



**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

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

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

[SIST EN 50600-2-5:2021](https://standards.iteh.com/catalog/standards/sist/5240b1c0-9c11-4b7d-b755-d62627373009/sist-en-50600-2-5-2021)

**ICS:**

35.030            Informacijska varnost            IT Security

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



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.

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, 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**

1	<b>Contents</b>	Page
2	<b>European foreword</b> .....	5
3	<b>Introduction</b> .....	6
4	<b>1 Scope</b> .....	9
5	<b>2 Normative references</b> .....	9
6	<b>3 Terms, definitions and abbreviations</b> .....	10
7	3.1 Terms and definitions .....	10
8	3.2 Abbreviations .....	11
9	<b>4 Conformance</b> .....	11
10	<b>5 Physical security</b> .....	11
11	5.1 General .....	11
12	5.2 Risk analysis and management.....	12
13	5.3 Designation of data centre spaces: Protection Classes .....	13
14	<b>6 Protection Class against unauthorized access</b> .....	13
15	6.1 General .....	13
16	6.1.1 Data centre configuration .....	13
17	6.1.2 Protection Classes .....	13
18	6.1.3 Protection Classes of specific infrastructures .....	16
19	6.1.4 Technical solutions to prevent unauthorized access .....	16
20	6.2 Access to the data centre premises .....	16
21	6.2.1 Premises with external physical barriers.....	16
22	6.2.2 Premises without external physical barriers.....	17
23	6.2.3 Roofs .....	18
24	6.2.4 Access routes .....	18
25	6.2.5 Parking .....	18
26	6.2.6 Employees and visitors .....	19
27	6.2.7 Pathways.....	19
28	6.2.8 Cabinets, racks and frames .....	20
29	6.3 Implementation .....	20
30	6.3.1 Protection Class 1 .....	20
31	6.3.2 Protection Class 2 .....	21
32	6.3.3 Protection Class 3 .....	21
33	6.3.4 Protection Class 4 .....	22
34	<b>7 Protection Class against intrusion to data centre spaces</b> .....	<b>23</b>
35	7.1 General .....	23
36	7.2 Technical solutions for the detection of intrusion.....	23
37	7.3 Implementation .....	23
38	7.3.1 Protection Class 1 .....	23
39	7.3.2 Protection Class 2 .....	24
40	7.3.3 Protection Class 3 .....	24
41	7.3.4 Protection Class 4 .....	25

42	<b>8</b>	<b>Protection Class against fire events igniting within data centre spaces</b>	<b>25</b>
43	8.1	General	25
44	8.1.1	Protection Classes	25
45	8.1.2	Fire compartments and barriers	26
46	8.1.3	Fire detection and fire alarm systems	27
47	8.1.4	Fixed firefighting systems	27
48	8.1.5	Portable firefighting equipment	29
49	8.2	Implementation	29
50	8.2.1	Protection Class 1	29
51	8.2.2	Protection Class 2	29
52	8.2.3	Protection Class 3	29
53	8.2.4	Protection Class 4	29
54	<b>9</b>	<b>Protection Class against environmental events (other than fire) within data centre spaces</b>	<b>30</b>
55	9.1	General	30
56	9.2	Implementation	30
57	9.2.1	Protection Class 1	30
58	9.2.2	Protection Class 2	30
59	9.2.3	Protection Class 3	31
60	9.2.4	Protection Class 4	31
61	<b>10</b>	<b>Protection Class against environmental events outside the data centre spaces</b>	<b>32</b>
62	10.1	General	32
63	10.2	Implementation	32
64	10.2.1	Protection Class 1	32
65	10.2.2	Protection Class 2	32
66	10.2.3	Protection Class 3	33
67	<b>11</b>	<b>Systems to prevent unauthorized access and intrusion</b>	<b>33</b>
68	11.1	General	33
69	11.2	Technology	34
70	11.2.1	Security lighting	34
71	11.2.2	Video surveillance systems	34
72	11.2.3	Intruder and holdup alarm systems	35
73	11.2.4	Access control	36
74	11.2.5	Alarm monitoring	36
75	<b>Annex A (informative)</b>	<b>Pressure relief: Additional information</b>	<b>37</b>
76	<b>A.1</b>	<b>General</b>	<b>37</b>
77	<b>A.2</b>	<b>Design considerations</b>	<b>37</b>
78		<b>Bibliography</b>	<b>39</b>
79			
80		<b>Figures</b>	
81		Figure 1 — Schematic relationship between the EN 50600 standards	7
82		Figure 2 — Risk analysis and management concepts	12
83		Figure 3 — Protection Classes within the 4-layer physical protection model	14

**prEN 50600-2-5:2020 (E)**

84	Figure 4 — Protection Class islands .....	15
85	Figure 5 — Connections between Protection Class islands .....	15
86	Figure 6 — Example of Protection Classes applied to data centre premises with external barriers .....	17
87	Figure 7 — Example of Protection Classes applied to data centre premises without external barriers .....	18
88		
89	<b>Tables</b>	
90	Table 1 — Protection Classes against unauthorized access .....	14
91	Table 2 — Technical solutions for access control .....	16
92	Table 3 — Technical solutions for intrusion detection .....	23
93	Table 4 — Protection Classes against internal fire events .....	26
94	Table 5 — Protection Classes against internal environmental events .....	30
95	Table 6 — Protection Classes against external environmental events .....	32
96	Table 7 — Elements of systems for the prevention of unauthorized access .....	33
97		

iTeh Standards  
 (<https://standards.iteh.ai>)  
 Document Preview

[SIST EN 50600-2-5:2021](https://standards.iteh.ai/catalog/standards/sist/32a6b1c0-9c11-4b7a-b753-db2027595089/sist-en-50600-2-5-2021)

<https://standards.iteh.ai/catalog/standards/sist/32a6b1c0-9c11-4b7a-b753-db2027595089/sist-en-50600-2-5-2021>

## 98 **European foreword**

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

101 This document is currently submitted to the Enquiry.

102 The following dates are proposed:

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

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

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

- 105 a) technical update to all clauses in response to user feedback;
- 106 b) new Clause 7 on Protection Classes against intrusion to data centre spaces added and Clause 6  
107 restructured accordingly;
- 108 c) references to relevant provisions of prEN 50600-2-1:2020 added to highlight the respective links to  
109 constructional requirements;
- 110 d) various editorial updates.

[SIST EN 50600-2-5:2021](https://standards.iteh.ai/catalog/standards/sist/32a6b1c0-9c11-4b7a-b753-db2027595089/sist-en-50600-2-5-2021)

<https://standards.iteh.ai/catalog/standards/sist/32a6b1c0-9c11-4b7a-b753-db2027595089/sist-en-50600-2-5-2021>

## 111 Introduction

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

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

121 The implementation of data centres varies in terms of:

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

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

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

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

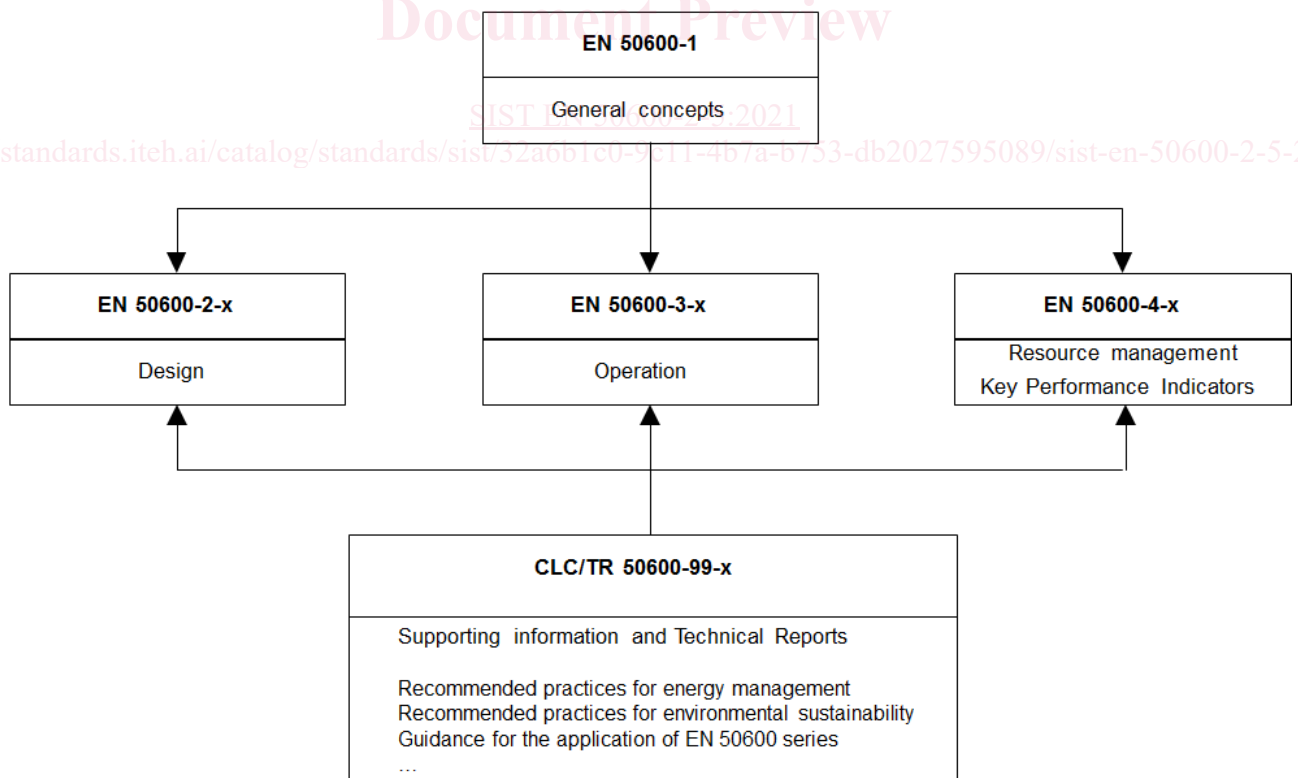
138 At the time of publication of this document, the EN 50600 series currently comprises the following standards:

- 139 — EN 50600-1, *Information technology — Data centre facilities and infrastructures — Part 1: General*  
 140 *concepts*;
- 141 — EN 50600-2-1, *Information technology — Data centre facilities and infrastructures — Part 2-1: Building*  
 142 *construction*;
- 143 — EN 50600-2-2, *Information technology — Data centre facilities and infrastructures — Part 2-2: Power*  
 144 *supply and distribution*;
- 145 — EN 50600-2-3, *Information technology — Data centre facilities and infrastructures — Part 2-3:*  
 146 *Environmental control*;
- 147 — EN 50600-2-4, *Information technology — Data centre facilities and infrastructures — Part 2-4:*  
 148 *Telecommunications cabling infrastructure*;



- 149 — EN 50600-2-5, *Information technology — Data centre facilities and infrastructures — Part 2-5: Security*  
150 *systems;*
- 151 — EN 50600-3-1, *Information technology — Data centre facilities and infrastructures — Part 3-1:*  
152 *Management and operational information;*
- 153 — EN 50600-4-1, *Information technology — Data centre facilities and infrastructures — Part 4-1: Overview*  
154 *of and general requirements for key performance indicators;*
- 155 — EN 50600-4-2, *Information technology — Data centre facilities and infrastructures — Part 4-2: Power*  
156 *Usage Effectiveness;*
- 157 — EN 50600-4-3, *Information technology — Data centre facilities and infrastructures — Part 4-3:*  
158 *Renewable Energy Factor;*
- 159 — EN 50600-4-6, *Information technology — Data centre facilities and infrastructures — Part 4-6: Energy*  
160 *Reuse Factor;*
- 161 — EN 50600-4-7, *Information technology — Data centre facilities and infrastructures — Part 4-7: Cooling*  
162 *Efficiency Ratio;*
- 163 — CLC/TR 50600-99-1, *Information technology — Data centre facilities and infrastructures — Part 99-1:*  
164 *Recommended practices for energy management;*
- 165 — CLC/TR 50600-99-2, *Information technology — Data centre facilities and infrastructures — Part 99-2:*  
166 *Recommended practices for environmental sustainability;*
- 167 — CLC/TR 50600-99-3, *Information technology — Data centre facilities and infrastructures — Part 99-3:*  
168 *Guidance for the application of EN 50600 series.*

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



170

171

**Figure 1 — Schematic relationship between the EN 50600 standards**

**prEN 50600-2-5:2020 (E)**

- 172 EN 50600-2-X standards specify requirements and recommendations for particular facilities and  
173 infrastructures to support the relevant classification for “availability”, “physical security” and “energy efficiency  
174 enablement” selected from EN 50600-1.
- 175 EN 50600-3-X documents specify requirements and recommendations for data centre operations, processes  
176 and management.
- 177 EN 50600-4-X documents specify requirements and recommendations for key performance indicators (KPIs)  
178 used to assess and improve the resource usage efficiency and effectiveness, respectively, of a data centre.
- 179 This document addresses the physical security of facilities and infrastructure within data centres together  
180 with the interfaces for monitoring the performance of those facilities and infrastructures in line EN 50600-3-1  
181 (in accordance with the requirements of EN 50600-1).
- 182 This document is intended for use by and collaboration between architects, building designers and builders,  
183 system and installation designers and security managers among others.
- 184 This series of documents does not address the selection of information technology and network  
185 telecommunications equipment, software and associated configuration issues.

## iTeh Standards (<https://standards.iteh.ai>) Document Preview

[SIST EN 50600-2-5:2021](https://standards.iteh.ai/catalog/standards/sist/32a6b1c0-9c11-4b7a-b753-db2027595089/sist-en-50600-2-5-2021)

<https://standards.iteh.ai/catalog/standards/sist/32a6b1c0-9c11-4b7a-b753-db2027595089/sist-en-50600-2-5-2021>

## 186 1 Scope

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

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

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

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

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

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

## 200 2 Normative references

201 The following documents are referred to in the text in such a way that some or all of their content constitutes  
202 requirements of this document. For dated references, only the edition cited applies. For undated references,  
203 the latest edition of the referenced document (including any amendments) applies.

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

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

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

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

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

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

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

211 EN 16750, *Fixed firefighting systems — Oxygen reduction systems — Design, installation, planning and  
212 maintenance*

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

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

215 EN 50518, *Monitoring and Alarm Receiving Centre*

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

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

## prEN 50600-2-5:2020 (E)

- 219 EN 50600-2-2, *Information technology — Data centre facilities and infrastructures — Part 2-2: Power supply*  
220 *and distribution*
- 221 EN 50600-2-3, *Information technology — Data centre facilities and infrastructures — Part 2-3: Environmental*  
222 *control*
- 223 EN 50600-2-4, *Information technology — Data centre facilities and infrastructures — Part 2-4:*  
224 *Telecommunications cabling infrastructure*
- 225 EN 50600-2-5, *Information technology — Data centre facilities and infrastructures — Part 2-5: Security*  
226 *systems*
- 227 EN 60839-11-1, *Alarm and electronic security systems — Part 11-1: Electronic access control systems -*  
228 *System and components requirements (IEC 60839-11-1)*
- 229 EN 62305 (series), *Protection against lightning (IEC 62305 series)*
- 230 EN 62676-1-1:2014, *Video surveillance systems for use in security applications — Part 1-1: System*  
231 *requirements — General (IEC 62676-1-1:2014)*

232 **3 Terms, definitions and abbreviations**233 **3.1 Terms and definitions**

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

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

236 — ISO Online browsing platform: available at <https://www.iso.org/obp>

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

238 **3.1.1**239 **authorized person**

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

242 **3.1.2**243 **forcible threat**

244 threat exhibited by physical force

245 **3.1.3**246 **frame**

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

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

249 **3.1.4**250 **free-standing barrier**

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

253 [SOURCE: prEN 50600-2-1:2020, 3.1.2]

254 **3.1.5**255 **hold time**

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