICAL COMMISSION

SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS –**Part 2-2: IACS Security Protection****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.

IEC 62443-2-2 has been prepared by IEC technical committee TC 65: Industrial-process measurement, control and automation, in collaboration with the liaison ISA standards committee 99: Industrial automation and control systems security. It is an International Standard.

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

Draft	Report on voting
XX/XX/FDIS	XX/XX/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/standardsdev/publications.

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

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

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

There is no simple recipe for how to secure an industrial automation and control system (IACS) and there is a good reason for this. It is because security is a matter of risk management. Every IACS presents a different risk to the organization depending upon the threats it is exposed to, the likelihood of those threats arising, the inherent vulnerabilities in the system, and the consequences if the system were to be compromised. Furthermore, every organization that owns and operates an IACS has a different tolerance for risk.

This document strives to give guidance for developing technical and process security measures applied to zones and conduits of an IACS and how to use relevant documents of the IEC 62443 series for this purpose. Readers are encouraged to familiarize themselves with the scope and concepts of IEC 62443-2-1, IEC 62443-2-4, IEC 62443-3-2, IEC 62443-3-3, IEC 62443-4-1, and IEC 62443-4-2 before reading this document.

Purpose and intended audience

The audience for this document is intended to include the asset owner, system integrator, product supplier, service provider, and compliance authority.

Usage within other parts of the IEC 62443 series

The document describes the activities for the design, implementation, and validation of an SPS and the use of IEC 62443-2-1, IEC 62443-2-4, IEC 62443-3-2, IEC 62443-3-3, IEC 62443-4-1, and IEC 62443-4-2 for supporting these activities.

1 Scope

This document provides guidance on the development and validation of a set of technical and process security measures called Security Protection Scheme (SPS). The asset owner practicing an IACS Security Program (SP) should ensure the design and application of an SPS to manage risks resulting from cyberthreats to operational facilities controlled by the IACS.

Figure 1 illustrates the content of this document using a simplified IACS life cycle.

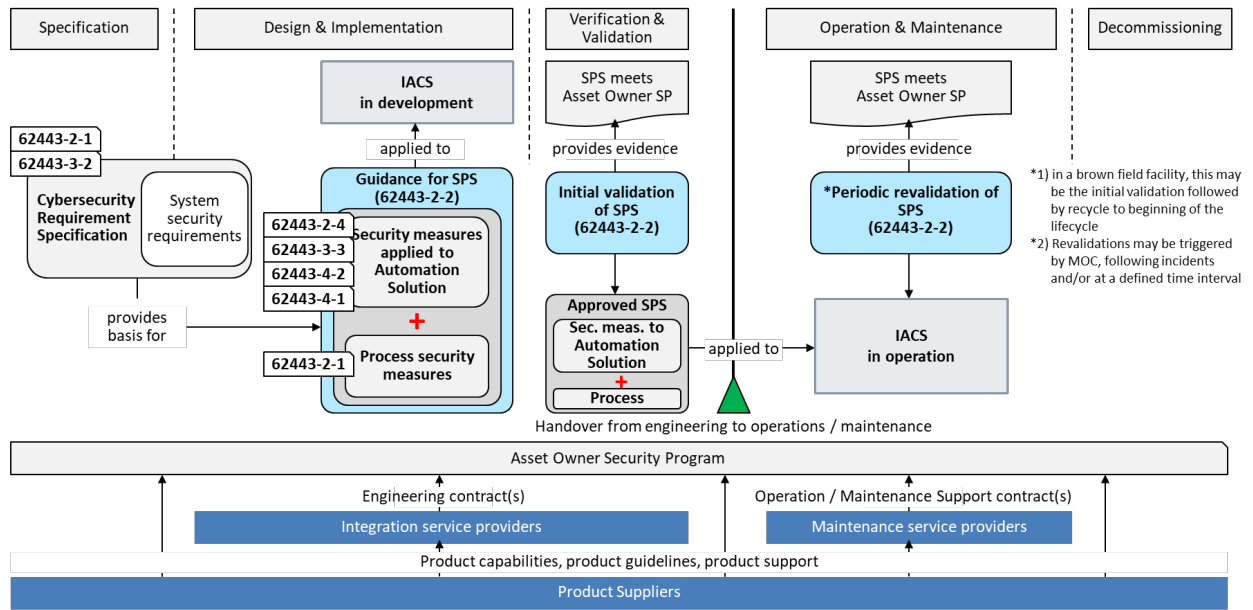


Figure 1 – Simplified Asset Owner Security Protection Scheme (SPS) Lifecycle

The document describes the activities for the design, implementation, and validation of an SPS and the use of IEC 62443-2-1, IEC 62443-2-4, IEC 62443-3-2, IEC 62443-3-3, IEC 62443-4-1, and IEC 62443-4-2 for supporting these activities.

Clause 4 describes the concept of the Security Protection Scheme (SPS).

Clause 5 describes the concept of Security Protection Ratings (SPR) and the methodology to determine the SPR values.

An overview of the roles and responsibilities involved in the activities for the design, implementation, and validation of the SPS is given in clause 6.

Clause 7 describes the roles and activities for generating the security requirements to be included in the Cybersecurity Requirement Specification (CRS).

Clause 8 describes the roles and activities for the design and implementation of the security measures applied to the Automation Solution.

Clause 9 describes the roles and activities for the documentation of the process security measures to be executed during operation.

Clause 10 describes the activities and results of the initial validation of the SPS before going into operation and the prediction of the SPR.

Clause 11 describes the activities and results of the periodic revalidation of the SPS during the operation and maintenance phase.

2 Normative references

Editor's note: the normative references will be defined at future stages of the document.

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

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

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

3.1 Terms and definitions

Editor's note: the terms and definitions will be updated at future stages of the document following reconciliation with an upcoming update of IEC 62443-1-1. The intent will be not to duplicate definitions in the new IEC 62443-1-1.

3.1.1

access

ability and means to communicate with or otherwise interact with a system to use system resources

Note 1 to entry: Access may involve physical access (authorization to be allowed physically in an area, possession of a physical key lock, PIN code, or access card or biometric attributes that allow access) or logical access (authorization to log in to a system and application, through a combination of logical and physical means).

3.1.2

access control

protection of system resources against unauthorized access; a process by which use of system resources is regulated according to a security policy and is permitted by only authorized entities (users, programs, processes, or other systems) according to that policy

3.1.3

accountability

property of a system (including all its system resources) that ensures that the actions of a system entity may be traced uniquely to that entity, which can be held responsible for its actions

3.1.4

asset owner

individual or organization accountable for one or more IACSs

3.1.5

automation solution

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

3.1.6

availability

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

3.1.7

compensating security measure

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

3.1.8

component

entity belonging to an IACS that exhibits the characteristics of one or more of a host device, network device, software application, or embedded device