PD IEC TS 63208:2020

BSI Standards Publication

Low-voltage switchgear and controlgear — Security aspects

bsi.

National foreword

This Published Document is the UK implementation of IEC TS 63208:2020.

The UK participation in its preparation was entrusted to Technical Committee PEL/121/1, Low voltage switchgear and controlgear.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Published by BSI Standards Limited 2020

ISBN 978 0 539 01839 4

ICS 29.130.20

Compliance with a British Standard cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 31 March 2020.

Amendments/corrigenda issued since publication

Date	Text affected

IEC TS 63208

Edition 1.0 2020-03

TECHNICAL SPECIFICATION

colour inside

Low-voltage switchgear and controlgear – Security aspects

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

ICS 29.130.20

ISBN 978-2-8322-8021-8

CONTENTS

FOREWORD 5
INTRODUCTION 7
1 Scope 8
2 Normative references 8
3 Terms, definitions and abbreviated terms 9
3.1 Terms and definitions 9
3.2 Abbreviated terms 12
4 General 13
5 Security objectives 13
6 Security lifecycle management 13
6.1 General 13
6.2 Security risk assessment 14
6.3 Response to security risk 15
6.4 Security requirement specification 16
6.5 Important data 16
6.6 System architecture 16
6.6.1 Control system 16
6.6.2 Levels of communication functionalities 16
6.6.3 Levels of connectivity 17
6.6.4 Control system exposure levels 19
7 Security requirements 20
7.1 General 20
7.2 Cybersecurity aspects 20
7.3 Physical access and environment 21
7.4 Equipment requirement 22
7.4.1 General 22
7.4.2 Hardening 22
7.4.3 Encryption techniques 22
7.4.4 Embedded software robustness and integrity 22
7.4.5 Denial of service 23
7.4.6 Authentication of users 23
7.4.7 Communication systems 24
7.4.8 Wireless communication 24
8 Instructions for installation, operation and maintenance 24
9 Development and testing 25
9.1 General development method 25
9.2 Testing 25
Annex A (informative) Cybersecurity and electrical system architecture 26
A.1 General 26
A.2 Typical architecture involving switchgear and controlgear and their assembly 26
A.2.1 Building 26
A.2.2 Manufacturing 27
A.3 Security levels and product standards 28
Annex B (informative) Use case studies 29
B.1 General 29

B.2 Use case 1 – Protection against malicious firmware upgrade of a circuit-breaker 29
B.3 Use case 2 – Protection against unauthorized access to electrical production network 30
B.4 Use case 3 – Protection against DDoS (distributed denial of service) attack through insecure IoT devices 31
B.5 Use case 4 – Protection against unauthorized access to the electrical network using illegitimate device 32
B.6 Use case 5 – Protection against malicious firmware upgrade of a sensor (e.g. proximity switch), mounted in a machine wired-connected by IO-Link interface 34
B.7 Use case 6 – HMI: human machine interface – Protection against unauthorized access to a simple sensor (mounted in a machine) – improper parametrization 35
B.8 Use case 7 – HMI: human machine interface – Protection against unauthorized access to a complex sensor (mounted in a machine) – improper parametrization 36
B.9 Use case 8 – Protection against unauthorized access to a sensor (e.g. proximity switch), mounted in a machine, connected by wireless communication interface (WCI) 38
Annex C (informative) Basic cybersecurity aspects 40
C.1 General 40
C.2 Identification and authentication 40
C.3 Use control 40
C.4 System integrity 40
C.5 Data confidentiality 41
C.6 Restricted data flow 41
C.7 Timely response to events 41
C.8 Resource availability 41
Annex D (informative) Guidelines for users of switchgear and controlgear 42
D.1 General 42
D.2 Risk assessment and security planning 42
D.2.1 Risk assessment 42
D.2.2 Security plan 42
D.3 Recommendations for design and installation of the system integrating switchgear and controlgear 43
D.3.1 General access control 43
D.3.2 Recommendations for local access 43
D.3.3 Recommendations for remote access 44
D.3.4 Recommendations for firmware upgrades 44
Bibliography 45

Figure 1 – Example of physical interfaces of an embedded device in an equipment which can be subject to an attack 14
Figure 2 – Control system architecture with switchgear and controlgear 17
Figure 3 – Control system connectivity level C3 18
Figure 4 – Control system connectivity level C4 18
Figure 5 – Control system connectivity level C5 19
Figure 6 – Switchgear and controlgear minimum security profile 20
Figure 7 – Example of security instruction symbol 25

Figure A.1 – Building electrical architecture 27
Figure A.2 – Industrial plants 28

Table 1 – Typical threats 14
Table 2 – Level of exposure of a control system 19

INTERNATIONAL ELECTROTECHNICAL COMMISSION

_____

LOW-VOLTAGE SWITCHGEAR AND CONTROLGEAR – SECURITY ASPECTS

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.

The main task of IEC technical committees is to prepare International Standards. In exceptional circumstances, a technical committee may propose the publication of a Technical Specification when

– the required support cannot be obtained for the publication of an International Standard, despite repeated efforts, or
– the subject is still under technical development or where, for any other reason, there is the future but no immediate possibility of an agreement on an International Standard.

Technical Specifications are subject to review within three years of publication to decide whether they can be transformed into International Standards.

IEC TS 63208, which is a Technical Specification, has been prepared by subcommittee 121A: Low-voltage switchgear and controlgear, of IEC technical committee 121: Switchgear and controlgear and their assemblies for low voltage.

The text of this Technical Specification is based on the following documents:

Draft TS	Report on voting
121A/321/DTS	121A/331A/RVDTS

Full information on the voting for the approval of this Technical Specification 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.

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.

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

The growing use of data communication capabilities by switchgear and controlgear (called “equipment” in this document) automatically increases cybersecurity risks. In addition, information technology is more often interconnected to and even integrated into industrial systems which therefore, increase this risk.

Very often, switchgear, such as circuit-breakers, or controlgear, such as overload relays or proximity switches, are equipped with data communication interface. They can be connected to a logic controller or remote display, with local and remote connectivity for giving access to data such as actual power supply values, monitoring data, data logging and remote upgrade.

For these typical applications for electrical distribution and machinery, minimum cybersecurity requirements are needed for maintaining an acceptable level of safety integrity of the protection functions for equipment, with or without data communication capability. These requirements are intended to limit the vulnerability of the data communication interfaces. To keep the largest freedom of innovation, the relevant requirements for a defined application are determined preferably by a systematic risk assessment approach.

The intention of this document is to:

1) develop an awareness of cybersecurity risks associated with unintended operation and loss of protective functions;
2) provide minimum cybersecurity requirements for equipment to mitigate the likelihood of unintended operation and loss of protective functions in the context of electrical distribution installations and control systems of machinery;
3) provide guidance to avoid impairing the functionality of equipment, in all operating modes, as a consequence of the implementation of security countermeasures.

This document gives guidance on countermeasures applicable to the design of the equipment (hardware, firmware, network interface, access control, system) and on additional countermeasures to be considered for the implementation and instruction for use. This document uses relevant references to ISO/IEC 27001, IEC 62443 (all parts) and IEC 62351 (all parts).

As a first stage, the content of this document is intended to be referenced by product standards. The common security requirement of IEC SC 121A product standards are expected to be moved to a future edition of IEC 60947-1.

LOW-VOLTAGE SWITCHGEAR AND CONTROLGEAR – SECURITY ASPECTS

1 Scope

This document applies to the security related main functions of switchgear and controlgear during the whole lifecycle of the equipment. It is applicable to wired and wireless data communication means and the physical accessibility to the equipment, within its limits of environmental conditions.

This document is intended to develop awareness about security aspects and provides recommendations and requirements on the appropriate countermeasures against vulnerability to threats.

In particular, it focuses on potential vulnerabilities to threats resulting in:

– unintended operation of the switching device or the control device or sensor, which can lead to hazardous situations;

– unavailability of the protective functions (overcurrent, earth leakage, etc.).

This document does not cover security requirement for information technology (IT) and for industrial automation and control systems (IACS), but it only implements in switchgear and controlgear appropriate security countermeasures derived from the base security publication ISO/IEC 27001 and the group security publications IEC 62443 (all parts).

This document, as a product security publication, follows IEC Guide 120 and includes typical use case studies as given in Annex B.

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 60364-7-729, *Low-voltage electrical installations – Part 7-729: Requirements for special installations or locations – Operating or maintenance gangways*

IEC 60947-1:2020, *Low-voltage switchgear and controlgear – General rules*

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

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

IEC TR 63201:2019, *Low-voltage switchgear and controlgear – Guidance for the development of embedded software*

ISO/IEC 27001:2013, *Information technology – Security techniques – Information security management systems – Requirements*

FIPS 186-4, *Digital Signature Standard (DSS)*