IEC TS 63208

Edition 1.0 2020-03

TECHNICAL SPECIFICATION

colour inside

Low-voltage switchgear and controlgear – Security aspects

IEC TS 63208:2020-03(en)

IEC Central Office
3, rue de Varembé
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 It also gives information on projects, replaced and withdrawn publications.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.

Electropedia - www.electropedia.org
The world's leading online dictionary on electrotechnology, containing more than 22 000 terminological entries in English and French, with equivalent terms in 16 additional languages. Also known as the International Electrotechnical Vocabulary (IEV) online.

IEC Glossary - std.iec.ch/glossary
67 000 electrotechnical terminology entries in English and French extracted from the Terms and Definitions clause of IEC publications issued since 2002. Some entries have been collected from earlier publications of IEC TC 37, 77, 86 and CISPR.

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

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

CONTENTS

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)*

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

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

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

3.1.1
audit log
logs collecting the evidence of selected user activities, exceptions, and information security events

Note 1 to entry: These logs are kept for an agreed period of time to assist in future investigations.

Note 2 to entry: Audit logs can be used to comply with legal requirements.

[SOURCE: ISO/IEC 24775-2:2014, 3.1.7]

3.1.2
attack
attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset

[SOURCE: ISO/IEC 27000:2018, 3.2]

3.1.3
attack surface
set of attack points that an attacker can use in order to trigger an attack

[SOURCE: ISO/TS 12812-2:2017, 3.4, modified – "enter or capture data in an information system" replaced by "trigger an attack".]

3.1.4
attack vector
path or means by which an attacker can gain access to a device in order to generate an attack

[SOURCE: ISO/IEC 27032:2012, 4.10, modified – "computer or network server" replaced by "device" and "deliver a malicious outcome" by "generate an attack".]

3.1.5
authentication
security measure designed to establish the validity of a transmission, message, or originator

[SOURCE: IEC TS 62443-1-1:2009, 3.2.13, modified – Last part of the definition deleted.]

3.1.6
authenticity
property that an entity is what it claims to be

[SOURCE: ISO/IEC 27000:2018, 3.6]

3.1.7
authorization
right or permission that is granted to a system entity or an individual to access a system resource

[SOURCE: IEC TS 62443-1-1:2009, 3.2.14, modified – Addition of "or an individual".]

3.1.8
availability
property of being accessible and usable upon demand by an authorized entity

[SOURCE: ISO/IEC 27000:2018, 3.7]

3.1.9
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities or processes

[SOURCE: ISO/IEC 24767-1:2008, 2.1.2]

3.1.10
countermeasure
action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken

[SOURCE: IEC TS 62443-1-1:2009, 3.2.33, modified – Note deleted.]

3.1.11
cybersecurity
preservation of confidentiality, integrity and availability of information in the cyberspace

Note 1 to entry: The objective is to reduce the risk of causing personal injury or endangering public health, losing public or consumer confidence, disclosing sensitive assets, failing to protect business assets or failing to comply with regulations. These concepts are applied to any system in the production process and include both stand-alone and networked components. Communications between systems may be either through internal messaging or by any human or machine interfaces that authenticate, operate, control, or exchange data with any of these control systems. Cybersecurity includes the concepts of identification, authentication, accountability, authorization, availability, and privacy.

[SOURCE: ISO/IEC 27032:2012, 4.20, modified – Notes replaced with the Note to entry.]

3.1.12
data integrity
property that data has not been changed, destroyed, or lost in an unauthorized or accidental manner

Note 1 to entry: This term deals with constancy of and confidence in data values, not with the information that the values represent or the trustworthiness of the source of the values.

[SOURCE: IEC TS 62443-1-1:2009, 3.2.38]

3.1.13
defence in depth
provision of multiple security protections, especially in layers, with the intent to delay if not prevent an attack

Note 1 to entry: Defence in depth implies layers of security and detection, even on single systems, and provides the following features:

- attackers are faced with breaking through or bypassing each layer without being detected;

– a flaw in one layer can be mitigated by capabilities in other layers;

– a system security becomes a set of layers within the overall network security.

[SOURCE: IEC TS 62443-1-1:2009, 3.2.40]

3.1.14
system integrity
property that a system performs its intended function in an unimpaired manner, free from deliberate or accidental unauthorized manipulation

[SOURCE: ISO/TR 11633-2:2009, 2.14, modified – "of the system" deleted.]

3.1.15
denial of service
prevention of authorized access to resources or the delaying of time-critical operations

[SOURCE: ISO 7498-2:1989, 3.3.25]

3.1.16
hazardous situation
circumstance in which people, property or the environment is/are exposed to one or more hazards

[SOURCE: ISO/IEC Guide 51:2014, 3.4]

3.1.17
security audit
independent review and examination of a system's records and activities to determine the adequacy of system controls, ensure compliance with established security policy and procedures, detect breaches in security services, and recommend any changes that are indicated for countermeasures

[SOURCE: IEC TS 62443-1-1:2009, 3.2.101]

3.1.18
security related main function
<of switchgear and controlgear> function of switchgear and controlgear whose failure can result in its unwanted operation which can lead to hazardous situations, in the loss or the corruption of its protective function, or in the loss or the corruption of an extended functionality defined by the manufacturer

Note 1 to entry: When an additonal function such as energy monitoring of a circuit-breaker can be subject to attack leading to the corruption of the security related main function, such as the short-circuit protection, this additional function is considered as a secuity related main function.

3.1.19
threat
potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm

[SOURCE: IEC TS 62443-1-1:2009, 3.2.125]

3.1.20
security policy
set of rules that specify or regulate how a system or organization provides security services to protect its assets

[SOURCE: IEC TS 62443-1-1:2009, 3.2.112]

3.1.21
security vulnerability
weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat

[SOURCE: ISO/IEC TR 24772:2013, 3.1.5.3]

3.1.22
security risk assessment
process that systematically identifies potential vulnerabilities to valuable system resources and threats to those resources, quantifies loss exposures and consequences based on probability of occurrence, and (optionally) recommends how to allocate resources to countermeasures to minimize the exposure

[SOURCE: IEC TS 62443-1-1:2009, 3.2.88, modified – "total exposure" replaced by "the exposure" and notes deleted.]

3.1.23
smart manufacturing
domain of integrated products, processes and resources (cyber, physical, human) to create and deliver products and services, which also collaborates with other domains within an enterprise's value chains and continuously improves its performance aspects

Note 1 to entry: Performance aspects include agility, efficiency, safety, security, sustainability or any other performance indicators identified by the enterprise.

Note 2 to entry: In addition to manufacturing, other enterprise domains can include engineering, logistics, marketing, procurement, sales or any other domains identified by the enterprise.

3.2 Abbreviated terms

APN	access point name
BMS	building management systems
BT	Bluetooth® [1]
CCTV	closed circuit television
CF	communication functionalities
CVSS	common vulnerability scoring system
CRL	certificate revocation list
DNP	distributed network protocol
DMZ	demilitarized zone
DoS	denial of service
DDoS	distributed denial of service
EMC	electromagnetic compatibility
ERP	enterprise resource planning
HMI	human machine interface
HVAC	heating, ventilation, and air conditioning
ICS	industrial control system
IDS	intrusion detection system
IPS	intrusion prevention system

[1] Bluetooth® trademark is an example of a suitable communication protocol available commercially. This information is given for the convenience of users of this document and does not constitute an endorsement by IEC of this communication protocol.

IT	information technology
IoT	Internet of things
JTAG	debugging interface "Joint Test Action Group" according to IEEE 1149 (all parts)
LAN	local area network
MAC	media access control
MLP	multiprotocol label switching
NFC	near field communication
OT	operational technology
PLC	programmable logic controller
P2P	peer to peer connection
RBAC	role based access control
RS485	recommended standard 485 (according to TIA 485-A)
SCADA	supervisory control and data acquisition
SD card	secure digital card
SSL	secure socket layer
ULP	universal logic plug
USB	universal serial bus
VPN	virtual private network
WCI	wireless communication interface
WLAN	wide local area network

4 General

The integrity or the availability of the main functions of switchgear and controlgear may depend on physical security and cybersecurity aspects. The existing procedures for physically accessing equipment shall be considered as part of the security countermeasures together with the cybersecurity countermeasures.

5 Security objectives

In the context of electrical distribution with switchgear and machine control with controlgear (see Annex A), the overall security objectives are to ensure they operate as designed and configured and specially to avoid unintended operation and to protect its security related main functions.

The main security aspects to be considered are: data integrity, authenticity and availability. They should be detailed in terms of what needs to be protected and how this can be achieved. See Annex C for an overview of the relevant security aspects to be considered and Clause A.3 for security levels.

6 Security lifecycle management

6.1 General

The protections against security attacks should be determined based on the results of a risk assessment in order to identify the potential threats and vulnerabilities, and to define the countermeasures in a document called security requirements specification. It should cover each phase of the life cycle of the equipment and the relevant stakeholders, and it should take into account its physical access and the limits of its environmental conditions (see Figure 1 as an example).