SLOVENSKI STANDARD
oSIST prEN 50600-2-5:2014

01-julij-2014

Informacijska tehnologija - Podatkovni centri in infrastruktura - 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

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

Ta slovenski standard je istoveten z: **prEN 50600-2-5:2014**

ICS:

35.110	Omreževanje	Networking

oSIST prEN 50600-2-5:2014 **en**

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

DRAFT
prEN 50600-2-5

May 2014

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 draft European Standard is submitted to CENELEC members for enquiry.
Deadline for CENELEC: 2014-10-10.

It has been drawn up by CLC/TC 215.

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.

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.

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: Avenue Marnix 17, B-1000 Brussels

Project: 23546 Ref. No. prEN 50600-2-5:2014 E

Contents

36 **Figures**

44 **Tables**

55

Foreword

This document (prEN 50600-2-5:2014) has been prepared by CLC/TC 215 "Electrotechnical aspects of telecommunication equipment".

This document is currently submitted to the Enquiry.

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

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, housing and supporting the information technology and network telecommunications equipment for data processing, data storage and data transport are required both by network operators (delivering those services to customer premises) and by enterprises within those customer premises.

Data centres need to provide scalable and flexible 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 (greenhouse gas emission) 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, network operator or mixed use facilities);

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:

a) owners, facility managers, ICT managers, project managers, main contractors;

b) architects, building designers and builders, system and installation designers;

c) facility and infrastructure integrators, suppliers of equipment;

d) installers, maintainers.

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

EN 50600-1: *Data centre facilities and infrastructures - Part 1: General concepts*

EN 50600-2-1: *Data centre facilities and infrastructures - Part 2-1: Building construction*

EN 50600-2-2: *Data centre facilities and infrastructures - Part 2-2: Power distribution*

EN 50600-2-3: *Data centre facilities and infrastructures - Part 2-3: Environmental control*

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

EN 50600-2-5: *Data centre facilities and infrastructures - Part 2-5: Security systems*

EN 50600-2-6: *Data centre facilities and infrastructures - Part 2-6: Management and operational information*

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

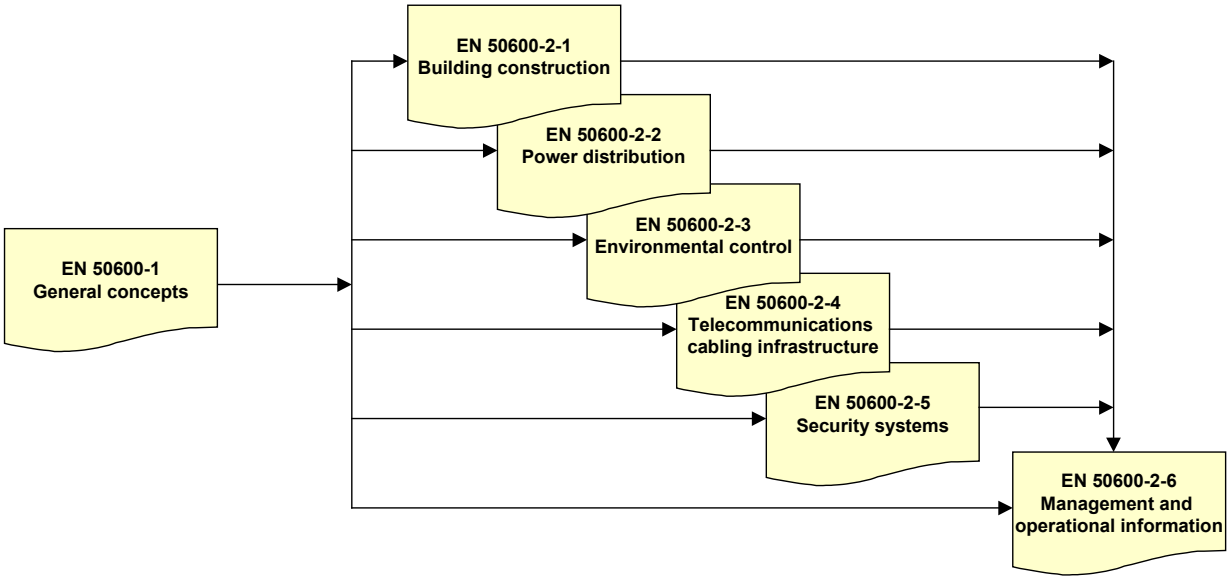

Figure 1 - Schematic relationship between the EN 50600 standards

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.

This European Standard addresses the security systems for facilities and infrastructure within data centres together with the interfaces for monitoring the performance of those facilities and infrastructures in line EN 50600-2-6 (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.

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 security systems employed within those spaces, in relation to protection against:

a) unauthorised access addressing constructional, organisational and technological solutions;

b) fire events internal to the data centre spaces;

c) other environmental events, other than fire, and including electromagnetic interference, vibration, flooding, gas and dust hazards which may exist

- internal to the data centre spaces;
- external to the data centre spaces.

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 54-2, *Fire detection and fire alarm systems – Part 2: Control and indicating equipment*

EN 54-7, *Fire detection and fire alarm systems – Part 7: Smoke detectors - Point detectors using scattered light, transmitted light or ionization*

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

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

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

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 [1], *Information Technology - Data centre facilities and infrastructures - Part 2-3: Environmental control*

EN 50600-2-4 [2], Information *Technology - Data centre facilities and infrastructures - Part 2-4: Telecommunications cabling infrastructure*

---

1) Draft for formal vote under preparation.

2) Circulated for CENELEC enquiry.

3 Terms, definitions and abbreviations

3.1 Terms and definitions

For the purposes of this document the definitions of EN 50600-1:2012 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 shall be maintained at an effective level with the space being protected. The predicted hold time shall be determined by the door fan test or a full discharge test

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

3.1.6
surreptitious attack
compromise of an asset via logical or physical means with the objective that the attack remains undetected

3.1.7
surreptitious threat
threat of a surreptitious attack by entities via logical or physical means leading to the compromise of that asset

3.2 Abbreviations

For the purposes of this document the abbreviations of EN 50600-1:2012 and the following apply.

CCTV closed-circuit television

ffs for further study

IDS intrusion detection system

PIDS perimeter intrusion detection system

4 Conformance

For a data centre to conform to this European Standard:

1) the required Protection Class of Clause 5 shall be applied to the spaces of the data centre;
2) the requirements of the relevant Protection and Area Class of Clauses 6 and 7 shall be applied;
3) the requirements of the relevant Protection Class of Clauses 8 and 9 shall be applied;
4) the security systems shall be in accordance with Clause 10;
5) local regulations, including safety, shall be met.

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.

Subclause 5.3 provides minimum requirements for the data centres spaces defined in EN 50600-1. The requirements and recommendations for those data centre spaces, and the security systems employed within those spaces, address protection against:

a) unauthorised access (see Clause 6);
b) fire events internal to the data centre spaces (see Clause 7);
c) other environmental events, other than fire, and including electromagnetic interference, vibration, flooding, gas and dust hazards which may exist:
   - internal to the data centre spaces (see Clause 8);
   - external to the data centre spaces (see Clause 9).

Constructional requirements for walls and penetrations are provided in EN 50600-2-1 and relevant cross-referenced are provided from this standard.

In order for a space within the data centre to be considered to be of a given Protection Class (and Area Class for Clauses 6 and 7), the architectural and engineering design of the space (or entry to that space) shall meet or exceed that Protection Class for all aspects detailed above.

5.2 Risk assessment

The requirements for operational security should be determined by the organisation responsible for data centre assets i.e. the data requiring protection on its hosted platform. The requirements should be determined following a risk assessment based on the threats posed to the data, and the “classification” of that data. Various risk assessment methodologies are available, further detailed guidance is provided by EN 31010.

Figure 2 illustrates the concept of the risk assessment which is described as follows:

a) asset value: the classification of the material should be determined at an early stage, so that is is possible to deploy appropriate protection countermeasures. The nature of the “classification” maybe “native”, or “raised” due to the effects of data aggregation;

b) likelihood: the probability of some form of attack against the protected assets;

c) threat (forcible or surreptitious) analysis: for example, posed by unauthorised access to the assets resulting in loss or unavailability of the assets;

d) vulnerability analysis: for example, inadequate physical security or technical controls of the hosted data.

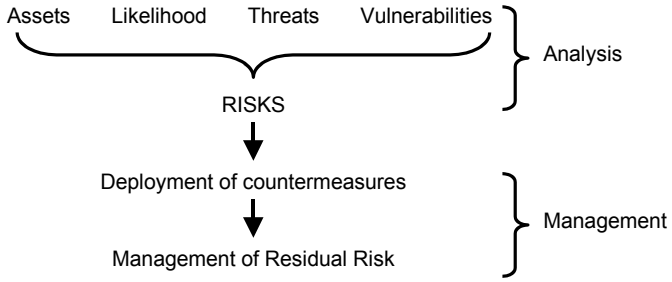

Figure 2 - Risk assessment concepts

These four items are analysed during the risk assessment process, to identify the baseline risk posed to the data centre. Management of the identified baseline risk employs appropriate countermeasures which may combine technical, physical and procedural controls.

Following the deployment of baseline countermeasures, further decisions shall be taken relating to the residual risk(s) as follows, driven by the risk appetite of the asset owner:

1) toleration - the remaining risk(s) are accepted and no additional countermeasures deployed;

2) treatment - additional controls are deployed to counter the remaining risk(s);

3) transferral - the risk(s) are transferred to another party, for example obtaining additional insurance cover the mitigate the risk(s);

4) termination - the activity posing the risk is terminated.

5.3 Designation of data centre spaces

5.3.1 Protection Classes

Each of the data centre spaces, independent of the size or purpose of the data centre, is designated as being of a particular Protection Class. The requirements for the Protection Class to be applied to the elements of the following facilities and infrastructures within the data centre are defined in:

a) EN 50600-2-2 for the power distribution system;

b) EN 50600-2-3 for the environmental control system;

c) EN 50600-2-4 for the telecommunications cabling.

In addition, Table 1 defines the minimum Protection Class that shall be applied for other data centre spaces subject to specific enhancements based upon the considerations of 5.3.2 and 5.3.3 together with the construction and configuration of the data centre described in 6.3.

It should be noted that the concept of Protection Class is not applied to an entire data centre i.e. there is no hierarchical intent and there is no concept of a data centre of a given Protection Class.

246 **Table 1 - Protection Classes for data centre spaces**

Protection Class 1	Protection Class 2	Protection Class 3	Protection Class 4
Personnel entrances to buildings or structures containing data centre spaces	Premises entrance facility Building entrance facilities The internal access to docking bays (the barrier of the docking bay providing the interface between Protection Classes 1 and 2) External premises security spaces Personnel entrances to the data centre spaces Storage spaces Holding spaces Testing spaces Data centre office spaces	Computer room spaces Control room space Data centre security spaces Telecommunications spaces	See 5.3.2.

247

248 ### 5.3.2 Enhancements of Protection Class

249 EN 50600-2-2 and EN 50600-2-3 require that all controls and equipment for their respective facilities and
250 infrastructures are accommodated within spaces of minimum Protection Class 3. As a primary purpose of the
251 power distribution and environmental control systems are to support the functionality of the IT equipment
252 within the computer room spaces, those computer room spaces shall be of Protection Class 3 (minimum).

253 This requirement only addresses the availability of the facilities and infrastructures and does not take into
254 account the security of any data stored, processed or transported within the computer room or similar
255 spaces.

256 However, a risk analysis of the type described in 5.2 may demand that the Protection Class for certain
257 spaces is increased. Examples of these situations include the additional protection that may be necessary in
258 relation to access controls associated with the cabinets, frames, or racks within a computer room space.

259 ### 5.3.3 Protection Class and Area Class

260 Table 1 defines the minimum Protection Class applicable to data centre spaces in conjunction with the
261 requirements of EN 50600-2-2, EN 50600-2-3 and EN 50600-2-4. However, the requirements for certain
262 spaces of a given Protection Class may differ as specified within Clauses 6 and 7. These specific
263 requirements are differentiated by Area Class as defined in each clause.

264 ## 6 Protection Class against unauthorised access

265 ### 6.1 General

266 This standard applies the four Protection Classes in relation to access to spaces accommodating the
267 elements of the different facilities and infrastructures as detailed in Table 2 (in accordance with EN 50600-1).

268 The Protection Classes feature increasing levels of access control. The areas of the data centre requiring the
269 greatest physical protection against unauthorised access will be accommodated in spaces with the highest
270 Protection Class.

271 This clause defines the rules for implementing such Classes.