SLOVENSKI STANDARD
oSIST prEN 50600-2-5:2020

01-julij-2020

Informacijska tehnologija - Naprave in infrastruktura podatkovnih centrov - 2-5. del: Varnostni sistemi

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

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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

kSIST FprEN 50600-2-5:2021
https://standards.iteh.ai/catalog/standards/sist/32a6b1c0-9c11-4b7a-b753-db2027595089/ksist-fpren-50600-2-5-2021

Ta slovenski standard je istoveten z: **prEN 50600-2-5**

ICS:

35.030	Informacijska varnost	IT Security

oSIST prEN 50600-2-5:2020 **en,fr**

2003-01.Slovenski inštitut za standardizacijo. Razmnoževanje celote ali delov tega standarda ni dovoljeno.

oSIST prEN 50600-2-5:2020

iTeh STANDARD PREVIEW
(standards.iteh.ai)

kSIST FprEN 50600-2-5:2021
https://standards.iteh.ai/catalog/standards/sist/32a6b1c0-9c11-4b7a-b753-db2027595089/ksist-fpren-50600-2-5-2021

oSIST prEN 50600-2-5:2020

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

DRAFT
prEN 50600-2-5

May 2020

ICS

Will supersede 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 draft European Standard is submitted to CENELEC members for enquiry.
Deadline for CENELEC: 2020-08-07.

It has been drawn up by CLC/TC 215.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

If this draft becomes a European Standard, 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.

This draft European Standard was established by CENELEC 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.

SIST FprEN 50600-2-5:2021
https://standards.iteh.ai/catalog/standards/sist/32a6b1a0-9c1d-4b7a-b753-

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.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Warning : This document is not a European Standard. It is distributed for review and comments. It is subject to change without notice and shall not be referred to as a European Standard.

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

© 2020 CENELEC All rights of exploitation in any form and by any means reserved worldwide for CENELEC Members.

oSIST prEN 50600-2-5:2020

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 11
5.1 General 11
5.2 Risk analysis and management 12
5.3 Designation of data centre spaces: Protection Classes 13
6 Protection Class against unauthorized access 13
6.1 General 13
6.1.1 Data centre configuration 13
6.1.2 Protection Classes 13
6.1.3 Protection Classes of specific infrastructures 16
6.1.4 Technical solutions to prevent unauthorized access 16
6.2 Access to the data centre premises 16
6.2.1 Premises with external physical barriers 16
6.2.2 Premises without external physical barriers 17
6.2.3 Roofs 18
6.2.4 Access routes 18
6.2.5 Parking 18
6.2.6 Employees and visitors 19
6.2.7 Pathways 19
6.2.8 Cabinets, racks and frames 20
6.3 Implementation 20
6.3.1 Protection Class 1 20
6.3.2 Protection Class 2 21
6.3.3 Protection Class 3 21
6.3.4 Protection Class 4 22
7 Protection Class against intrusion to data centre spaces 23
7.1 General 23
7.2 Technical solutions for the detection of intrusion 23
7.3 Implementation 23
7.3.1 Protection Class 1 23
7.3.2 Protection Class 2 24
7.3.3 Protection Class 3 24
7.3.4 Protection Class 4 25

iTeh STANDARD PREVIEW
(standards.iteh.ai)
kSIST FprEN 50600-2-5:2021
https://standards.iteh.ai/catalog/standards/sist/32a6b1c0-9c11-4b7a-b753-
ksist-fpren-50600-2-5-2021

oSIST prEN 50600-2-5:2020

8 Protection Class against fire events igniting within data centre spaces 25
8.1 General 25
8.1.1 Protection Classes 25
8.1.2 Fire compartments and barriers 26
8.1.3 Fire detection and fire alarm systems 27
8.1.4 Fixed firefighting systems 27
8.1.5 Portable firefighting equipment 29
8.2 Implementation 29
8.2.1 Protection Class 1 29
8.2.2 Protection Class 2 29
8.2.3 Protection Class 3 29
8.2.4 Protection Class 4 29
9 Protection Class against environmental events (other than fire) within data centre spaces 30
9.1 General 30
9.2 Implementation 30
9.2.1 Protection Class 1 30
9.2.2 Protection Class 2 30
9.2.3 Protection Class 3 31
9.2.4 Protection Class 4 31
10 Protection Class against environmental events outside the data centre spaces 32
10.1 General 32
10.2 Implementation 32
10.2.1 Protection Class 1 32
10.2.2 Protection Class 2 32
10.2.3 Protection Class 3 33
11 Systems to prevent unauthorized access and intrusion 33
11.1 General 33
11.2 Technology 34
11.2.1 Security lighting 34
11.2.2 Video surveillance systems 34
11.2.3 Intruder and holdup alarm systems 35
11.2.4 Access control 36
11.2.5 Alarm monitoring 36
Annex A (informative) **Pressure relief: Additional information 37**
A.1 General 37
A.2 Design considerations 37
Bibliography 39

Figures

Figure 1 — Schematic relationship between the EN 50600 standards 7
Figure 2 — Risk analysis and management concepts 12
Figure 3 — Protection Classes within the 4-layer physical protection model 14

iTeh STANDARD PREVIEW
(standards.iteh.ai)
kSIST FprEN 50600-2-5:2021
https://standards.iteh.ai/catalog/standards/sist/32a6b1c0-9c11-4b7a-b753-db2027595089/ksist-fpren-50600-2-5-2021

oSIST prEN 50600-2-5:2020

Figure 4 — Protection Class islands 15
Figure 5 — Connections between Protection Class islands 15
Figure 6 — Example of Protection Classes applied to data centre premises with external barriers 17
Figure 7 — Example of Protection Classes applied to data centre premises without external barriers 18

Tables

Table 1 — Protection Classes against unauthorized access 14
Table 2 — Technical solutions for access control 16
Table 3 — Technical solutions for intrusion detection 23
Table 4 — Protection Classes against internal fire events 26
Table 5 — Protection Classes against internal environmental events 30
Table 6 — Protection Classes against external environmental events 32
Table 7 — Elements of systems for the prevention of unauthorized access 33

iTeh STANDARD PREVIEW
(standards.iteh.ai)
kSIST FprEN 50600-2-5:2021
https://standards.iteh.ai/catalog/standards/sist/32a6b1c0-9c11-4b7a-b753-db2027595089/ksist-fpren-50600-2-5-2021

oSIST prEN 50600-2-5:2020

European foreword

This document (prEN 50600-2-5:2020) has been prepared by CLC/TC 215 “Electrotechnical aspects of telecommunication equipment”.

This document is currently submitted to the Enquiry.

The following dates are proposed:

• latest date by which the existence of this document has to be announced at national level	(doa)	dor + 6 months
• latest date by which this document has to be implemented at national level by publication of an identical national standard or by endorsement	(dop)	dor + 12 months
• latest date by which the national standards conflicting with this document have to be withdrawn	(dow)	dor + 36 months (to be confirmed or modified when voting)

This document will supersede 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:

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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;

kSIST FprEN 50600-2-5:2021
https://standards.iteh.ai/catalog/standards/sist/32a6b1c0-9c11-4b7a-b753-

c) references to relevant provisions of prEN 50600-2-1:2020 added to highlight the respective links to constructional requirements;

d) various editorial updates.

oSIST prEN 50600-2-5:2020

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 imperative in order to monitor achievement of the defined needs and objectives.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

This series 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:

kSIST FprEN 50600-2-5:2021
https://standards.iteh.ai/catalog/standards/sist/32a6b1a0-0c11-4b7a-b753-db27b75050f9/ksist-fpren-50600-2-5-2021

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 document, 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 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*;

oSIST prEN 50600-2-5:2020

— 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*;

— EN 50600-4-1, *Information technology — Data centre facilities and infrastructures — Part 4-1: Overview of and general requirements for key performance indicators*;

— EN 50600-4-2, *Information technology — Data centre facilities and infrastructures — Part 4-2: Power Usage Effectiveness*;

— EN 50600-4-3, *Information technology — Data centre facilities and infrastructures — Part 4-3: Renewable Energy Factor*;

— EN 50600-4-6, *Information technology — Data centre facilities and infrastructures — Part 4-6: Energy Reuse Factor*;

— EN 50600-4-7, *Information technology — Data centre facilities and infrastructures — Part 4-7: Cooling Efficiency Ratio*;

— CLC/TR 50600-99-1, *Information technology — Data centre facilities and infrastructures — Part 99-1: Recommended practices for energy management*;

— CLC/TR 50600-99-2, *Information technology — Data centre facilities and infrastructures — Part 99-2: Recommended practices for environmental sustainability*;

— CLC/TR 50600-99-3, *Information technology — Data centre facilities and infrastructures — Part 99-3: Guidance for the application of EN 50600 series*.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
kSIST FprEN 50600-2-5:2021
https://standards.iteh.ai/catalog/standards/sist/32a6b1c0-9c11-4b7a-b753-db2027595089/ksist-fpren-50600-2-5-2021

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

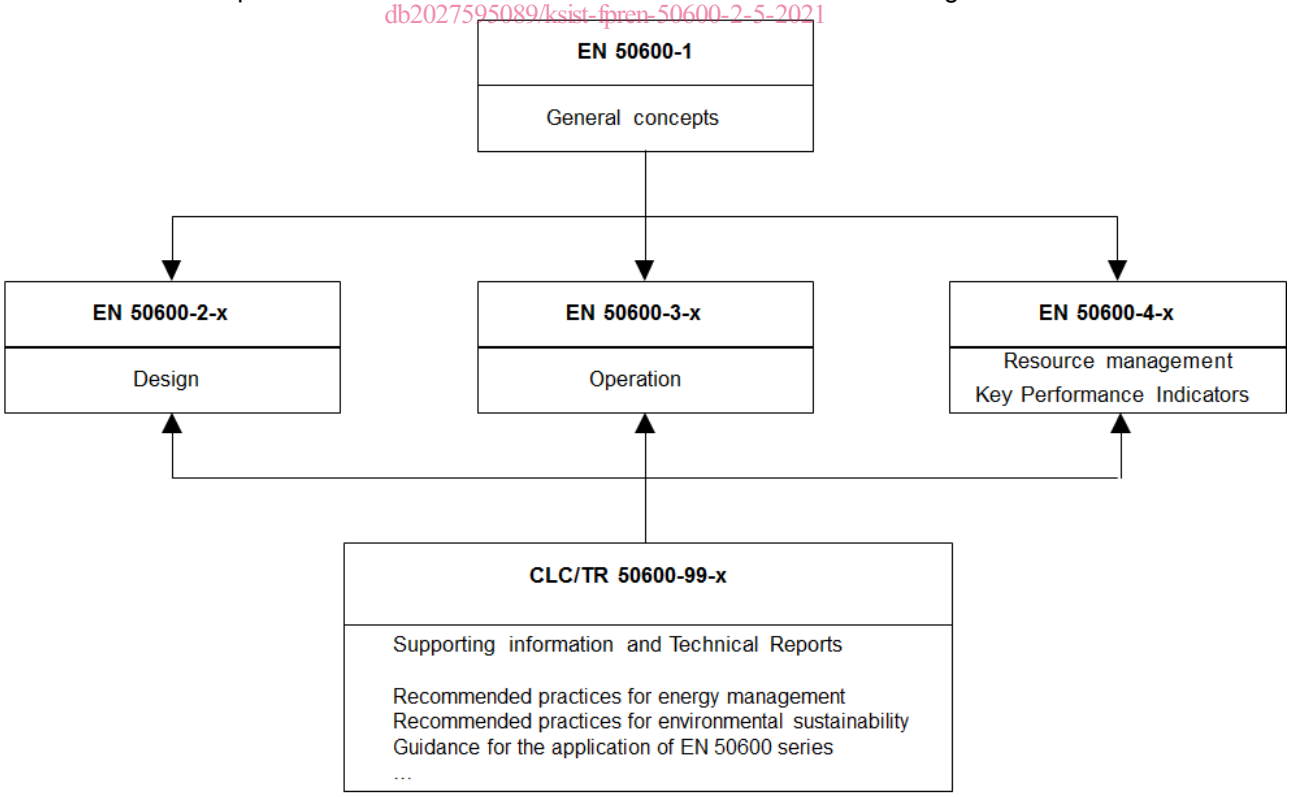

Figure 1 — Schematic relationship between the EN 50600 standards

oSIST prEN 50600-2-5:2020

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.

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
kSIST FprEN 50600-2-5:2021
https://standards.iteh.ai/catalog/standards/sist/32a6b1c0-9c11-4b7a-b753-db2027595089/ksist-fpren-50600-2-5-2021

oSIST prEN 50600-2-5:2020

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) other events within or 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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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.

kSIST FprEN 50600-2-5:2021
https://standards.iteh.ai/catalog/standards/sist/32a6b1c0-9c11-4b7a-b753-db2027595089/ksist-fpren-50600-2-5-2021

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*

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

oSIST prEN 50600-2-5:2020

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*

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

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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

SIST prEN 50600-2-5:2020
https://standards.iteh.ai/catalog/standards/sist/32a6b1c0-9c11-4b7a-b753-

— IEC Electropedia: available at http://www.electropedia.org/

-5-2021

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: prEN 50600-2-1:2020, 3.1.2]

3.1.5
hold time
time during which a concentration of fire extinguishant is maintained at an effective level with the space being protected

oSIST prEN 50600-2-5:2020

3.1.6
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

3.1.7
make-up air
air introduced into a data centre space to replace air that is exhausted through ventilation or combustion processes

[SOURCE: CLC/TR 50600-99-1:2019, 3.1.18]

3.1.8
rack
open construction, typically self-supporting and floor-mounted, for housing closures and other information technology equipment

[SOURCE: EN 50174-1:2018, 3.1.34]

3.1.9
residual risk
remaining risk(s) posed to the data centre assets requiring protection following the deployment of appropriate countermeasures

3.1.10
surreptitious attack
compromise of an asset via logical or physical means with the objective that the attack remains undetected

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3.1.11
surreptitious threat
threat of a surreptitious attack by entities via logical or physical means leading to the compromise of that asset

kSIST FprEN 50600-2-5:2021
https://standards.iteh.ai/catalog/standards/sist/52a661e0-9c11-4b7a-b755-db2027595089/ksist-fpren-50600-2-5-2021

3.2 Abbreviations

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

I&HAS intruder and holdup alarm systems

VSS video surveillance system

4 Conformance

For a data centre to conform to this document

1) the required Protection Class of Clause 5 shall be applied to each of the spaces of the data centre;

2) the requirements of the relevant Protection Class of Clauses 6, 7, 8, 9 and 10 shall be applied;

3) the systems to support the requirements of Clause 6 shall be in accordance with Clause 11.

5 Physical security

5.1 General

The degree of physical security applied to the facilities and infrastructures of a data centre has an influence on both the availability of function of, and the integrity/security of the data stored and processed within, the data centre.