

Information technology - Data centre facilities and
infrastructures - Part 2-5: Security systems

EESTI STANDARDI EESSÕNA

NATIONAL FOREWORD

See Eesti standard EVS-EN 50600-2-5:2016 sisaldab Euroopa standardi EN 50600-2-5:2016 ingliskeelset teksti.	This Estonian standard EVS-EN 50600-2-5:2016 consists of the English text of the European standard EN 50600-2-5:2016.
Standard on jõustunud sellekohase teate avaldamisega EVS Teatajas	This standard has been endorsed with a notification published in the official bulletin of the Estonian Centre for Standardisation.
Euroopa standardimisorganisatsioonid on teinud Euroopa standardi rahvuslikele liikmetele kättesaadavaks 25.03.2016.	Date of Availability of the European standard is 25.03.2016.
Standard on kättesaadav Eesti Standardikeskusest.	The standard is available from the Estonian Centre for Standardisation.

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile standardiosakond@evs.ee.

ICS 35.020, 35.110, 35.160

Standardite reprodutseerimise ja levitamise õigus kuulub Eesti Standardikeskusele

Andmete paljundamine, taastekitamine, kopeerimine, salvestamine elektroonsesse süsteemi või edastamine ükskõik millises vormis või millisel teel ilma Eesti Standardikeskuse kirjaliku loata on keelatud.

Kui Teil on küsimusi standardite autorikaitse kohta, võtke palun ühendust Eesti Standardikeskusega:

Aru 10, 10317 Tallinn, Eesti; koduleht www.evs.ee; telefon 605 5050; e-post info@evs.ee

The right to reproduce and distribute standards belongs to the Estonian Centre for Standardisation

No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, without a written permission from the Estonian Centre for Standardisation.

If you have any questions about copyright, please contact Estonian Centre for Standardisation:

Aru 10, 10317 Tallinn, Estonia; homepage www.evs.ee; phone +372 605 5050; e-mail info@evs.ee

ICS 35.020; 35.110; 35.160

English Version

Information technology - Data centre facilities and infrastructures - Part 2-5: Security systems

Technologie de l'information - Installation et infrastructures
de centres de traitement de données - Partie 2-5: Systèmes
de sécurité

Informationstechnik - Einrichtungen und Infrastrukturen von
Rechenzentren - Teil 2-5: Sicherungssysteme

This European Standard was approved by CENELEC on 2016-01-25. CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration.

Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CENELEC members are the national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.



European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Brussels

Contents

Page

European foreword.....	4
Introduction.....	5
1 Scope.....	8
2 Normative references.....	8
3 Terms, definitions and abbreviations	9
3.1 Terms and definitions	9
3.2 Abbreviations.....	10
4 Conformance	10
5 Physical security	10
5.1 General.....	10
5.2 Risk assessment.....	11
5.3 Designation of data centre spaces - Protection Classes	11
6 Protection Class against unauthorized access	12
6.1 General.....	12
6.2 Implementation	15
7 Protection Class against fire events igniting within data centre spaces	24
7.1 General.....	24
7.2 Implementation of Protection Class requirements	28
8 Protection Class against environmental events (other than fire) within data centre spaces	29
8.1 Protection Classes	29
8.2 Implementation	29
9 Protection Class against environmental events outside the data centre spaces	31
9.1 Protection Classes	31
9.2 Implementation	32
10 Systems to prevent unauthorized access	32
10.1 General.....	32
10.2 Technology.....	33
Annex A (informative) Pressure relief: Additional information	36
A.1 General.....	36
A.2 Design considerations	36
Bibliography.....	38

Figures

Figure 1 — Schematic relationship between the EN 50600 standards	6
Figure 2 — Risk assessment concepts	11
Figure 3 — Protection Classes within the 4-layer physical protection model	13
Figure 4 — Protection Class islands	14
Figure 5 — Interconnection between Protection Class islands	14
Figure 6 — Example of Protection Classes applied to data centre premises without external barriers	15
Figure 7 — Example of Protection Classes applied to data centre premises with external barriers	16

Tables

Table 1 — Examples of Protection Classes for data centre spaces	12
Table 2 — Protection Classes against unauthorized access	13
Table 3 — Protection Classes against internal fire events	24
Table 4 — Protection Classes against internal environmental events	29
Table 5 — Protection Classes against external environmental events	31
Table 6 — Elements of systems for the prevention of unauthorized access	33

European foreword

This document (EN 50600-2-5:2016) has been prepared by CLC/TC 215 “Electrotechnical aspects of telecommunication equipment”.

The following dates are fixed:

- latest date by which this document has to (dop) 2017-01-25
be implemented at national level by
publication of an identical national standard
or by endorsement
- latest date by which the national standards (dow) 2019-01-25
conflicting with this document have to be
withdrawn

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC [and/or CEN] shall not be held responsible for identifying any or all such patent rights.

This document has been prepared under a mandate given to CENELEC by the European Commission and the European Free Trade Association.

Regarding the various parts in the EN 50600 series, see the Introduction.

Introduction

The unrestricted access to internet-based information demanded by the information society has led to an exponential growth of both internet traffic and the volume of stored/retrieved data. Data centres are housing and supporting the information technology and network telecommunications equipment for data processing, data storage and data transport. They are required both by network operators (delivering those services to customer premises) and by enterprises within those customer premises.

Data centres need to provide modular, scalable and flexible facilities and infrastructures to easily accommodate the rapidly changing requirements of the market. In addition, energy consumption of data centres has become critical both from an environmental point of view (reduction of carbon footprint) and with respect to economical considerations (cost of energy) for the data centre operator.

The implementation of data centres varies in terms of:

- a) purpose (enterprise, co-location, co-hosting, or network operator);
- b) security level;
- c) physical size;
- d) accommodation (mobile, temporary and permanent constructions).

The needs of data centres also vary in terms of availability of service, the provision of security and the objectives for energy efficiency. These needs and objectives influence the design of data centres in terms of building construction, power distribution, environmental control and physical security. Effective management and operational information is required to monitor achievement of the defined needs and objectives.

This series of European Standards specifies requirements and recommendations to support the various parties involved in the design, planning, procurement, integration, installation, operation and maintenance of facilities and infrastructures within data centres. These parties include:

- 1) owners, facility managers, ICT managers, project managers, main contractors;
- 2) architects, consultants, building designers and builders, system and installation designers;
- 3) facility and infrastructure integrators, suppliers of equipment;
- 4) installers, maintainers.

At the time of publication of this European Standard, the EN 50600 series currently comprises the following standards:

- EN 50600-1, *Information technology — Data centre facilities and infrastructures — Part 1: General concepts*;
- EN 50600-2-1, *Information technology — Data centre facilities and infrastructures — Part 2-1: Building construction*;
- EN 50600-2-2, *Information technology — Data centre facilities and infrastructures — Part 2-2: Power distribution*;
- EN 50600-2-3, *Information technology — Data centre facilities and infrastructures — Part 2-3: Environmental control*;

- EN 50600-2-4, *Information technology — Data centre facilities and infrastructures — Part 2-4: Telecommunications cabling infrastructure*;
- EN 50600-2-5, *Information technology — Data centre facilities and infrastructures — Part 2-5: Security systems*;
- EN 50600-3-1, *Information technology — Data centre facilities and infrastructures — Part 3-1: Management and operational information*;
- FprEN 50600-4-1, *Information technology — Data centre facilities and infrastructures — Part 4-1: Overview of and general requirements for key performance indicators*;
- FprEN 50600-4-2, *Information technology — Data centre facilities and infrastructures — Part 4-2: Power Usage Effectiveness*;
- FprEN 50600-4-3, *Information technology — Data centre facilities and infrastructures — Part 4-3: Renewable Energy Factor*;
- CLC/TR 50600-99-1, *Information technology — Data centre facilities and infrastructures — Part 99-1: Recommended practices for energy management*.

The inter-relationship of the standards within the EN 50600 series is shown in Figure 1.

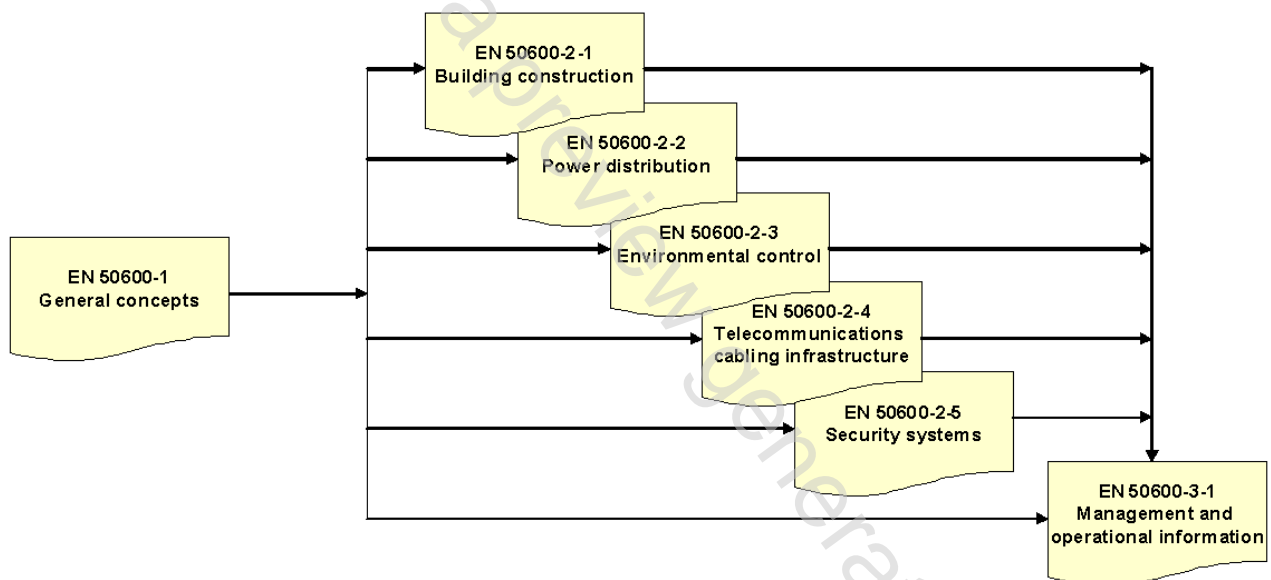


Figure 1 — Schematic relationship between the EN 50600 standards

EN 50600-2-X standards specify requirements and recommendations for particular facilities and infrastructures to support the relevant classification for “availability”, “physical security” and “energy efficiency enablement” selected from EN 50600-1.

EN 50600-3-X documents specify requirements and recommendations for data centre operations, processes and management.

This European Standard addresses the physical security of facilities and infrastructure within data centres together with the interfaces for monitoring the performance of those facilities and infrastructures in line EN 50600-3-1 (in accordance with the requirements of EN 50600-1).

This European Standard is intended for use by and collaboration between architects, building designers and builders, system and installation designers and security managers among others.

This series of European Standards does not address the selection of information technology and network telecommunications equipment, software and associated configuration issues.

This document is a preview generated by EVS

1 Scope

This European Standard addresses the physical security of data centres based upon the criteria and classifications for “availability”, “security” and “energy efficiency enablement” within EN 50600-1.

This European Standard provides designations for the data centres spaces defined in EN 50600-1.

This European Standard specifies requirements and recommendations for those data centre spaces, and the systems employed within those spaces, in relation to protection against:

- a) unauthorized access addressing constructional, organizational and technological solutions;
- b) fire events igniting within data centres spaces;
- c) other events within or outside the data centre spaces, which would affect the defined level of protection.

Safety and electromagnetic compatibility (EMC) requirements are outside the scope of this European Standard and are covered by other standards and regulations. However, information given in this European Standard may be of assistance in meeting these standards and regulations.

2 Normative references

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

EN 3 (all parts), *Portable fire extinguishers*

EN 54 (all parts), *Fire detection and fire alarm systems*

EN 54-13, *Fire detection and fire alarm systems — Part 13: Compatibility assessment of system components*

EN 54-20:2006, *Fire detection and fire alarm systems — Part 20: Aspirating smoke detectors*

EN 1047-2, *Secure storage units — Classification and methods of test for resistance to fire — Part 2: Data rooms and data container*

EN 1366-3, *Fire resistance tests for service installations — Part 3: Penetration seals*

EN 1627:2011, *Pedestrian doorsets, windows, curtain walling, grilles and shutters — Burglar resistance — Requirements and classification*

EN 1634 (all parts), *Fire resistance and smoke control tests for door and shutter assemblies, openable windows and elements of building hardware*

EN 12845, *Fixed firefighting systems — Automatic sprinkler systems — Design, installation and maintenance*

EN 13565-2, *Fixed firefighting systems — Foam systems — Part 2: Design, construction and maintenance*

CEN/TS 14816, *Fixed firefighting systems — Water spray systems — Design, installation and maintenance*

CEN/TS 14972, *Fixed firefighting systems — Watermist systems — Design and installation*

prEN 16750, *Fixed firefighting systems — Oxygen reduction systems — Design, installation, planning and maintenance*

EN 50131 (all parts), *Alarm systems — Intrusion and hold-up systems*

EN 50136 (all parts), *Alarm systems — Alarm transmission systems and equipment*

EN 50518 (all parts), *Monitoring and alarm receiving centre*

EN 50600-1, *Information technology — Data centre facilities and infrastructures — Part 1: General concepts*

EN 50600-2-1:2014, *Information technology — Data centre facilities and infrastructures — Part 2-1: Building construction*

EN 50600-2-2, *Information technology — Data centre facilities and infrastructures — Part 2-2: Power distribution*

EN 50600-2-3, *Information technology — Data centre facilities and infrastructures — Part 2-3: Environmental control*

EN 50600-2-4, *Information technology — Data centre facilities and infrastructures — Part 2-4: Telecommunications cabling infrastructure*

EN 60839-11-1, *Alarm and electronic security systems — Part 11-1: Electronic access control systems — System and components requirements (IEC 60839-11-1)*

EN 62676-1-1:2014, *Video surveillance systems for use in security applications — Part 1-1: System requirements — General (IEC 62676-1-1:2014)*

3 Terms, definitions and abbreviations

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in EN 50600-1 and the following apply.

3.1.1

forcible threat

threat exhibited by physical force

3.1.2

hold time

time during which a concentration of fire extinguishant is maintained at an effective level with the space being protected

3.1.3

information technology equipment

equipment providing data storage, processing and transport services together with equipment dedicated to providing direct connection to core and/or access networks

3.1.4

residual risk

remaining risk(s) posed to the data centre assets requiring protection following the deployment of appropriate countermeasures

3.1.5

security manager

individual with overall responsible for all operational security aspects of the data centre, including logical and physical control mechanisms or processes