TECHNICAL SPECIFICATION

ISO/IEC TS 22237-6

First edition
2018-05

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 TS 22237-6:2018(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

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

For an explanation on 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 the following URL: www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 39, *Sustainability for and by Information Technology.*

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

Introduction

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

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

The implementation of data centres varies in terms of:

a) purpose (enterprise, co-location, co-hosting, or network operator);

b) security level;

c) physical size;

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

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

The ISO/IEC TS 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, facility managers, ICT managers, project managers, main contractors;

2) architects, consultants, building designers and builders, system and installation designers;

3) facility and infrastructure integrators, suppliers of equipment;

4) installers, maintainers.

At the time of publication of this document, the ISO/IEC TS 22237 series will comprise the following documents:

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

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

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

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

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

ISO/IEC TS 22237-6, *Information technology — Data centre facilities and infrastructures — Part 6: Security systems*;

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

The inter-relationship of the specifications within the ISO/IEC TS 22237 series is shown in Figure 1.

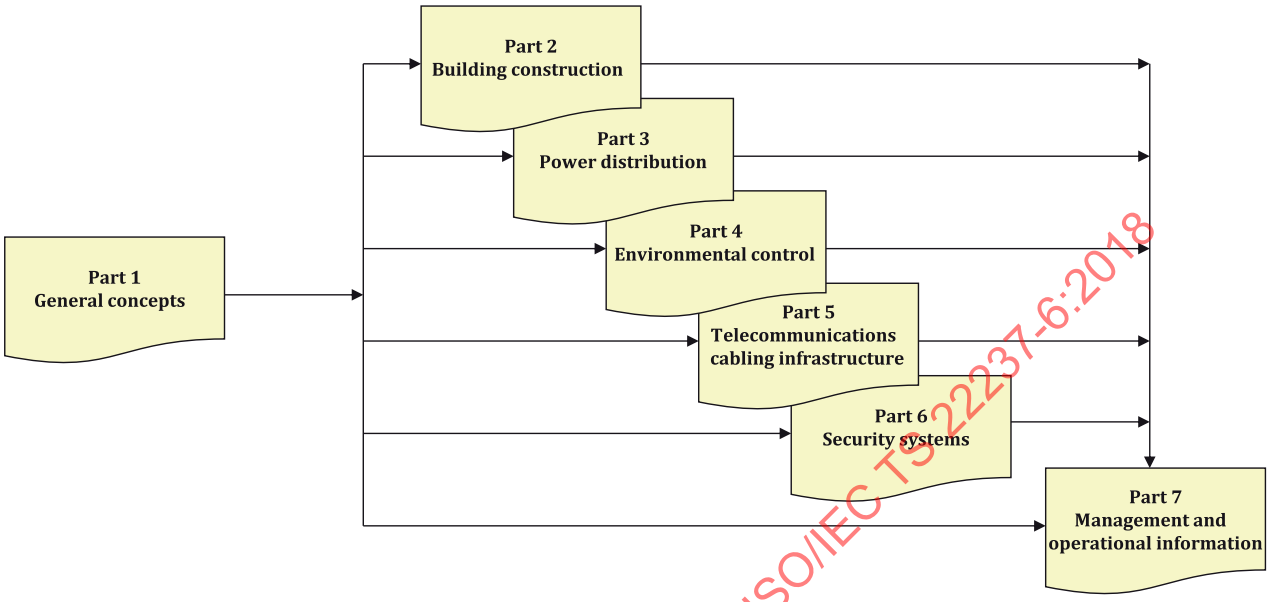

Figure 1 — Schematic relationship between the ISO/IEC TS 22237 series of documents

ISO/IEC TS 22237-2 to ISO/IEC TS 22237-6 specify requirements and recommendations for particular facilities and infrastructures to support the relevant classification for "availability", "physical security" and "energy efficiency enablement" selected from EN 50600-1.

This document, addresses the physical security of facilities and infrastructure within data centres together with the interfaces for monitoring the performance of those facilities and infrastructures in line with ISO/IEC TS 22237-7 (in accordance with the requirements of ISO/IEC TS 22237-1).

ISO/IEC TS 22237-7 addresses the operational and management information (in accordance with the requirements of ISO/IEC TS 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 TS 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 addresses the physical security of data centres based upon the criteria and classifications for "availability", "security" and "energy efficiency enablement" within ISO/IEC TS 22237-1.

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

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

a) unauthorized access addressing constructional, organizational and technological solutions;

b) fire events igniting within data centre spaces;

c) other events within or outside the data centre spaces, which would affect the defined level of protection.

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 may be of assistance in meeting these standards and regulations.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

ISO/IEC TS 22237-2:2018, *Information technology — Data centre facilities and infrastructures — Part 2: Building construction*

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

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

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

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

IEC 62676-1-1:2014, *Video surveillance systems for use in security applications — Part 1-1: System requirements — General*

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

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

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

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

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

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

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

EN 1634 (all parts), *Fire resistance and smoke control tests for door and shutter assemblies, openable windows and elements of building hardware*

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

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

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

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

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

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

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

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

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 TS 22237-1 and the following apply.

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

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

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

3.1.1
forcible threat
threat exhibited by physical force

3.1.2
hold time
time during which a concentration of fire extinguishant is maintained at an effective level with the space being protected

3.1.3
information technology equipment
equipment providing data storage, processing and transport services together with equipment dedicated to providing direct connection to core and/or access networks

3.1.4
residual risk
remaining risk(s) posed to the data centre assets requiring protection following the deployment of appropriate countermeasures

3.1.5
security manager
individual with overall responsible for all operational security aspects of the data centre, including logical and physical control mechanisms or processes

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

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

3.2 Abbreviated terms

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

I&HAS intruder and holdup alarm systems

VSS video surveillance system

4 Conformance

For a data centre to conform to this document:

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

5 Physical security

5.1 General

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

5.3 provides minimum requirements for the data centres spaces defined in ISO/IEC TS 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) fire events originating within data centres spaces (Clause 7);
c) other events within (see Clause 8) or outside (see Clause 9) the data centre spaces, which would affect the defined level of protection.

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

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

5.2 Risk assessment

The requirements for operational security should be determined by the organization responsible for data centre assets. The requirements should be determined following a risk assessment based on the threats posed to the data, and the "classification" of that data. See ISO/IEC TS 22237-1 for further information regarding risk assessment methodologies.

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

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

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

c) threat (forcible or surreptitious) analysis: for example, posed by 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.

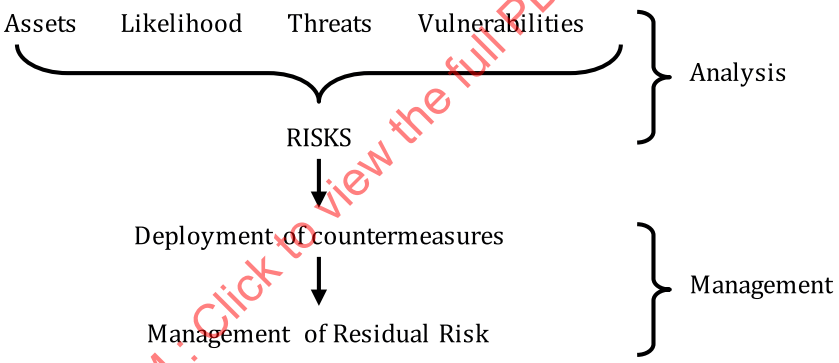

Figure 2 — Risk assessment concepts

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

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 the mitigate the risk(s);

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

5.3 Designation of data centre spaces — Protection Classes

Each of the data centre spaces, independent of the size or purpose of the data centre, is designated as being of a particular Protection Class. There is no concept of a data centre of a given Protection Class.

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

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

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

All telecommunications equipment and connections to the telecommunications cabling infrastructure shall be in areas of Protection Class 3. Where pathways containing telecommunication cabling are routed in areas of a lower Protection Class they shall be monitored for unauthorized access.

In addition, the risk assessment of 5.2 together with the construction and configuration of the data centre described in 6.2 will require other spaces to be defined in terms of Protection Class. An example of this is shown in Table 1.

Table 1 — Examples of Protection Classes for data centre spaces

Protection Class 1	Protection Class 2	Protection Class 3	Protection Class 4
Personnel entrances to buildings or structures containing data centre spaces	The internal access to docking bays (the barrier of the docking bay providing the interface between Protection Classes 1 and 2) External premises security spaces Personnel entrances to the data centre spaces Storage spaces Holding spaces Testing spaces Data centre office spaces	Premises entrance facility[a,b] Building entrance facilities[b] Computer room spaces Control room space Data centre security spaces	Cabinets, cages or rows of cabinets within the computer room space
a This applies to premises entrance facilities which are within the control of the data centre.			
b Access restrictions apply to pathways leading to areas of Protection Classes of a lower Protection Class.			

6 Protection Class against unauthorized access

6.1 General

This document applies the four Protection Classes in relation to access to spaces accommodating the elements of the different facilities and infrastructures as detailed in Table 2 (in accordance with ISO/IEC TS 22237-1).

Table 2 — 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 personnel (employees and visitors).	Area restricted to specified employees and visitors (other personnel with access to Class 2 shall be accompanied by personnel authorized to access Class 3 areas).	Area restricted to specified employees who have an identified need to have access (other personnel with access to Class 2 or 3 areas shall be accompanied by personnel 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.

It should not be assumed that:

a) all areas of a given Protection Class are accessible to persons having access to an area of that Protection Class;

b) persons having access to an area of that Protection Class have access to all areas of a lower Protection Class.

This clause defines the rules for implementing such 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. The implementation of physical security shall be effected according to the philosophy shown schematically in Figure 3, referred to as the “Onion Skin” or “Defence in Depth” approach/model.

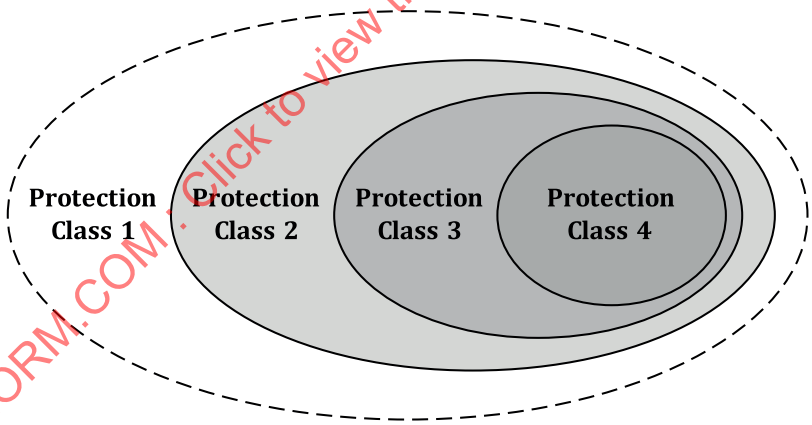

Figure 3 — Protection Classes within the 4-layer physical protection model

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

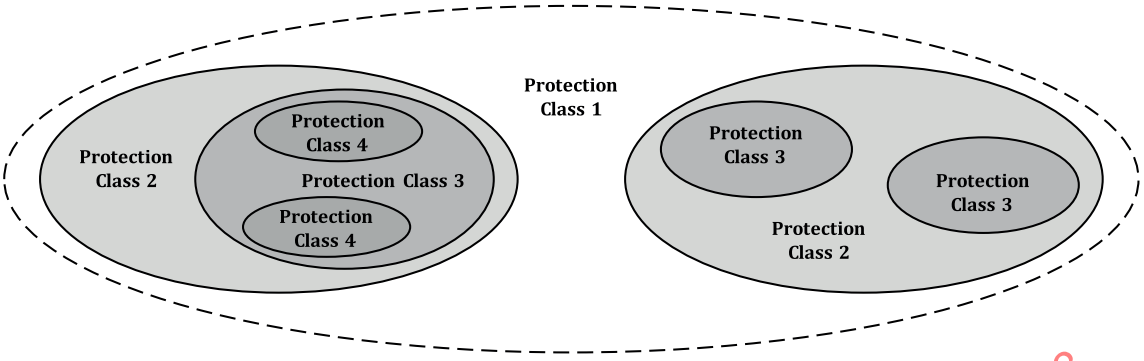

Figure 4 — Protection Class islands

5.3 provides examples of the Protection Classes applied to data centre spaces but the technological solutions to 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 TS 22237-2 to ISO/IEC TS 22237-6 cross boundaries from one Protection Class to another they shall be provided with protection suitable to the highest Protection Class interconnected as shown in Figure 5.

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

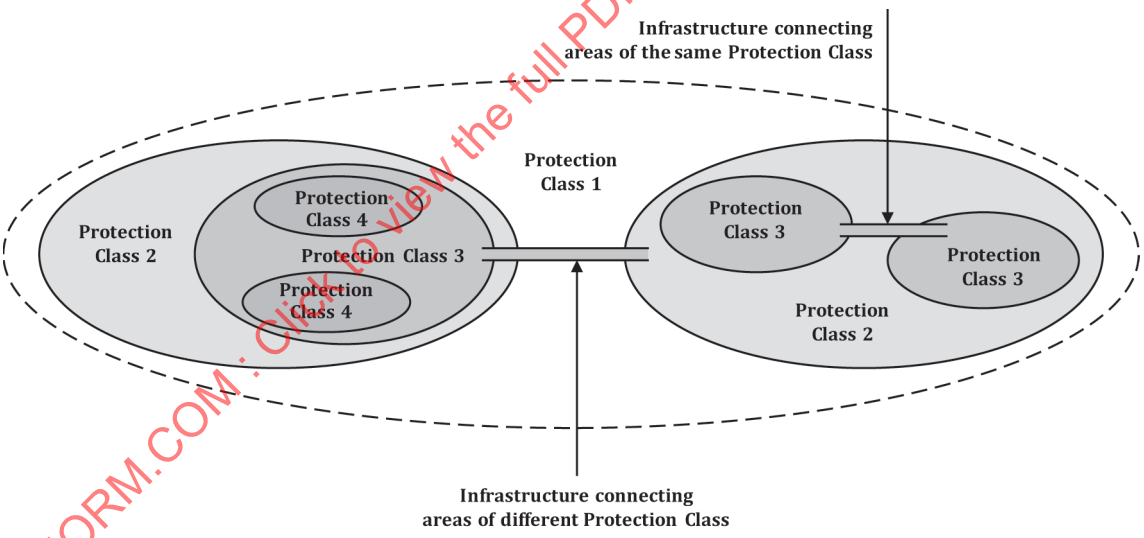

Figure 5 — Interconnection between Protection Class islands

Access control systems of a given Protection Class shall 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 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 may be required as determined by the output of the risk assessment process or the site security assessment.

6.2 Implementation

6.2.1 General

The barrier defining Protection Class 1 is the outer perimeter of the premises containing the data centre. 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.

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 6:

a) 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);

b) 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;

c) 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;

d) the Protection Class system operates horizontally and vertically (e.g. risers, lift shafts, stair wells, atriums, light-wells) for the buildings and structures i.e. if the roof-top is considered to be of Protection Class 1, appropriate barriers will be required to any roof-top structures which accommodate facilities or infrastructure requiring a higher Protection Class.

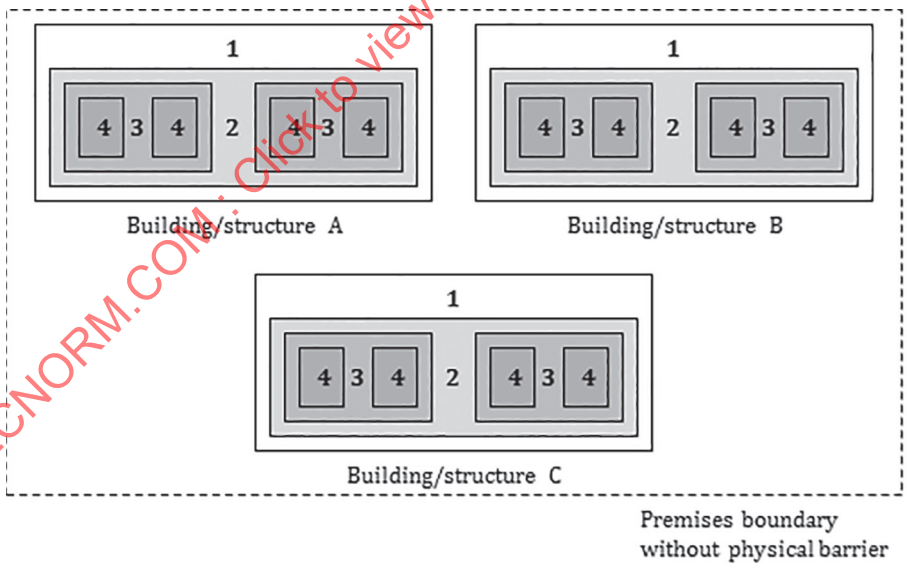

Figure 6 — Example of Protection Classes applied to data centre premises without external barriers

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 7:

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 designated data centre space and the area requiring Protection Class 4;

5) the Protection Class system operates horizontally and vertically (e.g. risers, lift shafts, stair wells, atriums, light-wells) for the buildings and structures i.e. if the roof-top is considered to be of Protection Class 2, appropriate barriers will be required to any roof-top structures which accommodate facilities or infrastructure requiring a higher Protection Class;

   This only applies in relation to protection against unauthorized access. For the purposes of protection against external environmental events a roof-top is considered to be a Protection Class 1 boundary only and any roof-top structures require additional protection.

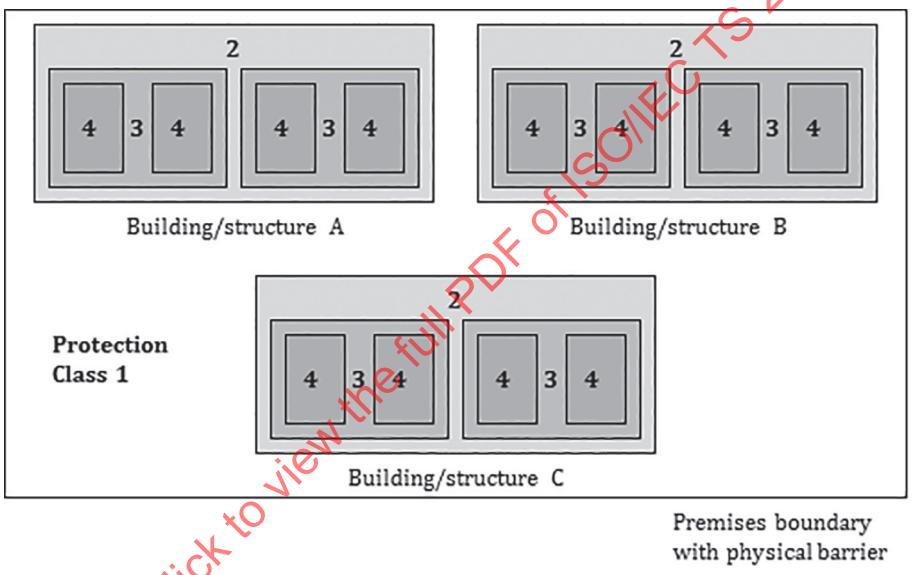

Figure 7 — Example of Protection Classes applied to data centre premises with external barriers

In Figure 7, the buildings/structures shown may be dedicated to specific spaces serving the various data centre infrastructures e.g. generator space or transformer space. Each building/structure shall apply appropriate barriers to protect the relevant infrastructure element. In addition, the barriers may be required to provide visual and acoustic screening.

As described above, roof-tops may be considered Protection Class 1 or 2, depending on the configuration of the premises containing the data centre. Any openings in roof-tops shall be protected in accordance with the Protection Class of the space immediately below the opening. In addition, any roof-top structures dedicated to specific spaces serving the various data centre infrastructures shall apply appropriate barriers to protect the relevant infrastructure element.

Any access routes to the roof, for purposes of maintenance and repair of the roof, roof-top structures and, where relevant, to infrastructure elements, shall be within areas of Protection Class equal to or higher than that of the roof-top.

The requirements for the barriers between areas of different Protection Class in relation to protection against unauthorized access are not based on their physical construction i.e. they may be fences, exterior

or interior walls of buildings together with doors and other penetrations fitted with appropriate systems (see Clause 10).

Any access points to spaces of a given Protection Class that are dedicated to a particular facility or infrastructure shall not provide an access route to general data centre spaces, or spaces which are dedicated to other facilities or infrastructures, of either the same or higher protection Class.

The combination of resistance offered by the boundaries of each Protection Class together with the monitoring of those boundaries shall present a person attempting unauthorized access by means of forcible threats with increasingly difficult challenges. The materials comprising those barriers shall be considered in terms of:

— the tools and equipment against which they are proven to provide resistance;

— the time required to penetrate those barriers using those tools and equipment.

Any surveillance and monitoring equipment shall take the penetration times into account. The requirements for access control systems which allow persons to cross the boundaries are described in Clause 10.

When a building houses more than the data centre, each boundary which is shared with external parties shall be considered as an external wall, i.e. a boundary of Protection Class 1. Any boundary which is shared with an adjacent building, not part of the data centre, shall be considered as an external wall, i.e. a boundary of Protection Class 1.

6.2.2 Access to the data centre premises

6.2.2.1 General

6.2.2.1.1 Requirements

Access routes shall be clearly signed to segregate employees, visitors and deliveries to the data centre.

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

6.2.2.1.2 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) sterile zones for the management and handling of visitors or deliveries;

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

6.2.2.2 Parking

6.2.2.2.1 Requirements

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

The outcome of a risk analysis, taking into account the security requirements of the site and the importance of the data involved, may place restrictions upon:

a) the designated location, and minimum distance from the data centre spaces, of any parking areas for visitors and unauthorized vehicles;

b) the designated location, and minimum distance from the data centre spaces, of any parking areas for employees;

c) the designated location, and minimum distance from the data centre spaces, of any parking areas for delivery vehicles;

d) the designated location, and minimum distance from the data centre spaces, of any parking areas for maintenance and emergency vehicles.

6.2.2.2.2 Recommendations

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 searching requirements;

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

f) operational security process requirements.

6.2.2.3 Visitors

6.2.2.3.1 Requirements

Suitable space shall be allocated for the processing of visitors.

6.2.2.3.2 Recommendations

Any doors leading to the data centre spaces should have appropriate door mechanisms in place to provide access to authorized personnel and authorized visitors only. 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 the visitor access.

6.2.2.4 Deliveries

6.2.2.4.1 Requirements

Movement of goods and personnel from the loading bay to other data centre spaces shall be controlled by appropriate security mechanisms (e.g. interlocks) applied at the inner boundary of the loading bay.

To accommodate deliveries in data centres requiring high levels of security control, additional operational controls shall be employed to support the delivery process. These may include but are not limited to:

a) provision of a sterile zone, or 'airlock' system at an external barrier of the loading bay by which goods are moved into the loading bay following which the external barrier is closed while the goods are unloaded;

b) provision for VSS monitoring.

6.2.2.4.2 Recommendations

No recommendations.

6.2.3 Protection Class 1

6.2.3.1 Requirements

6.2.3.1.1 Construction

The external boundary of areas designated Protection Class 1 shall be provided with an identifiable physical barrier.

All pedestrian doorsets, windows, grilles and shutters which form the external boundary of Protection Class 1 shall meet EN 1627:2011, Resistance Class 2.

Doors (and windows) at the boundary of Protection Class 1 shall be designed such that, when locked, any components (e.g. hinges) which would allow the door (and windows) to be opened are inaccessible from the areas outside Protection Class 1. Where this is not possible, the door (window) shall be protected by the use of a dowel and socket arrangements (i.e. dog bolts).

Pedestrian access to an area of Protection Class 1 shall be physically separated from the pedestrian access to any contained areas of a Protection Class 2. Vehicular access to an area of Protection Class 1 shall be physically separated from the vehicular access to any contained areas of a Protection Class 2.

Any penetrations of the physical barrier defining the outer boundary of Protection Class 1 shall prevent vehicle access to the premises except for those necessary to:

a) support operation (i.e. employee vehicles and associated parking facilities subject to the risk analysis of 6.2.2.2) and maintenance of the premises;

b) respond to emergency situations.

6.2.3.1.2 Organizational processes

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

6.2.3.2 Recommendations

Consideration should be given to:

a) pedestrian barriers or defined security boundary;

b) level and nature of security lighting;

c) type and style of VSS;

d) physical delay measures for buildings;

e) operational security procedures;

f) hostile vehicle mitigation;

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

h) access control requirements;

i) internal I&HAS;

j) mail and delivery screening protocols.

Where possible, the area outside but in close proximity to the physical barrier defining the outer boundary of Protection Class 1 should be subject to monitoring/surveillance subject to relevant controls for management and handling of images and other data (see Clause 10).

The areas of Protection Class 1:

1) should be subject to monitoring/surveillance subject to relevant controls for management and handling of images and other data;

2) should not contain objects (temporary or permanent) that would disrupt the effectiveness of monitoring/surveillance (e.g. any planting should be low growing, no parking outside designated areas, no shelters, etc).

6.2.4 Protection Class 2

6.2.4.1 General

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

6.2.4.2 Requirements

6.2.4.2.1 Construction

The external boundary of areas designated Protection Class 2 shall be provided with an identifiable physical barrier. If the boundary of a Protection Class 2 area is co-located with one or more boundaries of areas of Protection Class 1 then the boundary of the lower Protection Class shall meet the requirements of the Protection Class 2.

If deemed necessary following the risk assessment of 5.2, all pedestrian doorsets, windows, curtain walling, grilles and shutters which form the external boundary of Protection Class 2 shall meet EN 1627:2011, Resistance Class 3 unless alternative mitigation is employed.

Doors (and windows) at the boundary of Protection Class 2 shall be designed such that, when locked, any components (e.g. hinges) which would allow the door (and windows) to be opened are inaccessible from the areas of Protection Class 1. Where this is not possible, the door (window) shall be protected by the use of a dowel and socket arrangements (i.e. dog bolts).

Any penetrations of the physical barrier defining the outer boundary of Protection Class 2 shall prevent personnel access except for those persons authorized (both employees and visitors) to enter the spaces of the data centre. Such penetrations include those which are open or may be opened to enable normal or emergency function of the data centre infrastructures (such as pressure relief for gaseous extinguishing systems) where the prevention mechanisms shall be taken into account in the functional design of the penetration.

Vehicular access to an area of Protection Class 2 shall be physically separated from the vehicular access to any contained areas of a Protection Class 3.

Any penetrations of the physical barrier defining the outer boundary of Protection Class 2 enabling vehicular access shall incorporate a system which restricts access. Access shall only be allowed to those vehicles and personnel necessary to:

a) support operation and maintenance of the data centres facilities and infrastructures;

b) respond to emergency situations.

Access to areas of Protection Class 3 from docking bays, for receipt and dispatch of materials and equipment, shall be separate from personnel entrances to areas of Protection Class 3.

6.2.4.2.2 Organizational processes

The differing nature and function of the spaces serving the facilities and infrastructures of the data centre may 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).

Procedures shall be in place to detect and prevent:

a) undesirable or unnecessary access between areas of Protection Class 2;

b) unauthorized access from an area of Protection Class 2 to areas of a higher Protection Class.

Such procedures include an inspection by security personnel or scanning devices.

Procedures shall be in place to detect and prevent pedestrian access to the data centre spaces e.g. by means of an interlock for materials only.

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

6.2.4.3 Recommendations

Monitoring/surveillance should be applied to areas of Protection Class 2 subject to relevant controls for management and handling of images and other data.

Except in emergency situations, there should be only one penetration of the barrier to allow general personnel access to, and egress from, each area of Protection Class 2.

Any fittings attached to penetrations of the Protection Class 2 boundaries with the intention of restricting access from areas of Protection Class 1 (intrusion bars fitted to windows) should be designed to prevent attachment of towing cables, etc.

6.2.5 Protection Class 3

6.2.5.1 Requirements

6.2.5.1.1 Construction

The external boundary of areas designated Protection Class 3 shall be provided with an identifiable physical barrier.

If deemed necessary following the risk assessment of 5.2, all pedestrian doorsets, windows, grilles and shutters which form the external boundary of Protection Class 3 shall meet EN 1627:2011, Resistance Class 4 unless alternative mitigation is employed.

The boundaries of areas of Protection Class 3 shall not be co-located with those of Protection Class 1 (e.g. external walls or roof-tops of premises) unless appropriate constructional aspects ensure resistance equivalent to those of any pedestrian doorsets, windows.

If a boundary of an area of Protection Class 3 is co-located with one or more boundaries of areas of Protection Class 2 then the resistance to forced entry across the combined boundary shall be the sum of those applicable to Protection Class 2 and Protection Class 3.

Doors (and windows) at the boundary of Protection Class 3 shall be designed such that, when locked, any components (e.g. hinges) which would allow the door (and windows) to be opened are inaccessible from the areas of Protection Class 2. Where this is not possible, the door (window) shall be protected by the use of a dowel and socket arrangements (i.e. dog bolts).

Any penetrations of the physical barrier defining the outer boundary of Protection Class 3 shall prevent personnel access except for those persons authorized to enter areas of:

a) Protection Class 3;

b) Protection Class 2 provided that they are accompanied by personnel authorized to enter areas of Protection Class 3.

Such penetrations include those which are open or may be opened to enable normal or emergency function of the data centre infrastructures (such as pressure relief for gaseous extinguishing systems) where the prevention mechanisms shall be taken into account in the functional design of the penetration.

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.

6.2.5.1.2 Organizational processes

Procedures shall be in place to:

a) detect and prevent undesirable or unnecessary access between areas of Protection Class 3;

b) detect and prevent unauthorized access from an area of Protection Class 3 to areas of a Protection Class 4;

c) monitor and/or control the number of persons entering and leaving areas of Protection Class 3;

d) monitor and/or control materials and equipment entering and leaving areas of Protection Class 3.

Such procedures:

1) include a single person interlock for general pedestrian access together with or separate from interlocks for materials and equipment;

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

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

6.2.5.2 Recommendations

Monitoring/surveillance should be applied to areas of Protection Class 3 subject to relevant controls for management and handling of images and other data.

6.2.6 Protection Class 4

6.2.6.1 Requirements

6.2.6.1.1 Construction

The external boundary of areas designated Protection Class 4 shall be provided with an identifiable physical barrier.

If deemed necessary following the risk assessment of 5.2, all pedestrian doorsets, windows, grilles and shutters which form the external boundary of Protection Class 4 shall meet EN 1627:2011, Resistance Class 4 unless alternative mitigation is employed.

The boundaries of areas of Protection Class 4 shall not be co-located with those of Protection Class 1 (e.g. external walls or roof-tops of premises) unless appropriate constructional aspects ensure resistance equivalent to those of any pedestrian doorsets, windows (where justified following the risk assessment of 5.2), grilles and shutters.

If a boundary of a Protection Class 4 area is co-located with one or more boundaries of areas of a lower Protection Class then the resistance to forced entry across the combined boundary shall be the sum of those applicable to all the Protection Classes.

Doors (and windows) at the boundary of Protection Class 4 shall be designed such that, when locked, any components (e.g. hinges) which would allow the door (and windows) to be opened are inaccessible from the areas of Protection Class 3. Where this is not possible, the door (window) shall be protected by the use of a dowel and socket arrangements (i.e. dog bolts).

Any penetrations of the physical barrier defining the outer boundary of Protection Class 4 shall prevent personnel access except for those persons authorized to enter areas of:

a) Protection Class 4;

b) Protection Class 3 provided that they are accompanied by personnel authorized to enter areas of Protection Class 4.

Such penetrations include those which are open or may be opened to enable normal or emergency function of the data centre infrastructures (such as pressure relief for gaseous extinguishing systems) where the prevention mechanisms shall be taken into account in the functional design of the penetration.

6.2.6.1.2 Organizational processes

Procedures shall be in place to:

a) detect and prevent undesirable or unnecessary access between areas of Protection Class 4;

b) detect and prevent unauthorized access into areas of Protection Class 4;

c) monitor and/or control the number of persons entering and leaving areas of Protection Class 4;

d) monitor and/or control materials and equipment entering and leaving areas of Protection Class 4.

Such procedures:

1) include a single person interlock for general pedestrian access together with or separate from interlocks for materials and equipment;

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

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

6.2.6.2 Recommendations

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

Monitoring/surveillance should be applied to areas of Protection Class 4 subject to relevant controls for management and handling of images and other data.

6.2.7 Cabinets and arrangement of cabinets

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

7 Protection Class against fire events igniting within data centre spaces

7.1 General

7.1.1 Protection Classes

This document applies the four Protection Classes in relation to fire originating within spaces accommodating the elements of the different facilities and infrastructures as detailed in Table 3 (in accordance with ISO/IEC TS 22237-1).

Table 3 — 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 to be protected against fire by a detection and suppression system which maintains the function of that area during a fire in that area or one in a Class 1 area.	The area requires to be protected against fire by a detection and suppression system which maintains the function of that area during a fire in that area or one in a Class 1 or Class 2 area.	The area requires to be protected against fire by a detection and suppression system which enables critical data centre function to be secured during a fire in that area or one elsewhere in the data centre.

NOTE 1 For the purposes of this clause the term “fire suppression system” is synonymous with the term “fixed firefighting system”.

NOTE 2 For the purposes of this clause the term “fire detection system” is synonymous with the term “fire detection and alarm system”.

The type of fire detection (and alarm) system and firefighting system selected for each space shall take into account the Protection Class of the space and approach to be taken to maintaining the function of the space. For example, maintenance of function may be considered as a time period adequate to implement a disaster recovery programme i.e. by transferring the function of the data centre space to another space within or external to the data centre.

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.

This Clause addresses the fire detection and alarm, fixed and portable firefighting systems to be applied to the data centre spaces. It does not intentionally conflict with national or local regulations concerning fire safety. 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 require the disruption of all power supplies (including back-up systems) in non-data centre spaces.

7.1.2 Fire compartments and barriers

7.1.2.1 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 the components comprising, 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 resistance rating of doors or windows in a wall shall comply with the resistance rating of the walls and barriers. Their ability to resist the impact of firefighting water shall be taken into account.

Advice regarding the scheduling, installation sequence and suitability of particular fire-stopping techniques shall be sought from both the manufacturer and specialist contractors at the earliest possible opportunity.

Fire-stopping techniques applied to pathways that penetrate the boundary of a fire compartment shall be specified in terms of:

a) the fire rating, construction details and orientation of the fire compartment structure;

b) the type, size and material of the fire barrier penetration to be fire-stopped;

c) where there is no housing surrounding the components passing through the fire barrier, the size of the fire barrier penetration and the percentage fill at the penetration;

d) where there is a housing surrounding the components passing through the fire barrier, the size of the penetration internally and the percentage fill within the housing;

e) a detailed description of the fire-stopping system including any additional supports required for the components passing through the penetration.

The fire-stopping technique applied shall be proven to meet the specification criteria using the test methods given in EN 1366-3. Techniques based upon interacting components shall be regarded as a complete system and should only be used as such.

NOTE Additional information regarding high performance fire-stopping techniques can be sought from the offshore and petrochemical industries.

The system specifier shall:

1) obtain documentary evidence from the manufacturer/supplier which defines the capability of the fire-stopping technique;

2) verify that the proposed specification is covered within the scope of this document;

3) ensure that the fire-stopping technique is fit for purpose.

Fire-stopping techniques shall be installed in accordance with the manufacturer's/supplier's installation instructions. Each fire stop shall be clearly labelled or otherwise marked to indicate its function so as to be identifiable during future penetrations.

The design of, and access, to fire barriers shall enable periodic inspection in accordance with established schedules.

In the case of a fire alarm, fire damper devices shall close.

7.1.2.2 Recommendations

Fire damper devices should be equipped with their own power source and should be able to close automatically.

7.1.3 Fire detection and fire alarm systems

7.1.3.1 Requirements

To support the objectives of Table 3, fire alarm systems shall be installed in all data centre spaces that directly affect the availability of data centre facilities and infrastructures.

Consideration shall be given to the need for early detection of combustion products with pre-alarm. The pre-alarm shall not automatically disrupt the function of the facilities and infrastructures of the data centre (e.g. air flow produced by the environmental control systems shall not be disrupted). Where used:

— components of the fire detection and alarm system shall comply with the relevant parts of the EN 54 series;

— the system shall comply with EN 54-13.

Where used in spaces of Protection Class 3 and above, smoke detection (aspirating) systems shall comply with EN 54-20:2006, Sensitivity Class A or B.

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

7.1.3.2 Recommendations

CEN/TS 54-14 contains guidelines for the planning, design, installation, commissioning, use and maintenance of fire detection and alarm systems.

NOTE ISO 7240-14 provides alternative guidance.

7.1.4 Fixed firefighting systems

7.1.4.1 General

To support the objectives of Table 3, a fixed firefighting system shall be provided if it is deemed necessary in the outcome of risk assessment.

If a fixed firefighting system is to be installed 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; or a combination of these:

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

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

7.1.4.2 Fire extinguishing systems using gaseous agents

Gaseous systems shall be designed, installed and maintained considering the following standards:

a) ISO 14520-1 series (for gases other than carbon dioxide);

b) ISO 6183 (for carbon dioxide systems). 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.

With specific reference to cabinet gas systems, the following additional factors shall be taken into account:

1) the mechanical, climatic and electromagnetic impact of the discharge of the gaseous system on the equipment accommodated by the cabinet;

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

7.1.4.3 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 in accordance with EN 16750.

7.1.4.4 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 in accordance with EN 12845;

b) water mist — which shall be designed, installed and maintained in accordance with CEN/TS 14972 or national standards if 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."

7.1.4.5 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 in accordance with CEN/TS 14816.

7.1.4.6 Foam systems

Foam systems should not be used in occupied spaces containing electronic equipment.

Foam systems shall be designed, installed and maintained in accordance with EN 13565-2.

7.1.5 Portable firefighting equipment

Where portable fire extinguishers are provided:

a) they shall conform to the EN 3 series;

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

7.1.6 Structural considerations

Where gaseous extinguishing systems are used:

a) the boundaries of the protected space shall have sufficient structural strength and integrity to contain the extinguishant discharge and pressure relief shall be used to prevent excessive over- or under-pressurization of the protected space;

b) 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;

c) 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 ventilation of the protected space;

d) 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;

e) 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.

7.2 Implementation of Protection Class requirements

7.2.1 Protection Class 1

The detection of fire in an area of Protection Class 1 shall initiate a warning in other spaces of the data centre.

7.2.2 Protection Class 2

The detection of fire in an area of Protection Class 2 shall initiate a warning in other spaces of the data centre.

Spaces of Protection Class 2 shall be provided with detection and suppression solutions in accordance with 7.1.3 and 7.1.4 respectively.

In addition, a space of Protection Class 2 shall be able to maintain its intended function for a minimum of 60 min following the detection of fire in an adjacent area of Protection Class 1.

The boundaries (walls, floors and ceilings) of areas of Protection Class 2 shall provide the desired degree of physical protection against internal fire events in adjacent areas of Protection Class 1.

If an "early detection of fire" system is employed, the doors shall be smoke-tight in accordance with the EN 1634 series.

Doors shall have a fire rating of 60 min minimum in accordance with the EN 1634 series.

NOTE This requirement postdates and replaces those of ISO/IEC TS 22237–2:2018, 7.8.1.

7.2.3 Protection Classes 3 and 4

The detection of fire in an area shall initiate a warning in other spaces of the data centre.

Spaces of Protection Classes 3 and 4 shall be provided with detection and suppression solutions in accordance with 7.1.3 and 7.1.4 respectively.

The boundaries (walls, floors and ceilings) of areas of Protection Class 3 shall provide the desired degree of physical protection against internal fire events in adjacent areas of Protection Class 2.

If an "early detection of fire" system is employed the doors shall be smoke-tight in accordance with the EN 1634 series.

Doors shall have a fire rating of 90 min minimum in accordance with the EN 1634 series.

NOTE This requirement postdates and replaces those of ISO/IEC TS 22237–2:2018, 7.8.1.

Constructions meeting the requirements of EN 1047-2 provide the desired protection and may be located in any space.

8 Protection Class against environmental events (other than fire) within data centre spaces

8.1 Protection Classes

This document applies the four Protection Classes in relation to protection against internal environmental events (other than fire events of Clause 7) to spaces accommodating the elements of the different facilities and infrastructures as detailed in Table 4 (in accordance with ISO/IEC TS 22237-1).

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

Table 4 — 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 special protection applied	Mitigation applied	Mitigation applied	Mitigation applied

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. This clause defines the rules for implementing such Classes.

8.2 Implementation

8.2.1 General

Consideration shall be given to the electromagnetic environment of the data centre spaces which may disrupt the effective operation of data processing, data storage and data transport and of the supporting infrastructures. Procurement, installation and operation of equipment shall consider the electromagnetic compatibility characteristics of the data centre as a whole.

The design of the telecommunications cabling infrastructure and associated power distribution infrastructures shall take into account the security requirements of the data:

a) stored, processed or transported in the data centre;

b) controlling the operation of the infrastructures of the data centre.

Consideration shall be given to the protection against 'surreptitious' attacks against the walling structure; which may require additional wall linings to detect this form of penetration.

8.2.2 Protection Class 1

No special protection applied.

8.2.3 Protection Class 2

8.2.3.1 General

Areas of Protection Class 2 provide protection and maintain their function when subject to internal environmental events from an area of Protection Class 1.

8.2.3.2 Requirements

Interior walls shall provide the desired degree of physical protection against internal environmental events and provide a barrier against the ingress of contaminants (particulate, liquid or gaseous) including water resulting from firefighting activity.

Drainage systems and other piping systems (including those of the environmental control systems of ISO/IEC TS 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).

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.

An area of Protection Class 2 and above shall not be located underneath any openings in roof spaces unless drainage routes are provided that lie outside the area.

8.2.3.3 Recommendations

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

8.2.4 Protection Class 3

8.2.4.1 General

Areas of Protection Class 3 provide protection and maintain their function when subject to internal environmental events from an area of Protection Class 2.

8.2.4.2 Requirements

In addition to the requirements of 8.2.3.2, ceilings, doors and cable entries shall provide protection against the ingress of contaminants (particulate, liquid or gaseous) including water resulting from firefighting activity.

8.2.4.3 Recommendations

In addition to the recommendations of 8.2.3.3, room-in-room constructions should be considered.

8.2.5 Protection Class 4

8.2.5.1 General

Areas of Protection Class 4 provide protection and maintain their function when subject to internal environmental events from an area of Protection Class 3.

8.2.5.2 Requirements

In addition to the requirements of 8.2.4.2, room-in-room constructions shall be considered.

8.2.5.3 Recommendations

In addition to the recommendations of 8.2.4.3, room-in-room constructions should provide environments consistent capable of complying with the test regimes of EN 1047-2.

9 Protection Class against environmental events outside the data centre spaces

9.1 Protection Classes

This document applies the four Protection Classes in relation to protection against external environmental events to spaces accommodating the elements of the different facilities and infrastructures as detailed in Table 5 (in accordance with ISO/IEC TS 22237-1).

Examples of external environmental events include fire, electromagnetic interference, vibration (including earthquakes), flooding, gas and dust hazards.

Table 5 — Protection Classes against external environmental events

Type of protection	Class 1	Class 2	Class 3	Class 4
Protection against external environmental events	No special protection applied	Mitigation applied	Mitigation applied	Mitigation applied

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. This clause defines the rules for implementing such Classes.

9.2 Implementation

9.2.1 General

Boundaries of each Protection Class shall provide the desired degree of physical protection against external environmental events.

Consideration shall be given to external sources of electromagnetic interference which may 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.

For the purposes of this subclause, mobile telephone signals are considered to be external environmental issues since they provide communication via external networks. However, if screening of external mobile telephone signals is provided by a Protection Class boundary, then either:

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

