This document is a preview generated by EVS

INFOTEHNOLOOGIA. ANDMEKESKUSE RAJATISED JA TARISTUD. OSA 2-5: TURVASÜSTEEMID

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

EESTI STANDARDI EESSÕNA

NATIONAL FOREWORD

This document is a preview generated by EVS

See Eesti standard EVS-EN 50600-2-5:2021 sisaldab Euroopa standardi EN 50600-2-5:2021 ingliskeelset teksti.	This Estonian standard EVS-EN 50600-2-5:2021 consists of the English text of the European standard EN 50600-2-5:2021.
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 and Accreditation.
Euroopa standardimisorganisatsioonid on teinud Euroopa standardi rahvuslikele liikmetele kättesaadavaks 16.04.2021.	Date of Availability of the European standard is 16.04.2021.
Standard on kättesaadav Eesti Standardimis- ja Akrediteerimiskeskusest.	The standard is available from the Estonian Centre for Standardisation and Accreditation.

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 Standardimis- ja Akrediteerimiskeskusele

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

Kui Teil on küsimusi standardite autoriõiguse kaitse kohta, võtke palun ühendust Eesti Standardimis- ja Akrediteerimiskeskusega: 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 and Accreditation

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 and Accreditation.

If you have any questions about standards copyright protection, please contact the Estonian Centre for Standardisation and Accreditation: Homepage www.evs.ee; phone +372 605 5050; e-mail info@evs.ee

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN 50600-2-5

April 2021

ICS 35.020; 35.110; 35.160

Supersedes EN 50600-2-5:2016 and all of its amendments and corrigenda (if any)

English Version

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

Technologie de l'information - Installations 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 2021-03-22. 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, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, 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: Rue de la Science 23, B-1040 Brussels

© 2021 CENELEC All rights of exploitation in any form and by any means reserved worldwide for CENELEC Members.

Ref. No. EN 50600-2-5:2021 E

This document is a preview generated by EVS

Contents

Page

European foreword **5**
Introduction **6**
1 Scope **9**
2 Normative references **9**
3 Terms, definitions and abbreviations **10**
3.1 Terms and definitions 10
3.2 Abbreviations 11
4 Conformance **11**
5 Physical security **12**
5.1 General 12
5.2 Risk analysis and management 12
5.3 Designation of data centre spaces: Protection Classes 13
6 Protection against unauthorized access **13**
6.1 General 13
6.1.1 Data centre configuration 13
6.1.2 Protection Classes 14
6.1.3 Protection Classes of specific infrastructures 16
6.1.4 Levels for access control 16
6.2 Access to the data centre premises 17
6.2.1 Premises with external physical barriers 17
6.2.2 Premises without external physical barriers 18
6.2.3 Roofs 19
6.2.4 Access routes 19
6.2.5 Parking 19
6.2.6 Employees and visitors 20
6.2.7 Pathways 20
6.2.8 Cabinets, racks and frames 21
6.3 Implementation 21
6.3.1 Protection Class 1 21
6.3.2 Protection Class 2 22
6.3.3 Protection Class 3 22
6.3.4 Protection Class 4 23
7 Protection against intrusion to data centre spaces **24**
7.1 General 24
7.2 Level for the detection of intrusion 24
7.3 Implementation 24
7.3.1 Protection Class 1 24
7.3.2 Protection Class 2 25
7.3.3 Protection Class 3 26
7.3.4 Protection Class 4 26

This document is a preview generated by EVS

8 Protection against fire events igniting within data centre spaces 27
8.1 General 27
8.1.1 Protection Classes 27
8.1.2 Fire compartments and barriers 28
8.1.3 Fire detection and fire alarm systems 28
8.1.4 Fixed firefighting systems 28
8.1.5 Portable firefighting equipment 30
8.2 Implementation 31
8.2.1 Protection Class 1 31
8.2.2 Protection Class 2 31
8.2.3 Protection Class 3 31
8.2.4 Protection Class 4 31
9 Protection against environmental events (other than fire) within data centre spaces 31
9.1 General 31
9.2 Implementation 32
9.2.1 Protection Class 1 32
9.2.2 Protection Class 2 32
9.2.3 Protection Class 3 32
9.2.4 Protection Class 4 32
10 Protection against environmental events outside the data centre spaces 33
10.1 General 33
10.2 Implementation 34
10.2.1 Protection Class 1 34
10.2.2 Protection Class 2 34
10.2.3 Protection Class 3 34
11 Systems to prevent unauthorized access and intrusion 34
11.1 General 34
11.2 Technology 35
11.2.1 Security lighting 35
11.2.2 Video surveillance systems 36
11.2.3 Intruder and holdup alarm systems 37
11.2.4 Access control systems 37
11.2.5 Event and alarm monitoring 37
Annex A (informative) **Pressure relief: Additional information 38**
A.1 General 38
A.2 Design considerations 38
Bibliography 40

Figures

Figure 1 — Schematic relationship between the EN 50600 standards 7
Figure 2 — Risk analysis and management concepts 13
Figure 3 — Protection Classes within the 4-layer physical protection model 15

This document is a preview generated by EVS

Figure 4 — Protection Class islands 15
Figure 5 — Connections between Protection Class islands 16
Figure 6 — Example of Protection Classes applied to data centre premises with external barriers 18
Figure 7 — Example of Protection Classes applied to data centre premises without external barriers 19

Tables

Table 1 — Protection Classes against unauthorized access 14
Table 2 — Options for access control 17
Table 3 — Options for intrusion detection 24
Table 4 — Protection Classes against internal fire events 27
Table 5 — Protection Classes against internal environmental events 31
Table 6 — Protection Classes against external environmental events 33
Table 7 — Elements of systems for the prevention of unauthorized access 35

This document is a preview generated by EVS

European foreword

This document (EN 50600-2-5:2021) 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 be implemented at national level by publication of an identical national standard or by endorsement (dop) 2022-03-22
- latest date by which the national standards conflicting with this document have to be withdrawn (dow) 2024-03-22

This document supersedes EN 50600-2-5:2016 and all of its amendments and corrigenda (if any).

This document includes the following significant technical changes with respect to EN 50600-2-5:2016:

a) technical update to all clauses in response to user feedback;

b) new Clause 7 on Protection Classes against intrusion to data centre spaces added and Clause 6 restructured accordingly;

c) references to relevant provisions of EN 50600-2-1:2021 added to highlight the respective links to constructional requirements;

d) various editorial updates.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CENELEC 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.

This document is a preview generated by EVS

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 usually 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 environmental 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, telecommunications cabling and physical security as well as the operation of the data centre. Effective management and operational information is important in order to monitor achievement of the defined needs and objectives.

Recognizing the substantial resource consumption, particularly of energy, of larger data centres, it is also important to provide tools for the assessment of that consumption both in terms of overall value and of source mix and to provide Key Performance Indicators (KPIs) to evaluate trends and drive performance improvements.

At the time of publication of this document, the EN 50600 series is designed as a framework of standards, technical specifications and technical reports covering the design, the operation and management, the key performance indicators for energy efficient operation of the data centre as well as a data centre maturity model.

The EN 50600-2 series defines the requirements for the data centre design.

The EN 50600-3 series defines the requirements for the operation and the management of the data centre.

The EN 50600-4 series defines the key performance indicators for the data centre.

The CLC/TS 50600-5 series defines the data centre maturity model requirements and recommendations.

The CLC/TR 50600-99-X Technical Reports cover recommended practices and guidance for specific topics around data centre operation and design.

This series of documents 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, operators, facility managers, ICT managers, project managers, main contractors;

2) consulting engineers, architects, building designers and builders, system and installation designers, auditors, test and commissioning agents;

3) facility and infrastructure integrators, suppliers of equipment;

4) installers, maintainers.

This document is a preview generated by EVS

At the time of publication of this document, the EN 50600-2 series comprises the following documents:

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 supply and 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*;

CLC/TS 50600-2-10, *Information technology — Data centre facilities and infrastructures — Part 2-10: Earthquake risk and impact analysis;*

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

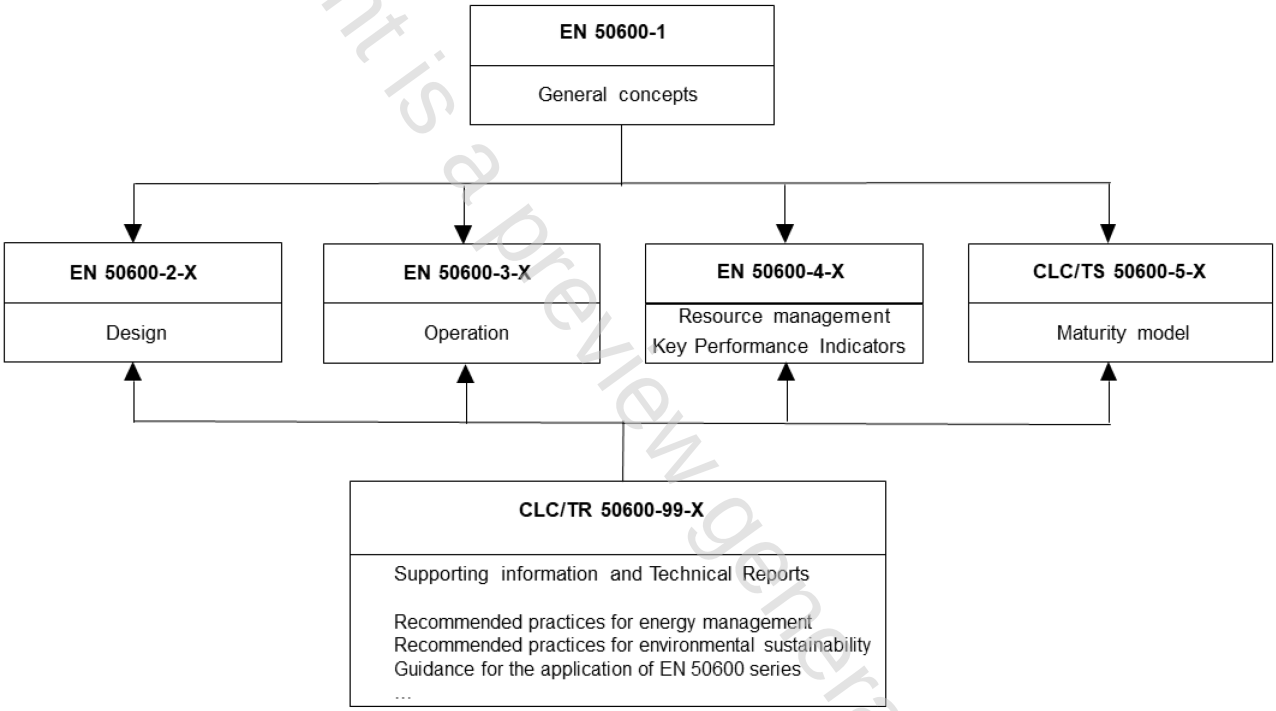

Figure 1 — Schematic relationship between the EN 50600 standards

EN 50600-2-X documents 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.

EN 50600-4-X documents specify requirements and recommendations for key performance indicators (KPIs) used to assess and improve the resource usage efficiency and effectiveness, respectively, of a data centre.

This document 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 with EN 50600-3-1 (in accordance with the requirements of EN 50600-1).

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

This document is a preview generated by EVS

This series of documents 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 document 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 document provides designations for the data centres spaces defined in EN 50600-1.

This document 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 organizational and technological solutions;

b) intrusion;

c) fire events igniting within data centres spaces;

d) environmental events (other than fire) within the data centre spaces which would affect the defined level of protection;

e) environmental events outside the data centre spaces which would affect the defined level of protection.

NOTE Constructional requirements and recommendations are provided by reference to EN 50600-2-1.

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

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.

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

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

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

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*

EN 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, *Monitoring and Alarm Receiving Centre*

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

This document is a preview generated by EVS

EN 50600-2-1:2021, *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 supply and 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 60839-11-2, *Alarm and electronic security systems — Part 11-2: Electronic access control systems - Application guidelines (IEC 60839-11-2)*

EN 62305 (series), *Protection against lightning (IEC 62305 series)*

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

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.

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/

3.1.1
authorized person
person having been assessed and subsequently provided with access credentials to specific areas within the data centre

3.1.2
forcible threat
threat exhibited by physical force

3.1.3
frame
open construction, typically wall-mounted, for housing closures and other information technology equipment

[SOURCE: EN 50174-1:2018, 3.1.21]

3.1.4
free-standing barrier
wall, fence, gate, turnstile or other similar self-supporting barrier, and their associated foundations, designed to prevent entry to a space of a given Protection Class

[SOURCE: EN 50600-2-1:2021, 3.1.2]

This document is a preview generated by EVS