FINAL
DRAFT

INTERNATIONAL
STANDARD

**ISO/IEC
FDIS
22237-6**

ISO/IEC JTC **1**/SC **39**

Secretariat: **ANSI**

Voting begins on:
2023-11-09

Voting terminates on:
2024-01-04

Information technology — Data centre facilities and infrastructures —

Part 6: Security systems

Technologie de l'information — Installation et infrastructures de centres de traitement de données —

Partie 6: Systèmes de sécurité

Reference number
ISO/IEC FDIS 22237-6:2023(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 39, *Sustainability, IT and data centres*.

This first edition cancels and replaces ISO/IEC TS 22237-6:2018, which has been technically revised.

The main changes are as follows:

— a new Clause 7, "Protection against intrusion to data centre spaces", has been added. Clause 6 has been restructured accordingly;

— references to relevant provisions of ISO/IEC 22237-2 have been added to highlight the respective links to constructional requirements;

A list of all parts in the ISO/IEC 22237 series can be found on the ISO and IEC websites.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

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 house and support 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 economic 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 facilities);

b) security level;

c) physical size; and

d) accommodation (mobile, temporary and permanent constructions).

NOTE Cloud services can be provided by all data centre types mentioned.

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. Effective management and operational information are required to monitor achievement of the defined needs and objectives.

The ISO/IEC 22237 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:

1) owners, operators, facility managers, ICT managers, project managers, main contractors;

2) consultants, architects, building designers and builders, system/installation designers, auditors, test and commissioning agents;

3) suppliers of equipment; and

4) installers, maintainers.

The inter-relationship of the various documents within the ISO/IEC 22237 series at the time of publication is shown in Figure 1.

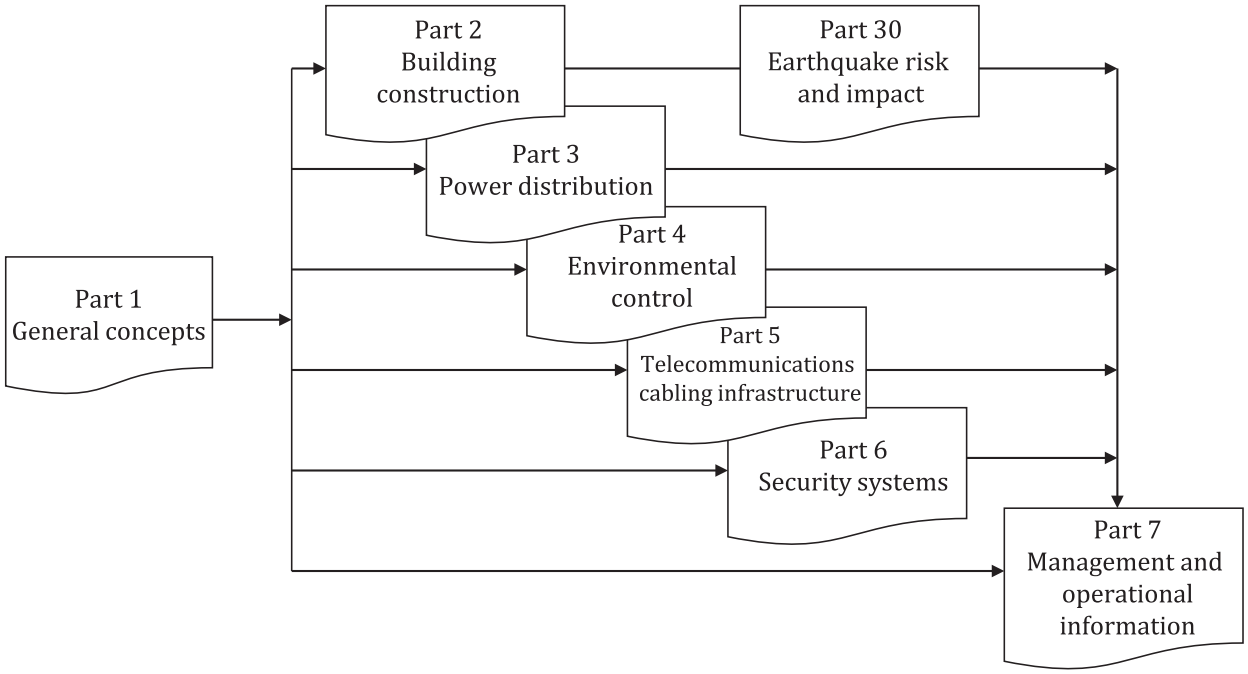


Figure 1 — Schematic relationship between the documents of the ISO/IEC 22237 series

ISO/IEC 22237-2 to ISO/IEC 22237-6 specify requirements and recommendations for particular facilities and infrastructures to support the relevant classification for "availability", "physical security" and "energy efficiency enablement" according to ISO/IEC 22237–1.

This document, ISO/IEC 22237-6, 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 ISO/IEC TS 22237-7 (in accordance with the requirements of ISO/IEC 22237-1).

ISO/IEC TS 22237-7 addresses the operational and management information (in accordance with the requirements of ISO/IEC 22237-1.

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

The ISO/IEC 22237 series does not address the selection of information technology and network telecommunications equipment, software and associated configuration issues.

Information technology — Data centre facilities and infrastructures —

Part 6: Security systems

1 Scope

This document specifies requirements and recommendations concerning the physical security of data centres based on the criteria and classifications for "availability", "security" and "energy efficiency enablement" within ISO/IEC 22237-1.

This document provides designations for the data centres spaces defined in ISO/IEC 22237-1.

This document specifies requirements and recommendations for such 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) internal fire events igniting within data centres spaces;

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

e) external 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 ISO/IEC 22237-2.

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

Conformance of data centres to the present document is covered in Clause 4.

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.

ISO/IEC 22237-1, *Information technology — Data centre facilities and infrastructures — Part 1: General concepts*

ISO/IEC 22237-2, *Information technology — Data centre facilities and infrastructures — Part 2: Building construction*

ISO/IEC 22237-3, *Information technology — Data centre facilities and infrastructures — Part 3: Power distribution*

ISO/IEC 22237-4, *Information technology — Data centre facilities and infrastructures — Part 4: Environmental control*

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

IEC 60839-11-2, *Alarm and electronic security systems - Part 11-2: Electronic access control systems - Application guidelines*

IEC 62305 (all parts), *Protection against lightning*

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

3 Terms, definitions and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 22237-1 and the following apply.

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

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

— IEC Electropedia: available at https://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

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: ISO/IEC 22237-2:2023, 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

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

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

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

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

3.2 Abbreviated terms

For the purposes of this document, the abbreviated terms given in ISO/IEC 22237-1 and the following apply.

EMC	electromagnetic compatibility
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 Classes of Clause 5 shall be applied to each of the spaces of the data centre according to the risk analysis of 5.2;

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 the data centre 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 ISO/IEC 22237-1. The requirements and recommendations for those data centre spaces, and the systems employed within those spaces, address protection against:

a) unauthorized access (see Clause 6);

b) intrusion (see Clause 7);

c) fire events originating within data centres spaces (see Clause 8);

d) environmental events (other than fire) within the data centre spaces which would affect the defined level of protection (see Clause 9);

e) environmental events outside the data centre spaces which would affect the defined level of protection (see Clause 10).

Constructional requirements for walls and penetrations are provided in ISO/IEC 22237-2 and relevant cross-references are provided throughout this document.

5.2 Risk analysis and management

The requirements for security should be determined:

— by the organization responsible for data centre assets;

— following a risk assessment based on the threats posed to the data (and the "classification" of the data) and the processes hosted by the data centre. See ISO/IEC 22237-1 for further information regarding risk assessment methodologies.

Figure 2 illustrates the concept of the risk analysis and management and is described as follows:

a) asset value analysis: a classification ("native", or "raised" due to the effects of data aggregation) of the assets should be determined at an early stage, so that it is possible to deploy appropriate protection countermeasures;

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

c) forcible threat and surreptitious threat analysis: for example, posed by unauthorized 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.

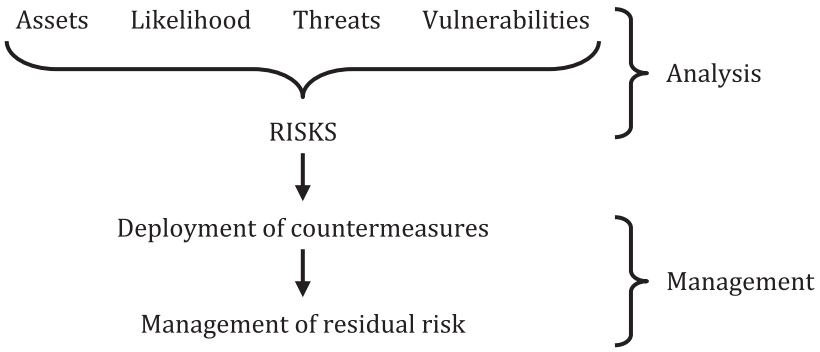


Figure 2 — Risk analysis and management concepts

These four items are analysed to identify the baseline risk posed to the data centre. Management of the identified baseline risk employs appropriate technical, physical and procedural countermeasures or a combination thereof at the appropriate security level.

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

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

2) treatment — additional measures are deployed to counter the remaining risk(s);

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

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

5.3 Designation of data centre spaces: Protection Classes

A data centre space can be accommodated in buildings, or other structures external to buildings, and can be dedicated to a particular data centre infrastructure e.g. generator space or transformer space.

There is no concept of a data centre of a given Protection Class.

Each data centre space, independent of the size or purpose of the data centre, is designated as being of a particular Protection Class with reference to each of the aspects in a) to e) of 5.1.

The Protection Class of a given space does not need to be the same for all aspects. For example, a generator within an isolated structure does not need a fire compartment but requires protection against both unauthorized access and intrusion.

The Protection Classes address the following aspects:

a) protection against unauthorized access;

b) protection against intrusion to data centre spaces;

c) protection against internal fire events igniting within data centre spaces;

d) protection against internal environmental events (other than fire) within data centre spaces;

e) protection against external environmental events outside the data centre spaces.

Each of these aspects are independent of each other. Protection Classes are not required to be aligned between aspects.

In addition, the risk analysis of 5.2 together with the construction and configuration of the data centre described in 6.2 will require the spaces of the data centre to be defined in terms of Protection Class for each aspect of security.

The Protection Class system operates horizontally and vertically (e.g. risers, lift shafts, stair wells, atriums, light-wells) for the buildings and structures.

6 Protection against unauthorized access

6.1 General

6.1.1 Data centre configuration

The facilities and infrastructures of the data centre may be accommodated in part, or all, of a single building or structure within the premises or may be distributed across several buildings or structures.

The implementation of barriers between areas of different Protection Classes in terms of protection against unauthorized access is based on their physical construction. The protection can be supplemented by technical and organizational measures. For example, free-standing barriers, external or internal walls of buildings, together with doors and other ducts, may be equipped with appropriate technical security systems (see Clause 11) and supplemented by appropriate organizational processes.

6.1.2 Protection Classes

This document defines four Protection Classes in relation to access to spaces accommodating the elements of the different facilities and infrastructures, as detailed in Table 1.

Table 1 — Protection Classes against unauthorized access

Type of protection	Class 1	Class 2	Class 3	Class 4
Protection against unauthorized access	Public or semi-public area.	Area that is accessible to all authorized persons (employees, tenants and visitors).	Area restricted to specified employees and tenants (visitors and other persons with access to Class 2 shall be accompanied by persons authorized to access Class 3 areas).	Area restricted to specified employees and tenants who have an identified need to have access (visitors and other persons with access to Class 2 or Class 3 areas shall be accompanied by persons authorized to access Class 4 areas).

The Protection Classes feature increasing levels of access control. The areas of the data centre requiring the greatest physical protection against unauthorized access will be accommodated in spaces with the highest Protection Class. Further guidance can be found in the IEC 60839-11 series.

As a fundamental principle:

a) authorized persons have access to specific areas (or groups of areas) of a given Protection Class;

b) authorized persons able to access specific areas (or groups of areas) of a given Protection Class do not have automatic access to all areas of a lower Protection Class.

This subclause defines the rules for implementing such Protection Classes.

The access to spaces and systems shall be limited to the inevitable necessary operative minimum. This applies to the aspects of spaces, time, personnel and knowledge. Physical security shall be implemented according to the philosophy shown schematically in Figure 3, referred to as the “onion skin” or “defence in depth” approach/model.

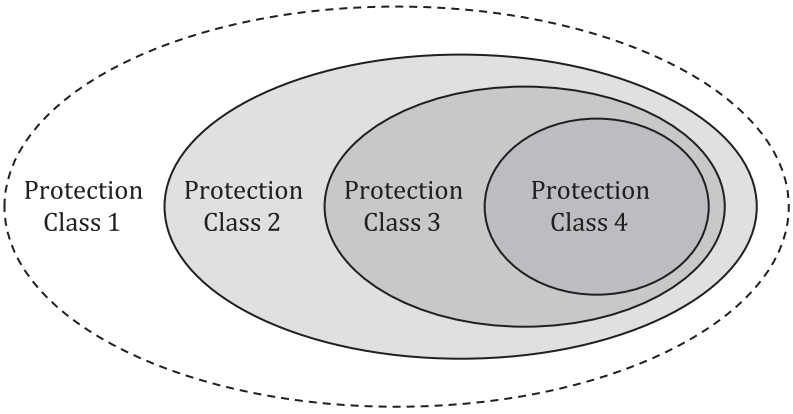


Figure 3 — Protection Classes within the 4-layer physical protection model

In order to be applicable to more general implementations of data centres, the simplistic model of Figure 3 can be visualized as a series of Protection Class islands as shown in Figure 4.

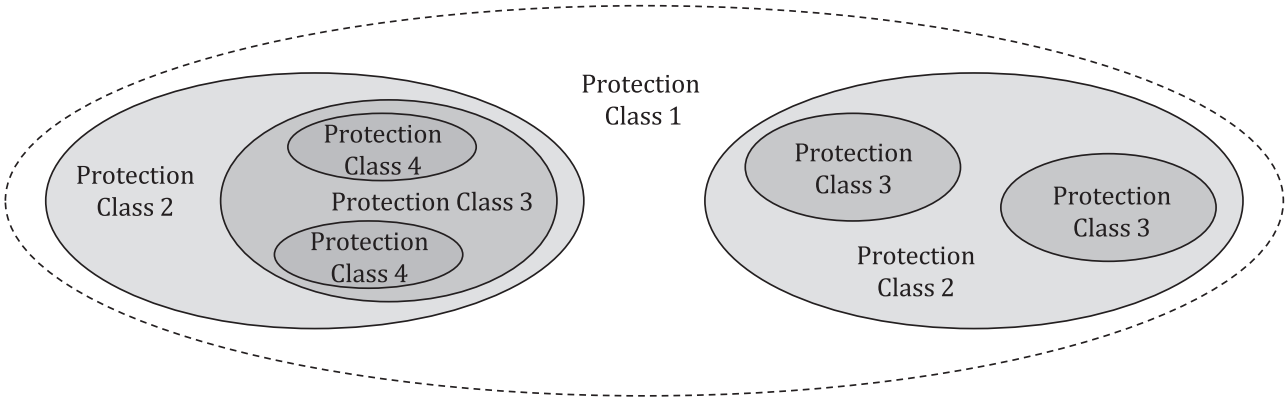


Figure 4 — Protection Class islands

Subclause 5.3 provides examples of the Protection Classes applied to data centre spaces but the technological solutions for the control of unauthorized access vary across the particular data centre spaces within a Protection Class.

All elements of the border/barrier of an area with a given Protection Class shall have the same level of resistance to unauthorized access. Where the data centre infrastructures specified in ISO/IEC 22237-2 to ISO/IEC 22237-6 cross boundaries from one Protection Class to another, they shall be provided with protection suitable to the lower Protection Class interconnected as shown in Figure 5.

NOTE National or local regulations can prevent security measures from being applied to pathways (e.g. maintenance holes, etc.) for infrastructures external to the premises.

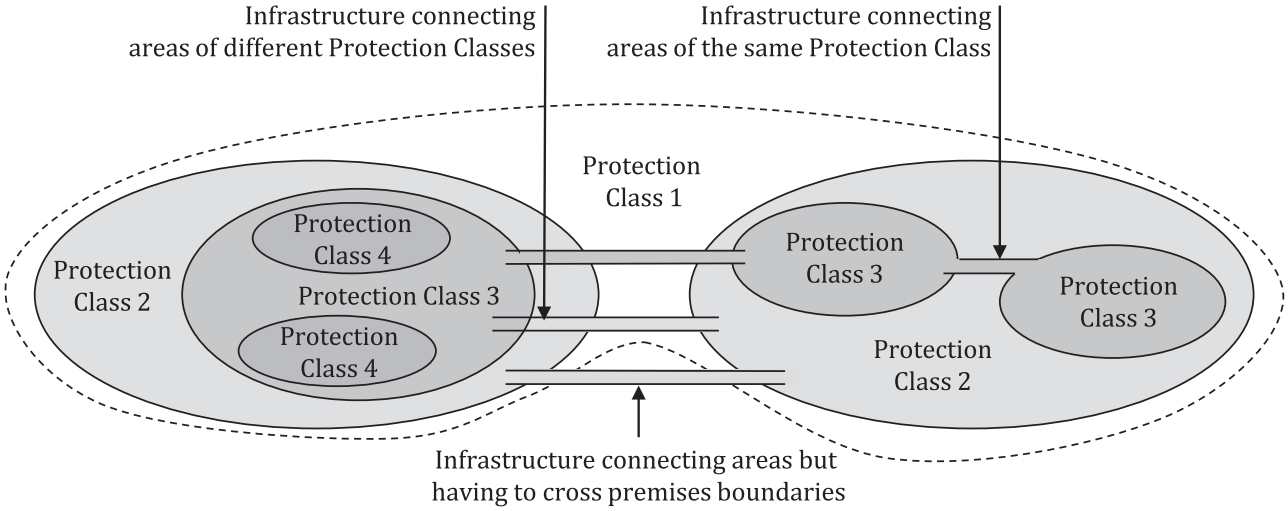


Figure 5 — Connections between Protection Class islands

Access control systems of a given Protection Class should be managed from areas with the same or higher Protection Class.

Pathways of the data centre infrastructures (e.g. power supply, environmental control and telecommunications cabling) shall be designed to prevent unauthorized passage between areas of different Protection Class.

Data centres and their complementary functions of technical infrastructure shall be organized in areas which mirror the needs of security, safety and availability of the data centre, and which match the assumed risks and protection goals.

The risk-bearing elements of the data centre should be located as far from the public or other unauthorized personnel as possible. Where this is not practicable, additional protection measures can be required as determined by the output of the risk assessment process or the site security assessment.

6.1.3 Protection Classes of specific infrastructures

The requirements for the Protection Class which shall be applied to the elements of the following facilities and infrastructures within the data centre are defined in:

a) ISO/IEC 22237-3 for the power distribution system;

b) ISO/IEC 22237-4 for the environmental control system;

NOTE Relevant requirements are also intended to be included in a future edition of ISO/IEC TS 22237-5 for the telecommunications cabling infrastructure.

6.1.4 Levels for access control

Table 2 describes four levels for access control to data centre spaces. The appropriate solution shall be specified to allow the crossing of the boundary of each Protection Class. Information in 11.2.4 provides details of the functionality options which can be applied.

Table 2 — Examples for access control

Security level	Access control intensity	Examples
1 (low)	Manual access control (no automation)	Mechanical key and lock plus manual access log
2 (medium)	Automated access control with single Factor authentication	Using an electronic ID medium (e.g. card or other ID token) plus electronic access log
3 (high)	Automated access control with two Factor authentication	Using an electronic ID medium (e.g. card or other ID token) together with another factor (e.g. PIN or biometry) plus electronic access log
4 (very high)	Enforced automated access control	Solutions to enforce the prevention of unregistered or unauthorized access or piggy-backing in addition to security level 3
NOTE Wearing a visible badge is possible for all security levels.		

6.2 Access to the data centre premises

6.2.1 Premises with external physical barriers

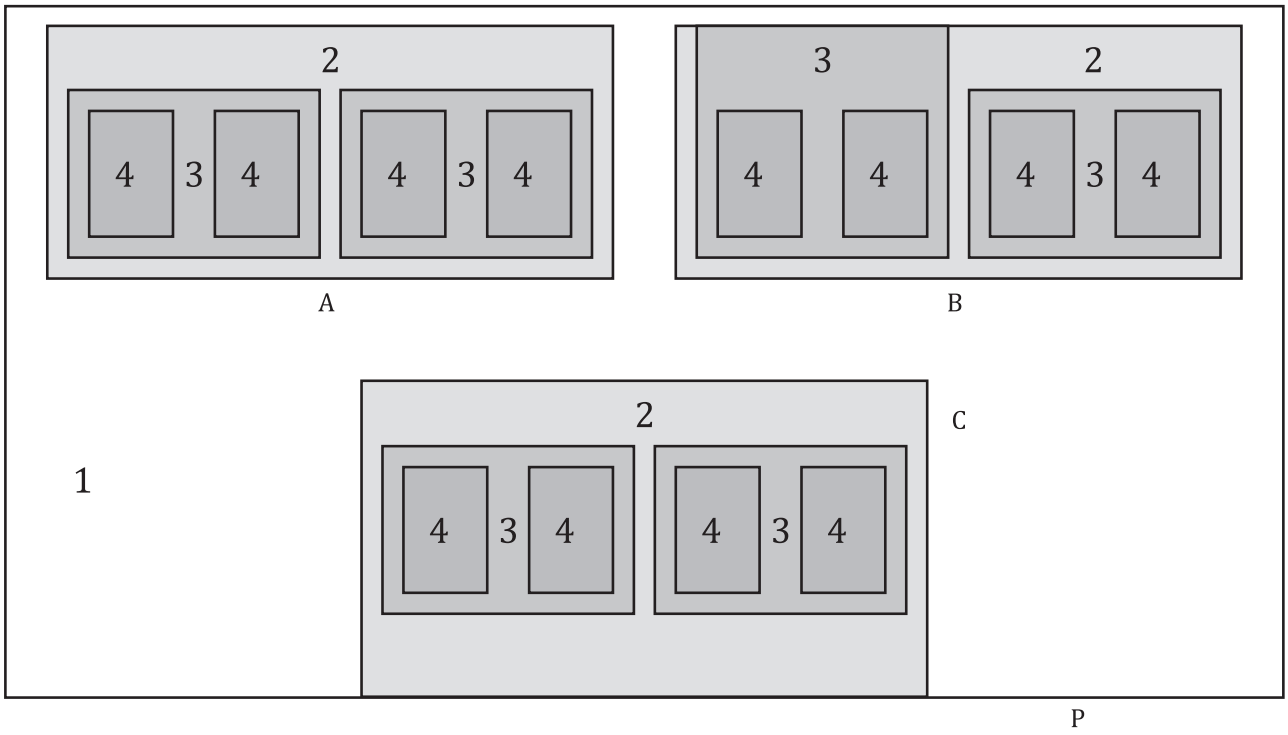
If the premises are provided with an external physical barrier that provides a demarcation of Protection Class 1, then, as shown in the example of Figure 6:

1) the number of penetrations of the boundary of Protection Class 1 for personnel and vehicular access shall be minimized;

2) the boundary of Protection Class 2 would represent the exterior walls and associated entrances of the buildings and other structures comprising the data centre and its associated spaces;

3) the boundary of Protection Class 3 would represent the barrier between any entrances of buildings or structures comprising the premises and the areas comprising the data centre and its associated spaces (these spaces may be in separate buildings or structures of Protection Class 2);

4) the boundary of Protection Class 4 would represent the barrier between the entrance to the area requiring Protection Class 3 and the area requiring Protection Class 4.



Key

1, 2, 3, 4	protection class 1 to 4
A, B, C	buildings A, B, C
P	premises boundary with physical barrier

Figure 6 — Example of Protection Classes applied to data centre premises with external barriers

6.2.2 Premises without external physical barriers

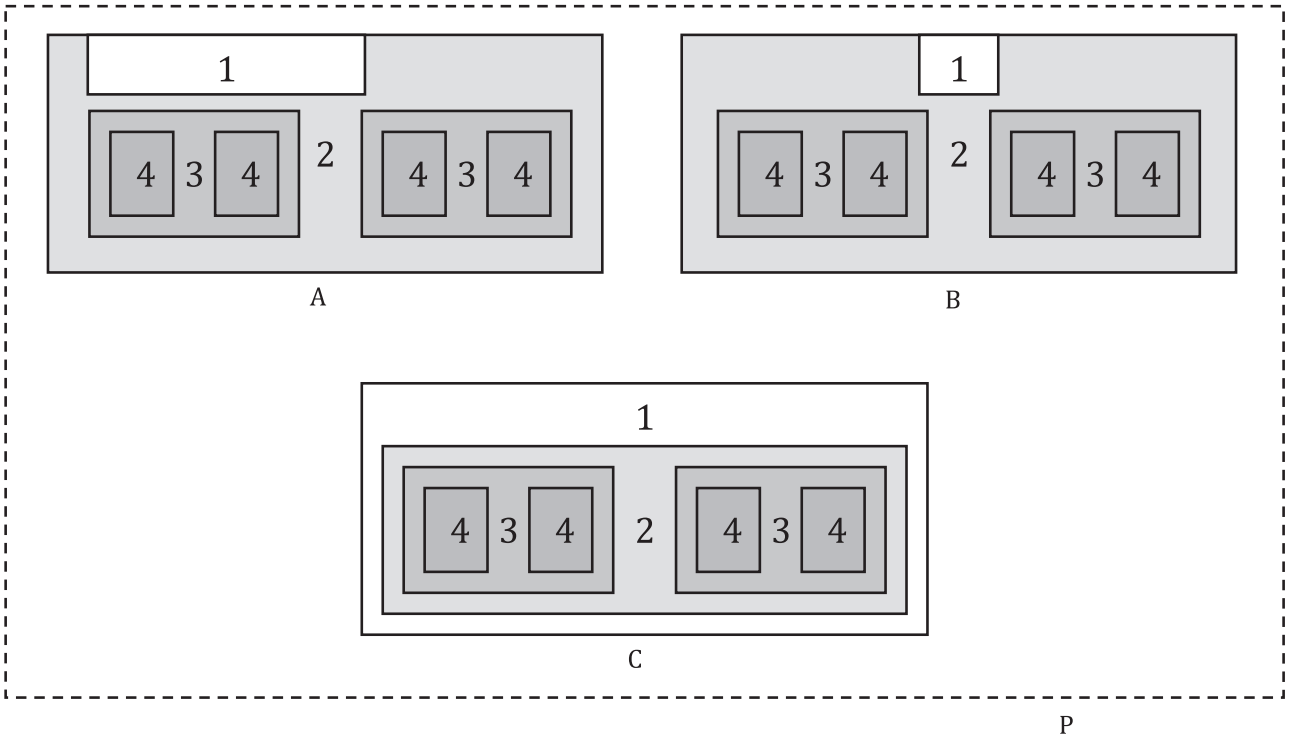
If the premises enable full and unrestricted public access to the boundaries of the building(s) or other structures, the exterior walls (or other defined internal barrier) of the building(s)/structures(s) represent the boundary of Protection Class 1. In such a case, as shown in the example of Figure 7:

1) the number of penetrations of the boundary of Protection Class 1 for personnel and vehicular access shall be minimized and these should be considered as points of surveillance and access detection;

2) the boundary of Protection Class 2 would represent the barrier between any entrances of buildings or structures comprising the premises and the areas comprising the data centre and its associated spaces (these spaces may be in separate buildings or structures of Protection Class 1);

3) the boundary of Protection Class 3 would represent the barrier between the entrance to the designated data centre space and the area requiring Protection Class 3;

4) the boundary of Protection Class 4 would represent the barrier between the entrance to the area requiring Protection Class 3 and the area requiring Protection Class 4.



Key

1, 2, 3, 4	protection class 1 to 4
A, B, C	buildings A, B, C
P	premises boundary with physical barier

Figure 7 — Example of Protection Classes applied to data centre premises without external barriers

6.2.3 Roofs

Appropriate barriers will be required to prevent unauthorized access to roof-top structures which accommodate facilities or infrastructure requiring a higher Protection Class.

Where possible, access routes to the roof for purposes of maintenance and repair of the roof, roof-top structures or infrastructure elements, shall be from within areas of Protection Class that are equal to the highest Protection Class of the roof-top structures.

6.2.4 Access routes

6.2.4.1 Requirements

Access routes shall be clearly signed to separate employees and visitors from deliveries to the data centre.

Plans shall exist which address operation in situations where the primary access routes are unavailable.

6.2.4.2 Recommendations

Consideration should be given to any requirements for:

a) enhanced lighting on access approach routes;

b) hostile vehicle mitigation on data centre approach routes;

c) fences and other boundary controls;

d) secondary access route, in case the primary route becomes unavailable.

6.2.5 Parking

6.2.5.1 Requirements

The requirements of a given Protection Class address vehicular access to the premises containing the data centre.

Consideration shall be given to and can place restrictions upon the designated location and minimum distance from the data centre spaces of any parking areas for:

a) visitors and unauthorized vehicles;

b) employees;

c) delivery vehicles;

d) maintenance and emergency vehicles.

6.2.5.2 Recommendations

Designated parking areas should be provided for visitors and other unauthorized vehicles.

Consideration should be given to:

a) video surveillance system (VSS) monitoring of the parking area;

b) location of the vehicle parking outside of the data centre perimeter;

c) lighting requirements;

d) vehicle identification and inspection requirements;

e) passage of vehicle occupants from the parking location to the data centre, including access control requirements;

f) operational security process requirements.

6.2.6 Employees and visitors

6.2.6.1 Requirements

Suitable space shall be allocated for the assessment and processing of employees and visitors in order to provide them with appropriate access credentials as authorized persons.

A system shall be in place to revoke the access credentials of authorized persons:

a) immediately upon termination of employment;

b) upon departure of a visitor.

This system shall include manual or automatic procedures to ensure that all physical access mechanisms (e.g. keys, access cards, etc.) are returned or disabled without the loss of access by other authorized persons.

6.2.6.2 Recommendations

The use of anti-passback door controls should be considered based upon either the overall security requirements of the data centre or to meet operational requirements.

Consideration should be given to VSS monitoring of access by authorized persons.

6.2.7 Pathways

6.2.7.1 Requirements

Undesirable or unnecessary access to infrastructure components and equipment within pathways, where justified according to the risk analysis of 5.2, shall be controlled by applying mechanical access control and, where appropriate, by monitoring. Based on the necessary security level (which is based on the risk assessment in 5.2), appropriate mitigation shall be provided when pathways of a given Protection Class pass through areas of a lower Protection Class.

6.2.7.2 Recommendations

Consideration should be given to VSS monitoring.

6.2.8 Cabinets, racks and frames

6.2.8.1 Requirements

Undesirable or unnecessary access to equipment inside cabinets or arrangements of cabinets, racks or frames, where justified following the risk analysis of 5.2, shall be controlled by applying mechanical or electronic access control and, where appropriate, by monitoring unauthorized opening of the cabinets.

6.2.8.2 Recommendations

Consideration should be given to VSS monitoring of access by authorized persons.

6.3 Implementation

6.3.1 Protection Class 1

6.3.1.1 Requirements

6.3.1.1.1 Construction

Shall conform to ISO/IEC 22237-2.

6.3.1.1.2 Organizational processes

The organizational process shall be adjusted to the physical security systems.

6.3.1.2 Recommendations

6.3.1.2.1 Construction

See ISO/IEC 22237-2.

6.3.1.2.2 Organizational processes

Consideration should be given to:

a) pedestrian barriers or defined security boundaries;

b) level and nature of security lighting;

c) provision of VSS;

d) operational security procedures;

e) hostile vehicle mitigation;

f) perimeter intruder and holdup alarm systems (I&HAS);

g) access control requirements;

h) internal I&HAS;

i) mail and delivery screening protocols.

6.3.2 Protection Class 2

6.3.2.1 General

Outer boundaries of areas of Protection Class 2 may be co-located with those of Protection Class 1.

6.3.2.2 Requirements

6.3.2.2.1 Construction

Shall conform to ISO/IEC 22237-2.

6.3.2.2.2 Organizational processes

The differing nature and function of the spaces serving the facilities and infrastructures of the data centre can allow/demand separate rules for access provision (i.e. if the premises contain multiple buildings/structures each which has specific functions or if the data centre spaces accommodate assets owned or operated by multiple entities).

Any penetrations of the physical barrier defining the outer boundary of Protection Class 2 shall prevent vehicle access to the premises except for those necessary for:

a) support operations (i.e. employee vehicles and associated parking facilities subject to the risk analysis of 5.2) and maintenance of the premises;

b) responding to emergency situations.

Any doors leading to the data centre spaces shall have appropriate door mechanisms in place to provide access to authorized persons only.

Procedures shall be in place (e.g. by means of an interlock, inspection by security personnel or scanning devices (examples see IEC 60839-11-1) to detect and prevent unauthorized access to the space.

Any opening of an emergency exit door shall trigger an alarm within the intrusion alarm system which initiates an appropriate response.

6.3.2.3 Recommendations

The number of penetrations of the barrier (excluding emergency exit doors) to allow general personnel access to, and egress from, each area of Protection Class 2 should be minimized.

The selection and location of emergency exit routes (escape routes) should not enable access to areas of a higher Protection Class.

6.3.3 Protection Class 3

6.3.3.1 Requirements

6.3.3.1.1 Construction

Shall conform to ISO/IEC 22237-2.

6.3.3.1.2 Organizational processes

Penetrations of the physical barrier defining the outer boundary of Protection Class 3 shall enable access to authorized persons. Additional access credentials are required to allow authorized persons to be accompanied by a defined number of persons having credentials to access areas of Protection Class 2.

Based on the necessary security level for individual spaces, appropriate procedures shall be in place (e.g. by means of an interlock, inspection by security personnel or scanning devices) to:

a) detect and prevent unauthorized access to the space;

b) monitor and/or control materials and equipment entering and leaving areas of Protection Class 3 (unless implemented at the relevant boundary of Protection Class 4).

Such procedures shall take into account any requirements for emergency exit functionality and for any vehicular access in emergency situations.

Any doors leading to the data centre spaces shall have appropriate door mechanisms in place to provide access to authorized persons only.

Any penetrations of the physical barrier defining the outer boundary of Protection Class 3 shall prevent vehicle access other than by emergency response vehicles unless accompanied by personnel authorized to access relevant areas of Protection Class 3.

Any opening of an emergency exit door shall trigger an alarm which initiates an appropriate response. The appropriate solution for such a function depends on the necessary security level.

6.3.3.2 Recommendations

The boundary of a Protection Class 3 area should not be co-located with boundaries to Protection Class 1.

The selection and location of emergency exit routes (escape routes) should not enable access to areas of Protection Class 4.

6.3.4 Protection Class 4

6.3.4.1 Requirements

6.3.4.1.1 Construction

Shall conform to ISO/IEC 22237-2.

6.3.4.1.2 Organizational processes

Penetrations of the physical barrier defining the outer boundary of Protection Class 4 shall enable access to authorized persons. Additional access credentials are required to allow authorized persons to be accompanied by a defined number of persons having credentials to access areas of Protection Classes 2 and 3.

Procedures shall be in place (e.g. by means of an interlock, inspection by security personnel or scanning devices) to:

a) detect and prevent unauthorised access to the space;

b) monitor and/or control materials and equipment entering and leaving areas of Protection Class 4 (unless implemented at a relevant boundary of Protection Class 3).

Any doors leading to the data centre spaces shall have appropriate door mechanisms in place to provide access to authorized persons only.

Such procedures shall take into account any requirements for emergency exit functionality and for any access in emergency situations.

Any opening of an emergency exit door shall trigger an alarm which initiates an appropriate response. The appropriate solution for such a function depends on the necessary security level.

6.3.4.2 Recommendations

The boundary of a Protection Class 4 area should not be co-located with boundaries to Protection Classes 1 or 2.

7 Protection against intrusion to data centre spaces

7.1 General

Appropriate protection against intrusion to data centre spaces depends on the necessary security level. Adequate and effective protection against intrusion to data centre spaces requires a combination of structural resistance (walls, doors, etc.), organizational measures and technical security measures. Appropriate structural resistance and organizational measures are the foundation.

The determination of appropriate Protection Classes in relation to intrusion can follow the “onion skin” concept outlined in 6.1.2.

The Protection Class of any part of the roof structure shall meet the Protection Class of the space immediately beneath that area. Appropriate barriers will be required for any roof-top structures which accommodate facilities or infrastructure requiring a higher Protection Class.

Data obtained during monitoring/surveillance should be subject to relevant controls for management and handling of images and other data taking into consideration local or national legislation (see Clause 11).

7.2 Level for the detection of intrusion

Table 3 describes four levels for the detection of potential or actual intrusion which can be applied at, outside or within Protection Class boundaries.

The appropriate solution shall be specific to each space. The solution for each space within a Protection Class boundary may differ depending upon the risk assessment associated with the equipment accommodated or activities undertaken in each space. Information in 11.2.2 provides details of the functionality options which can be applied.

Table 3 — Options for intrusion detection

Security level	Option	Examples
1	Visual inspection	Video surveillance System to record effective visual inspection
2	Local monitoring of specific areas within a space	Video surveillance (Category “observe” of IEC 62676-4) Motion detection Beam-break detection
3	Boundary monitoring	Video surveillance (Category “recognize” of IEC 62676-4) Motion detection Door contact and breakage sensors
4	Complete space monitoring	Video surveillance (Category “identify” of IEC 62676-4) Motion detection

7.3 Implementation

7.3.1 Protection Class 1

7.3.1.1 Requirements

7.3.1.1.1 General

So far as is practicable, the construction of the boundary of Protection Class 1 together with the surveillance systems surrounding that space shall be designed to detect and prevent intrusion in accordance with the required security level which is determined by the risk assessment according to 5.2.

7.3.1.1.2 Construction

Shall conform to ISO/IEC 22237-2.

7.3.1.1.3 Intrusion detection

See 11.2.2.1 and 11.2.3.1.

7.3.1.2 Recommendations

7.3.1.2.1 Surveillance

Areas of Protection Class 1 and, where possible, the area outside but in close proximity to the physical barriers defining the outer boundary of Protection Class 1 should be subject to monitoring/surveillance and should not contain objects (temporary or permanent) that would disrupt the effectiveness of monitoring/surveillance (e.g. any plants should be low-growing, no parking outside designated areas, no shelters, etc).

See 11.2.2.2 for further information.

7.3.2 Protection Class 2

7.3.2.1 Requirements

7.3.2.1.1 General

The construction of the boundary of Protection Class 2 together with the surveillance, intrusion detection and response systems surrounding that space shall be designed to delay intrusion in

accordance with the required security level which is determined by the risk assessment according to 5.2.

7.3.2.1.2 Construction

Shall conform to ISO/IEC 22237-2.

7.3.2.1.3 Intrusion detection

See 11.2.2.1 and 11.2.3.1.

7.3.2.1.4 Response systems

The response system to deter or detain potential intruders, following identification of potential intrusions, shall be matched to the construction of the boundary.

7.3.2.2 Recommendations

7.3.2.2.1 Construction

See ISO/IEC 22237-2:2021, 8.6.1.

7.3.2.2.2 Surveillance

Areas of Protection Class 2 and, where possible, the area outside but in close proximity to the physical barriers defining the outer boundary of Protection Class 2 should be subject to monitoring/surveillance and should not contain objects (temporary or permanent) that would disrupt the effectiveness of monitoring/surveillance.

See 11.2.2.2 for further information.

7.3.3 Protection Class 3

7.3.3.1 Requirements

7.3.3.1.1 General

The construction of the boundary of Protection Class 3 together with the surveillance, intrusion detection and response systems covered by this document surrounding that space shall be designed to prevent intrusion in accordance with the required security level which is determined by the risk assessment according to 5.2.

7.3.3.1.2 Construction

Shall conform to ISO/IEC 22237-2.

7.3.3.1.3 Intrusion detection

See 11.2.2.1 and 11.2.3.1.

7.3.3.1.4 Response systems

The response system to deter or detain potential intruders, following identification of potential intrusions, shall be matched to the construction of the boundary.

7.3.3.2 Recommendations

7.3.3.2.1 Surveillance

Areas of Protection Class 3 and, where possible, the area outside but in close proximity to the physical barriers defining the outer boundary of Protection Class 3 should be subject to monitoring/surveillance and should not contain objects (temporary or permanent) that would disrupt the effectiveness of monitoring/surveillance.

See 11.2.2.2 for further information.

7.3.4 Protection Class 4

7.3.4.1 Requirements

7.3.4.1.1 General

The construction of the boundary of Protection Class 4 together with the surveillance, intrusion detection and response systems covered by this document surrounding that space shall be designed to prevent intrusion in accordance with the required security level which is determined by the risk assessment according to 5.2.

7.3.4.1.2 Construction

Shall conform to ISO/IEC 22237-2.

7.3.4.1.3 Intrusion detection

See 11.2.2.1 and 11.2.3.1.

7.3.4.1.4 Response systems

The response system to deter or detain potential intruders, following identification of potential intrusions, shall be matched to the construction of the boundary.

7.3.4.2 Recommendations

7.3.4.2.1 Surveillance

Areas of Protection Class 4 and, where possible, the area outside but in close proximity to the physical barriers defining the outer boundary of Protection Class 4 should be subject to monitoring/surveillance and should not contain objects (temporary or permanent) that would disrupt the effectiveness of monitoring/surveillance.

See 11.2.2.2 for further information.

8 Protection against internal fire events (fire events igniting within data centre spaces)

8.1 General

8.1.1 Protection Classes

This document defines four Protection Classes in relation to fire originating within spaces accommodating the elements of the different facilities and infrastructures, as detailed in Table 4.

Table 4 — Protection Classes against internal fire events

Type of protection	Class 1	Class 2	Class 3	Class 4
Protection against internal fire	No special protection applied	The area requires protection against fire by a detection system.	The area requires protection against fire by a detection system (with optional early detection with pre-alarm) appropriate for a specific data centre infrastructure (e.g. generators, switchgears) and with non-fixed firefighting systems.	The area requires protection against fire by a detection system (with early detection with pre-alarm) and, if deemed necessary in the outcome of risk assessment, by a fixed firefighting system.

NOTE 1 For the purposes of this clause, the term "fire suppression system" is synonymous with the term "fixed firefighting system" adopted by CEN/TC 191.

NOTE 2 For the purposes of this clause, the term "fire detection system" is synonymous with the term "fire detection and alarm system" adopted by CEN/TC 72 and defined in EN 54–1.[12]

It is presupposed that national or local regulations for fire detection, alarms and suppression are applied in all spaces, independent of Protection Class. This clause addresses the fire detection and alarm, fixed and portable firefighting systems to be applied to the data centre spaces. The impact of fire-fighting procedures on the availability of the facilities and infrastructures in the data centre spaces shall be considered, including fire-fighting procedures, which could require the disruption of all power supplies (including back-up systems).

The type of fire detection system and firefighting systems selected for each space shall take into account the Protection Class of the space and approach to be taken in maintaining the function of the space.

The Protection Classes feature increasing levels of fire detection and reaction. The areas of the data centre requiring the greatest protection against internal fire events will be accommodated in spaces with the highest Protection Class.

8.1.2 Fire compartments and barriers

8.1.2.1 Requirements

The data centre spaces shall be considered as a series of fire compartments, each with its own objectives for fire detection, alarm and suppression.

All of the components comprising the boundary of a fire compartment and any pathways that penetrate the boundary of a fire compartment shall take into account the potential for spread of fire and combustion products (smoke and toxic gases).

The walls and barriers separating the fire compartments shall have a minimum fire rating in accordance with the requirements of the highest Protection Class present at the boundary of the fire compartment.

The constructional requirements of ISO/IEC 22237-2 apply.

8.1.2.2 Recommendations

See ISO/IEC 22237-2 for constructional recommendations.

8.1.3 Fire detection and fire alarm systems

8.1.3.1 Requirements

To support the objectives of Table 4 and independent of any requirements of national or local regulations, fire detection and fire alarm systems shall be installed in data centre spaces of Protection Class 2 and above.

Consideration shall be given to the need for early detection of combustion products with pre-alarm. Where used:

— components of the fire detection and alarm system shall take the applicable regional and national standards into consideration.

NOTE 1 For Europe, relevant parts of the EN 54 series[11] are applicable.

— the system shall take the applicable regional and national standards into consideration.

NOTE 2 For Europe, EN 54-13[13] is applicable.

NOTE 3 For the US, NFPA 72,[32] NFPA 75[33] and NFPA 76[34] are applicable.

NOTE 4 For Japan; the Fire Service Act of Japan with related ordinance and local regulation are applicable.[40]

Where used in spaces of Protection Class 3 and above, smoke detection (aspirating) systems shall take applicable regional and national standards into consideration, respectively.

NOTE 5 For Europe, EN 54-20:2006,[14] Sensitivity Class A or B is applicable.

The method of monitoring alarms (see 11.2.5) shall be determined during the design of the fire detection and alarm systems.

The time between the detection and activation of the suppression system shall allow the safe egress of personnel, where appropriate.

8.1.3.2 Recommendations

In the absence of national or local codes or regulations, ISO 7240-14 contains guidelines for the planning, design, installation, commissioning, use and maintenance of fire detection and alarm systems.

NOTE CEN/TS 54-14[24] provides alternative guidance.

An alarm should not automatically disrupt the function of the facilities and infrastructures of the data centre (e.g. re-circulation of air within the fire compartments produced by the environmental control systems should not be disrupted but the supply to fresh air into the fire compartment should be prevented).

8.1.4 Fixed firefighting systems

8.1.4.1 General

To support the objectives of Table 4, a fixed firefighting system shall be provided if it is deemed necessary in the outcome of the risk analysis of 5.2.

If it is intended to install a fixed firefighting system either to extinguish an incipient fire in any part of the protected space (including within cabinets) or to prevent a fire from spreading outside the protected space:

a) the system shall be designed to minimize hazards to personnel;

b) the system should be designed to minimize hazards to equipment;

c) the equipment accommodated within the space should be designed or located to maximize the efficiency of the fixed fighting system.

The selection of firefighting system can restrict the type of equipment to be accommodated within the protected space.

The selection and implementation of specific solutions shall take into consideration the appropriate standards and national or local regulations concerning their use.

See ISO/IEC 22237-2 for constructional requirements and recommendations to support the firefighting systems selected.

8.1.4.2 Fire extinguishing systems using gaseous agents

It is presupposed that gaseous systems are designed, installed and maintained in accordance with national or local regulations. In the absence of such regulations, the following standards should be considered:

— for Europe: EN 15004 series[18] (for gases other than carbon dioxide);

— for the US: NFPA 2001[37] and NFPA 2010;[38]

— for Japan: the Fire Service Act of Japan with related ordinance and local regulation is applicable;[40]

— ISO 6183 (for carbon dioxide systems) and for the US, NFPA 12.[31] However, carbon dioxide, which is lethal at normal extinguishing concentrations, shall only be used in spaces within which appropriate procedures are in place to protect personnel.

Where gaseous extinguishing systems are used:

a) to prevent loss of extinguishant through openings to adjacent hazards or work areas, any openings in the boundaries of the protected space shall be either be provided with fixed seals or equipped with automatic sealing systems and the predicted hold time shall be determined by the door fan test or a full discharge test;

b) to avoid re-ignition from a persistent ignition source (e.g. heat source or “deep-seated” fire), the effective concentration of extinguishant shall be maintained for the specified hold time by emergency actions such as turning off the make-up air ventilation of the protected space;

c) in the absence of national or local regulations, the minimum hold time shall be 10 min but a longer time shall be considered to reflect the predicted time to allow personnel to react to the fire and shut-down, where applicable, the equipment in the space;

d) smoke and heat exhaust ventilation systems in spaces with gas extinguishing systems shall not open automatically and shall only be triggered manually. The triggering device shall be protected against unauthorized access.

To avoid damage to buildings and equipment by excessively high or low pressure, pressure relief devices shall be provided. See Annex A for further details.

The following additional factors shall be taken into account:

1) the mechanical (including acoustic), climatic and electromagnetic impact of the discharge of the gaseous system on the equipment accommodated within the area served by the extinguishing system;

2) the design calculations for the system should compensate for leakage of extinguishing agent where necessary.

8.1.4.3 Oxygen reduction systems

Oxygen reduction fire prevention systems maintain the oxygen at a reduced concentration to inhibit ignition or spread of fire.

Oxygen reduction fire prevention systems shall be designed, installed and maintained taking into consideration the applicable regional and national standards, respectively.

NOTE For Europe, EN 16750[20] is applicable.

8.1.4.4 Water-based fire suppression systems

In the data centre spaces, any water-based systems shall be pre-action, i.e. the pipework is charged with air or inert gas, with water introduced only after fire has been detected.

The two water-based technologies are:

a) sprinklers, which shall be designed, installed and maintained taking into consideration applicable regional and national standards;

   NOTE 1 For Europe, EN 12845[16] is applicable;

b) water mist, which shall be designed, installed and maintained taking into consideration applicable regional and national standards.

   NOTE 2 For Europe, CEN/TS 14972[25] is applicable.

   NOTE 3 For the US, NFPA 750[35] is applicable.

The main purpose of water-based fire suppression systems is the protection of the building and spaces. For the protection of electrical equipment, the risks of equipment damage associated with water-based systems shall be considered.

Where water-based fire suppression systems are used in conjunction with aisle containment within data centre spaces, the sprinkler/nozzle layout shall be adjusted to ensure effective extinguishing of the fire inside the containment.

If sprinkler/nozzle adjustment is not possible or desirable, the containment system should be adapted to enable the water-based fire suppression systems to be effective using solutions such as:

1) a pivoting roof that opens when under specific conditions (e.g. a specified signal from a fire detection and alarm system);

2) a roof system made of a material that weakens and collapses when heated due to a fire or collapses due to the weight of the extinguishing water, if acceptable to national or local regulations.

8.1.4.5 Condensed aerosol systems

Condensed aerosol systems should not be used in occupied spaces or in spaces containing electronic equipment.

Condensed aerosol systems shall be designed, installed and maintained taking into consideration applicable regional and national standards, respectively.

NOTE 1 For Europe, EN 15276-2[19] is applicable.

NOTE 2 For the US, NFPA 2010[38] is applicable.

8.1.4.6 Foam systems

Foam systems should not be used in occupied spaces containing electronic equipment (e.g. telecommunications spaces and computer room spaces).

Foam systems shall be designed, installed and maintained taking into consideration applicable regional and national standards, respectively.

NOTE 1 For Europe, EN 13565-2[17] is applicable.

NOTE 2 For the US, NFPA 11[29] and NFPA 11A[30] are applicable.

8.1.5 Portable firefighting equipment

Where portable fire extinguishers are provided:

a) they shall take into consideration the applicable regional and national standards, respectively;

NOTE 1 For Europe, the EN 3 series[10] is applicable.

NOTE 2 For the US, NFPA 10[28] is applicable.

NOTE 3 For Japan, the Fire Service Act of Japan with related ordinance and local regulation is applicable.[40]

b) the number and location of portable fire extinguishers and the nature of the extinguishing agents shall take into consideration national regulations and shall be in accordance with the outcome of a risk assessment.

8.2 Implementation

8.2.1 Protection Class 1

No additional requirements or recommendations.

8.2.2 Protection Class 2

Areas of Protection Class 2 shall be provided with detection solutions in accordance with 8.1.3.

8.2.3 Protection Class 3

Areas of Protection Classes 3 shall be provided with detection and suppression solutions in accordance with 8.1.3 and 8.1.5 respectively.

8.2.4 Protection Class 4

Areas of Protection Class 4 shall be provided with detection solutions in accordance with 8.1.3 and suppression solutions in accordance with 8.1.5 and 8.1.4 (if required).

9 Protection against internal environmental events (other than fire within data centre spaces)

9.1 General

This document defines four Protection Classes in relation to protection against internal environmental events (other than the fire events of Clause 8) in spaces accommodating the elements of the different facilities and infrastructures as detailed in Table 5.

Examples of internal environmental events include vibration, flooding, leakage, gas and dust hazards.

Table 5 — Protection Classes against internal environmental events

Type of protection	Class 1	Class 2	Class 3	Class 4
Protection against internal environmental events (other than fire)	No requirements	Event detection only	Event detection and mitigation	Protection from events in surrounding spaces Event detection and mitigation within the space

The Protection Classes feature increasing levels of resistance to internal environmental events. The areas of the data centre requiring the greatest physical protection against internal environmental events will be accommodated in spaces with the highest Protection Class.

In addition, consideration shall be given to the electromagnetic environment of the data centre spaces which could disrupt the effective operation of data processing, data storage and data transfer and of the supporting infrastructures.

Procurement, installation and operation of equipment shall consider the electromagnetic compatibility characteristics of the data centre as a whole.

9.2 Implementation

9.2.1 Protection Class 1

Not applicable.

9.2.2 Protection Class 2

9.2.2.1 Requirements

Areas of Protection Class 2 shall be provided with sensors able to detect the relevant internal environmental events.

9.2.2.2 Recommendations

For further study.

9.2.3 Protection Class 3

9.2.3.1 General

Areas of Protection Class 3 provide detection and mitigation when subject to internal environmental events.

9.2.3.2 Requirements

Areas of Protection Class 3 shall be provided with sensors able to detect the relevant internal environmental events.

Drainage systems and other piping systems (including those of the environmental control systems of ISO/IEC 22237-4) shall not be present unless suitable mitigation is applied in case of leakage.

Penetrations that may be opened to enable normal or emergency function of the data centre infrastructures (such as pressure relief for gaseous extinguishing systems) shall, when closed, provide protection against the ingress of contaminants (particulate, liquid or gaseous).

Vibration shall be mitigated by dampers. Examples for dampers against seismic vibration can be found in ISO/IEC TS 22237-30.

9.2.3.3 Recommendations

Where possible, mitigation should be implemented by the use of construction methods and materials.

Walls, ceilings and cable entries should provide protection against the ingress of contaminants (particulate, liquid or gaseous) including water resulting from firefighting activity.

Areas of Protection Class 3 shall not be located underneath any openings in roof spaces unless drainage routes are provided.

9.2.4 Protection Class 4

9.2.4.1 General

Areas of Protection Class 4 provide detection and mitigation when subject to internal environmental events within their area and provide protection against internal environmental events in surrounding spaces.

9.2.4.2 Requirements

Areas of Protection Class 4 shall be surrounded in three dimensions by areas of Protection Class 3.

The outer boundaries of Protection Class 4 may be co-located with those of Protection Class 3 provided they are not penetrated from areas of a lower Protection Class.

Areas of Protection Class 4 shall be provided with sensors able to detect the relevant internal events.

Walls, ceilings and cable entries shall provide protection against the ingress of contaminants (particulate, liquid or gaseous) including water resulting from firefighting activity.

Interior walls shall provide the desired degree of physical protection against internal environmental events.

Where there is an identified risk of ingress of contaminants (including water resulting from firefighting activity) from other spaces, mitigation shall be provided in the form of:

a) sealing;

b) detection;

c) drainage.

Areas of Protection Class 4 shall not be located underneath any openings in roof spaces unless drainage routes are provided.

Room-in-room constructions shall be considered.

9.2.4.3 Recommendations

Areas of Protection Class 4 shall not be located underneath any openings in roof spaces unless drainage routes are provided.

Room-in-room constructions should provide environments consistently capable of conforming to the test regimes of applicable regional and national standards.

NOTE For Europe, EN 1047-2[15] is applicable.

10 Protection against external environmental events (events outside the data centre spaces)

10.1 General

This document defines three Protection Classes in relation to protection against external environmental events in spaces accommodating the elements of the different facilities and infrastructures as detailed in Table 6. The requirements of the Protection Classes shall be applied when subject to identified risk.

Examples of external environmental events include fire, lightning, electromagnetic interference, vibration (excluding seismic activity), flooding, gas and dust hazards.

Table 6 — Protection Classes against external environmental events

Type of protection	Class 1	Class 2	Class 3
Protection against external environmental events	No requirements	Event detection and mitigation	Protection from events in surrounding spaces

The Protection Classes feature increasing levels of resistance to external environmental events. The areas of the data centre requiring the greatest physical protection against external environmental events will be accommodated in spaces with the highest Protection Class.

Consideration shall be given to external sources of electromagnetic interference which could disrupt the effective operation of data processing, data storage and data transport. Assessment of the electromagnetic environment shall be undertaken in order to determine the need for any specific mitigation measures.

If shielding of external mobile telephone signals is provided by a Protection Class boundary, then either:

a) mobile telephones shall be forbidden within the boundary; or

b) a base station shall be provided within the boundary to prevent any mobile phones from becoming a source of electromagnetic interference.

In the case of seismic activity, the guidance for planning and mitigation can be found in ISO/IEC TS 22237-30.

10.2 Implementation

10.2.1 Protection Class 1

No requirements.

10.2.2 Protection Class 2

10.2.2.1 General

Areas of Protection Class 2 provide detection and mitigation when subject to external environmental events.

10.2.2.2 Requirements

Any penetrations of the boundaries to areas of Protection Class 2 which are open or could be opened to enable normal or emergency function of the data centre infrastructures (such as pressure relief for gaseous extinguishing systems) shall be provided with physical protection to prevent ingress of objects that might damage or restrict that function. Such physical protection shall be taken into account in the functional design of the penetration.

Buildings or structures accommodating areas of Protection Class 2 shall have a lightning protection system in accordance with the IEC 62305 series. Where the building or structure has a mesh bonding network for telecommunications equipment in accordance with ISO/IEC 30129, an "integrated lightning protection system" according to IEC 62305-4 is preferred. Other lightning protection systems, including the "isolated lightning protection system" according to IEC 62305-3, may be used provided that specific restrictions are applied as agreed between the planners of the lightning protection system and the bonding network.

NOTE 1 In the US, NFPA 780[36] is applicable.

NOTE 2 For Japan, JIS Z 9290[27] is applicable.

10.2.2.3 Recommendations

Where possible, mitigation should be implemented by the use of construction methods and materials.

10.2.3 Protection Class 3

10.2.3.1 General

Areas of Protection Class 3 provide protection against external environmental events.

10.2.3.2 Requirements

Areas of Protection Class 3 shall be surrounded in three dimensions by areas of Protection Class 2.

The outer boundaries of Protection Class 3 may be co-located with those of Protection Class 2 provided they are not penetrated from areas of a lower Protection Class.

Walls, ceilings and cable entries shall provide protection against the ingress of contaminants (particulate, liquid or gaseous) including water resulting from firefighting activity.

10.2.3.3 Recommendations

For further study.

11 Systems to prevent unauthorized access and intrusion

11.1 General

Systems employed to prevent unauthorized access are comprised of a number of elements, as described in Table 7.

Table 7 — Elements of systems for the prevention of unauthorized access

Subject	Element	Reference
Personnel	It will be ensured that sufficiently qualified personnel are in place, who have received the appropriate training to ensure the security system will function correctly in support of operational needs. Relevant and applicable background checks should have been performed to manage and mitigate insider threats. In situations requiring the highest security level, personnel will require additional vetting to support this assurance.	ISO/IEC TS 22237-7
Processes	Relevant operational processes will be designed and operated within the data centre and operational site. The operational processes will support and integrate with all systems necessary for the secure operation of the site. For example, processes in relation to the management and handling of visitors to the site, and the receipt and processing of deliveries to the site.	ISO/IEC TS 22237-7
Physical	Appropriate physical controls will be designed and operated on the site, providing the relevant classes of protection. The nature, number and type of physical controls will be determined by the risk assessment, or operational requirements as directed by hosted entities.	Clause 6 and Clause 7
Technology	A variety of systems will support the operations of the site, and will include as necessary, automatic access control systems, VSS systems, etc.	11.2

The selection and implementation of specific solutions shall be in accordance with the appropriate standards. It is presupposed that statutory and regulatory requirements are considered in the selection and implementation process. Appropriate references are provided in 11.2.2 and 11.2.3.

NOTE For example, for Europe, CLC/TS 50398[26] provides guidance on the integration of alarms and other systems.

11.2 Technology

11.2.1 Security lighting

Correct deployment of security lighting will provide an effective deterrent against intruders and support the use of VSS monitoring (see 11.2.2). The lighting should be deployed in strategic locations, particularly at site entry points. The correct deployment of lighting will aid and support mobile site security patrols.

Specialist advice should be obtained in order to select the appropriate lighting technology as a variety of solutions exist.

Security lighting should provide a minimum of 10 lux and should be deployed such that deep shadows are avoided around the data centre spaces being protected.

Security lighting at external perimeter barriers should be directed inwards to enable intruders to be identified directly or by silhouette.

In appropriate circumstances, additional security lighting may be installed which is ground-based behind the boundary fence line. This lighting would face outwards and provides an effective light shield, making observation of activities behind this light barrier difficult during hours of darkness.

Lighting should be controlled by a photoelectric cell, timers or other means. An appropriate selection of controls should be in place to protect the lights from being tampered with or disabled.

11.2.2 Video surveillance systems

11.2.2.1 Requirements

Where justified and based on the needed security level (see 7.2), which is determined by the output of the risk assessment of 5.2, the video surveillance system (VSS) shall meet the requirements of the appropriate Grade of IEC 62676-1-1, which is selected in line with the necessary security level.

The requirements for each VSS shall be determined taking into account:

a) what is under surveillance, i.e. “hot spots” (e.g. entrances, escape doors, loading bays), boundaries or complete spaces;

b) the nature of the surveillance, i.e. simple monitoring, recording or recording with a system for video analysis;

c) the requirements for management of all the video channels and the need for false-alarm-proof video analytics algorithms to minimize human involvement.

11.2.2.2 Recommendations

External cameras should be positioned to monitor:

a) approaches to the data centre premises;

b) access points to the data centre premises and spaces;

c) windows, doors and roof tops of the data centre premises and spaces.

Appropriate tests should be performed to ensure the system operates and provides the desired image quality in all expected weather and lighting conditions.

Internal cameras should be positioned to monitor:

1) approaches to specific data centre spaces;

2) entry/egress from areas of one Protection Class to another or between areas of a given Protection Class;

3) stairwell entrances and stairwells;

4) emergency exits.

Consideration should be given to the need for, and practicality of the installation of cameras in voids above or below data centre spaces.

Where the computer room space accommodates equipment and data owned by multiple entities, close liaison with those entities should be employed to determine any monitoring requirements.

Monitoring of VSS images should be in “real-time” and “event driven” with images relayed to an appropriately secured area, with only authorized access permitted (e.g. on-site guarding personnel). Recorded images shall be retained in accordance with local data protection regulations. If no such regulation exists, then the images should be retained for a minimum of 31 days.

Use and recording of images for the prevention and detection of crime shall take into consideration national or local regulations.

11.2.3 Intruder and holdup alarm systems

11.2.3.1 Requirements

Where justified and based on the necessary security level (see 7.2), which is determined by the output of the risk assessment of 5.2, the intruder and hold-up alarm system (I&HAS) shall take into consideration the requirements of applicable regional and national standards, respectively, with the security grade selected in line with the necessary security level.

NOTE For Europe, the EN 50131 series[21] is applicable.

11.2.3.2 Recommendations

Specialist advice should be obtained in order to select the appropriate I&HAS technology as a variety of solutions exist.

Critical areas and other areas indicated by a risk assessment or operational requirements should be monitored and supported by an intruder detection system. Where there is an operational requirement, or requirement indicated by the results of a risk assessment indicating that a local police response is required, the system shall send an alert that conforms with the requirements or the alarm receiver.

Responses to the activation of the intruder detection system will be incorporated into the local site operating procedures.

11.2.4 Access control systems

11.2.4.1 Requirements

Where justified and based on the necessary security level (see 6.1.4), which is determined by the output of the risk assessment of 5.2, the access control system shall meet the requirements of IEC 60839-11-1 and IEC 60839-11-2 with the security grade selected in line with the necessary security level.

NOTE Further information is provided in IEC 60839–11–2.

The requirements for each element of the access control system shall be determined taking into account:

— the type of control (i.e. mechanical lock, electronic lock, intercom system);

— the directionality of boundary access control (i.e. uni-directional, bi-directional);

— the prevention of passback;

— the prevention of repeated use of access technology;

— alarm generation upon access attempt without prior authorization (sabotage protection);

— the application of timed access controls for certain spaces.

11.2.4.2 Recommendations

Integration of the access control system (e.g. electronic locks and sensors with the VSS system) should be considered. Utilization of a combination of different authentication methods (card, PIN, biometrics, etc.) should be considered.

11.2.5 Event and alarm monitoring

Systems and facilities for the remote monitoring of alarms shall take into consideration the applicable regional and national standards, respectively. It should be ensured that security systems used have a coordinated time.

NOTE For Europe, the EN 50136 series[22] and EN 50518[23] are applicable.

Annex A
(informative)

Pressure relief: additional information

A.1 General

The following information is typically considered by designers of a firefighting system which requires the provision of pressure relief (both under- and over-pressure) within the spaces served.

A.2 Design considerations

Where required following the assessment:

a) each structurally segregated area within the protected space should be equipped with a separate pressure relief device or other means of pressure relief;

b) the pressure relief device should be installed so as to make sure that it is not positioned in the immediate discharge area of the nozzles of the extinguishing system;

c) the pressure required for opening should be higher than the geodetic pressure generated by the extinguishing gas at the level of the pressure relief vent (if the extinguishing gas is heavier than air, a geodetic pressure builds up in the lower part of the room depending on the density ratio of extinguishing gas/air and on the room height. Pressure relief devices opening by over-pressure and installed in the lower part of the room could cause the extinguishing gas to escape after the flooding process, in particular under the effect of leaks in the upper part of the room);

d) pressure relief should not be provided by means of active exhaust suction devices;

e) the pressure relief device should be sufficiently dimensioned, taking into the account the allowable overpressure in the room, the maximum mass flow during the activation of the extinguishing process and the type of pressure relief (resistance coefficient of the vent, pressure drop in a duct);

f) in order to avoid personal and property damage, the fire and extinguishing gases released by the pressure relief device should not result in a hazard outside the extinguishing zone.

   For this reason, the pressure relief should lead directly through a vent into the open.

   If pressure relief into the open requires the use of a duct:

   1) the pressure drop of the duct should be calculated additionally and considered for the dimensioning of the cross-sectional surface;

   2) the duct should be suitable for taking up both the pressures and the gas flows;

   3) the duct should be sufficiently gas tight and should not be equipped with other outlets;

   4) the duct should be designed so as to make sure that during pressure relief the fire is prevented from spreading into other areas and that damage of the duct resulting in a failure can be excluded.

   In exceptional cases where pressure relief is possible only via ventilation system, the above requirements apply to the ducts used. Account should be taken of the flow velocities and the possible failure of the shut-off devices.

g) the pressure relief device should close after completed pressure relief and equalization of room pressure;

h) pressure relief devices depending on an external power supply should be triggered directly by the extinguishing system or by the component triggering the extinguishing system and should be energized by one of those using non-electrical energy;

i) where electrically triggered pressure relief devices are used:

   1) guidelines for the triggering of extinguishing systems should apply;

   2) they should be provided with a monitored back-up power supply adequate for guaranteeing sufficient pressure relief for the specified hold time;

   3) if pressure relief is provided by means of a vent or a duct directly into the open and if no regulations for fire protection in terms of a fire resistant segregation of the perimeter walls containing the pressure relief vents is observed, louvered shutters may be used which open as a result of their own weight or via reset springs at a certain overpressure in the room, i.e. switching into an inclined position and returning to home position after a decrease of pressure, thus closing the aperture. If pressure relief is provided by means of a fire rated vent which complies to the fire resistant segregation of the perimeter walls, louvered shutters/flaps may be used which open at a certain overpressure in the room and close by their own weight or via reset springs, i.e. switching into an inclined position and returning to home position after a decrease of pressure, thus closing the aperture;

   4) as an alternative, pressure relief shutters or vents may be used which are opened and closed e.g. by a pressure container which is directly controlled (i.e. opened and closed) by the extinguishing system. If requirements in terms of a structural segregation are to be observed, the pressure relief devices should be designed accordingly.

Bibliography

[1] ISO/IEC/TS 22237-7, *Information technology — Data centre facilities and infrastructures — Part 7: Management and operational information*

[2] ISO/IEC/TS 22237-30, *Information technology — Data centre facilities and infrastructures — Part 30: Earthquake risk and impact analysis*

[3] ISO/IEC 30129, *Information technology — Telecommunications bonding networks for buildings and other structures*

[4] IEC 60839-11-31, *Alarm and electronic security systems — Part 11-31: Electronic access control systems — IP interoperability implementation based on Web services — Core specification*

[5] IEC 60839-11-32, *Alarm and electronic security systems — Part 11-32: Electronic access control systems — IP interoperability implementation based on Web services — Access control specification*

[6] IEC 62676 (all parts), *Video surveillance systems for use in security applications*

[7] IEC 62676-4, *Video surveillance systems for use in security applications - Part 4: Application guidelines*

[8] ISO 6183, *Fire protection equipment — Carbon dioxide extinguishing systems for use on premises — Design and installation*

[9] ISO 7240-14, *Fire detection and alarm systems — Part 14: Design, installation, commissioning and service of fire detection and fire alarm systems in and around buildings*

[10] EN 3 (all parts), *Portable fire extinguishers*

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

[12] EN 54-1, *Fire detection and fire alarm systems — Part 1: Introduction*

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

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

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

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

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

[18] EN 15004 (all parts), *Fixed firefighting systems — Gas extinguishing systems*

[19] EN 15276-2, *Fixed firefighting systems — Condensed aerosol extinguishing systems — Part 2: Design, installation and maintenance*

[20] EN 16750, *Fixed firefighting systems — Oxygen reduction systems — Design, installation, planning and maintenance*

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

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

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

[24] CEN/TS 54-14, *Fire detection and fire alarm systems — Part 14: Guidelines for planning, design, installation, commissioning, use and maintenance*

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

[26] CLC/TS 50398, *Alarm systems — Combined and integrated alarm systems — General requirements*

[27] JIS Z 9290-(all parts), *Protection against lightning*

[28] NFPA 10, *Standard for portable fire extinguishers*

[29] NFPA 11, *Standard for low-, medium-, and high-expansion foam*

[30] NFPA 11A, *Standard for Medium- and High-Expansion Foam Systems*

[31] NFPA 12, *Standard on carbon dioxide extinguishing systems*

[32] NFPA 72, *National fire alarm and signaling code*

[33] NFPA 75, *Standard for the fire protection of information technology equipment*

[34] NFPA 76, *Standard for the fire protection of telecommunications facilities*

[35] NFPA 750, *Standard on water mist fire protection systems*

[36] NFPA 780, *Standard for the installation of lightning protection systems*

[37] NFPA 2001, *Standard on clean agent fire extinguishing systems*

[38] NFPA 2010, *Standard for fixed aerosol fire-extinguishing systems*

[39] ISO/IEC/TS 22237-5, *Information technology — Data centre facilities and infrastructures — Part 5: Telecommunications cabling infrastructure*

[40] Fire Service Act of Japan

ICS 13.220.99; 35.020; 13.310

Price based on 35 pages