Rittal – The System.
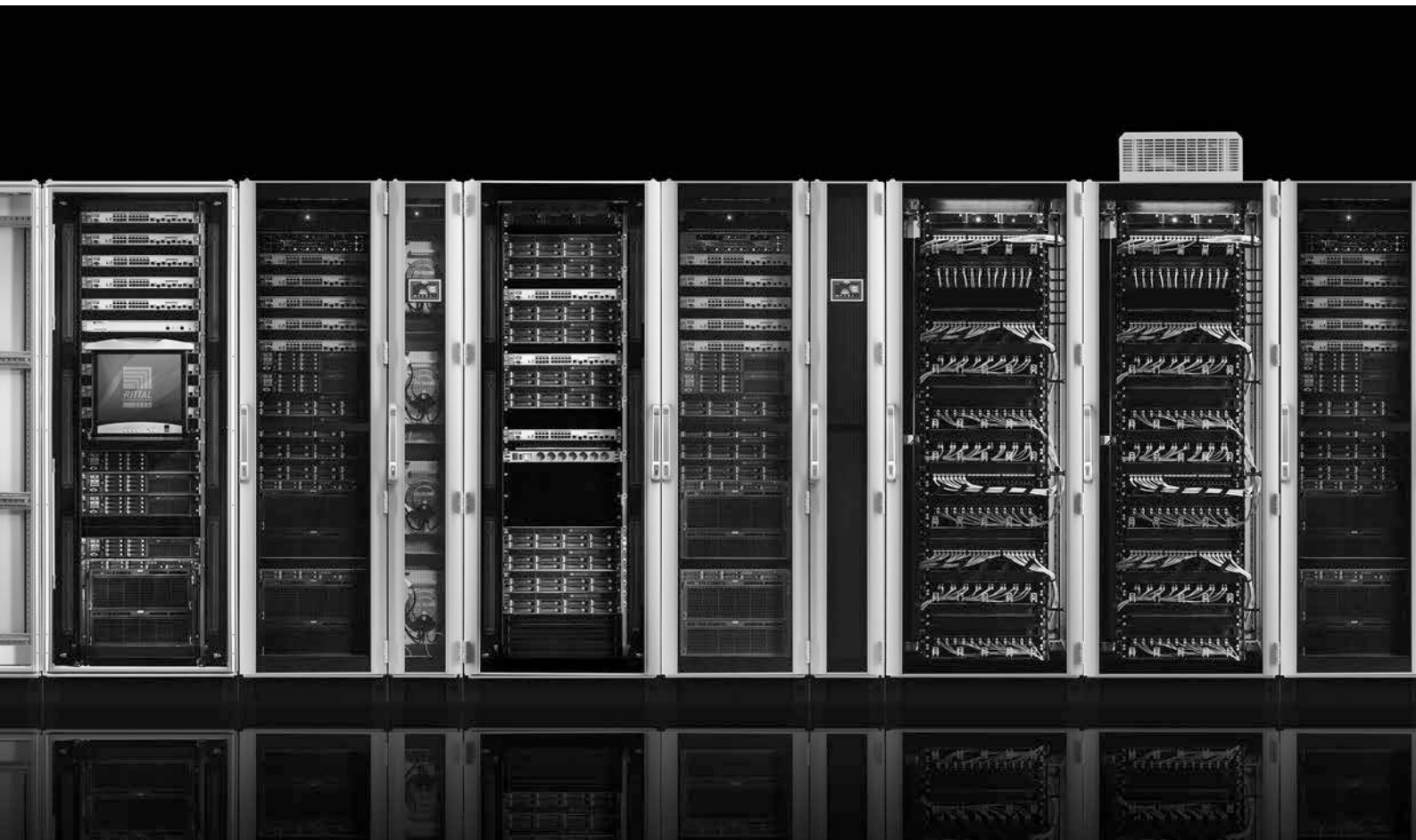
Faster – better – everywhere.

White paper
Physical security in IT and data centre technology

Bernd Hanstein

RITTAL

Contents

Author: Bernd Hanstein

After receiving a Diplom degree in physics from the Justus Liebig University in Gießen in 1987, Bernd Hanstein joined the central research unit of Siemens AG, where he worked on test methods for highly integrated circuitry. He subsequently occupied various positions within the Public Networks Group of Siemens AG, with responsibility for the implementation of major ICT projects. In 2002, Bernd Hanstein moved to Siemens VDO Automotive as senior manager responsible for the worldwide system testing of in-vehicle multimedia devices. Since 2007, he has been head of IT product management at Rittal in Herborn. His key interests: IT components, RiMatrix system solutions and data centre technologies.

List of images

List of tables

Executive summary

Data centres represent a key technology in an increasingly digitised world. They house the servers and storage systems with their associated network components so that applications are present with the agreed availability and the required performance. Equally important is the physical infrastructure that provides the power and cooling for these components, as well as permitting the monitoring of all the operating parameters.

Increasing importance is being given to all aspects of security. This starts with well-known anti-virus protection and firewall systems, although protection against physical threats also calls for increasing attention. Besides defence against such very real threats as burglary and theft, it also involves avoiding unwanted eavesdropping via the EMC irradiation from IT equipment, as well as the "traditional" potential dangers of fire, smoke, water and dust, to only name but a few.

This white paper explores each of these threat scenarios and reveals the measures that can be used to counter physical hazards.

Introduction

Computer technology represents one of the basic building blocks of modern society. There is no area where computer and networked communication have not arrived. These services, whether they are consciously perceived or simply work quietly in the background, call for computing power and network infrastructure. This must also be physically provided in data centres by hardware and software in an appropriate environment comprising climate control, power supply and network connection - in spite of all the virtualisation. But data centres should also guard against physical threats such as fire, water damage, burglary and theft. Protection against these risks is becoming increasingly important due to the world's constantly advancing digitisation.
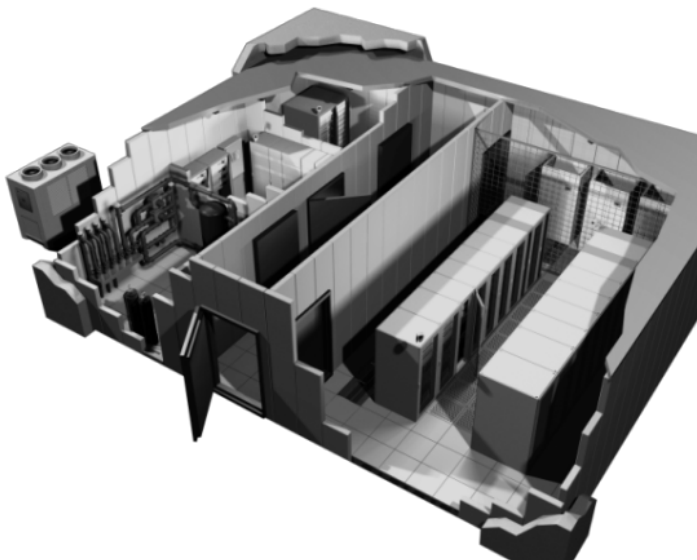
Figure 1: Sketch of the physical infrastructure of a data centre

The protection of data centres from physical hazards must begin on several levels, because the threats also act through different vectors. The basic protection catalogues of the Federal Office for Security in Information Technology (BSI) list 27 risks for data centres [Ref. 1], including everything from "Acts of God" (force majeure), organisational defects and technical failures to intentional action.

However, on the other hand, help is provided by proven IT security concepts that are tailored to the respective hazards. For example, fire protection walls, whose cable glands are also able to withstand fire for a sufficiently long period. An even bigger problem is water vapour, which is emitted by concrete at high temperatures due to its crystalline residual moisture. Here, vapour barriers and heat protection fittings must be used. Numerous aspects must be observed when it comes to planning, facilities and construction so that a data centre can reliably protect its contents. This applies of course not only to rooms made of conventional masonry, but also for modular

versions of data centres, as Rittal also offers with its basic protection room, High availability Room and the Micro Data Centre.

Where once a few days of downtime per year were perfectly acceptable, industry's increasing dependence on digital systems has led to far tighter requirements. And that with good reason, because IT failures are very costly for the German economy. Medium-sized firms alone have to cope with the loss of business-critical IT systems worth up to €380,000 per company and year. This has emerged from a survey carried out in 2013 by the market research company Techconsult [Ref. 2] involving 300 companies with 200 to 4,999 employees. A survey by EMC [Ref. 3] also revealed there had been either data losses or downtimes at 56% of companies in Germany during the previous twelve months.

An all-round approach always helps when it comes to protecting complex systems. A data centre consists of a large number of systems: climate control, power supply and distribution, network connectivity, access control, and last but not least the structural shell, designed as a conventionally built room or as a modular "room-in-room" system. It is not so important that the individual components are resistant to fire and water but rather that the entire system meets these criteria. Users must scrutinise certifications and quality seals carefully to find out whether the protective effect covers the entire system and not only individual items. That is why the successfully completed testing of the system is always more meaningful with respect to the protective effect than a series of individual tests.

Climate control, power supply, data connection – all of these elements need to be optimally integrated into the data centre concept and their management needs to be coupled to data centre administration. Rittal offers special white papers on many of these areas such as climate control, 19"-inch enclosure technology and data centre management.

Test procedures and test institutes

Even though complete packages are available for the certification of data centres, ultimately it comes down to examining the individual systems. For a data centre, fire protection, as well as protection against water damage or dust and smoke must be backed up by individual verifications. A whole series of international standards cover this, including the Deutsche Institut für Normung (German Institute for Standardisation, DIN), European standards (EN), the European Certification Body GmbH (ECB) and the International Organization for Standardization (ISO).

The advantage of including agreed standards in individual contracts is that lawsuits can be avoided from the outset because the standards represent clear definitions. In purchase and service contract law, when it comes to material defects, the prima facie evidence shows that user of the standard has complied with the necessary attention. Thus, the user can also reject any charges of negligence.

Manufacturers themselves can also carry out tests, if they are accredited for performing tests, for example, the protection class test.

The ECB in particular is now regarded by many users as the authoritative certifier for data centres. The European Certification Body GmbH is a neutral, accredited certification body in accordance with ISO/IEC 17065 [Ref. 4]. It grants "ECB•S" certificates for the products of the security industry. ECB•S certification from the ESSA is based solely on the requirements of European standards and is internationally recognised. Each product is individually registered and its technical production may be subject unannounced quality monitoring at any time. For the insurance industry, this certification is a reliable and objective basis for the calculation of risks and of the associated safety classification. The Rittal High Availability room also has ECB•S certification.

Figure 2: Rittal ECB•S certificate

The most serious physical hazards for a data centre are fire, water, dust and fumes, debris, EM radiation and unauthorised access. One or more relevant standards must be adhered to for each of these risk vectors. For instance, it is often necessary that a wall must have a specific fire resistance, for example, F90 or F120 according to DIN 4102 or EI 90 or EI 120 according to the EN 1363 [Ref. 8]. Such a wall will fulfil its function in a fire for 90 or respectively 120 minutes. The aim of this classification is to protect human life, not the data centre. If the IT is to be the focus of protection, then it is important that the data centre as a whole can withstand the fire – not just a wall.

The Federal Office for Information Security (BSI) is also calling for system-wide testing for IT-related areas. Thus, although Measure 1.6 "Compliance with fire safety

regulations" [Ref. 5] only demands that the existing fire protection regulations such as DIN 4102 "Fire behaviour of building materials and components" [Ref. 6] and regulations of the MBO, LBO, MLAR and the requirements of building supervisory authorities must be strictly observed. However, for rooms where important IT devices and data carriers (servers, backup, etc.) are housed, the regulations of EN 1047 Part 2 [DIN 4102 "Fire behaviour of building materials and building components" Ref. 7] be observed.

Detailed consideration of the physical threats

Fire

Fire is probably the one threat to data centres and server rooms that administrators fear most. Even small fires can cause severe damage to IT equipment and infrastructure due to the aggressive gases that are given off. Testing for fire resistance is thus very intensive. Even for the F90/EI90 component test as per DIN 4102/ EN 1363 [Ref. 6, Ref. 8], individual elements such as walls, doors and building materials are subjected to flame treatment in accordance with a uniform temperature curve. Testing is conducted at more than 1,100°C for 90 minutes. During testing, the temperature on the side away from the fire must not increase by more than 140 K (up to 180 K on occasions). Relative air humidity is not measured during this test. Depending on the building material concerned, humidity may rise to 100% after a very short time, which would be dangerous for the server and the infrastructure in the data centre.

Real protection is only guaranteed by a system test in which the complete data centre and all its components such as doors, as well as bulkheads for cables and pipes are tested under conditions similar to those in an emergency. A system test in accordance with EN 1047-2 [DIN 4102 "Fire behaviour of building materials and building components" Ref. 7] for example, requires that flames are applied for 60 minutes. This is followed by a 24-hour cooling-off period in the closed fire furnace. This time is referred to as a "post-heating period". The test piece remains in the fire area until the highest temperature in the specimen is reached after a few hours. Particular attention is paid to structurally weak points such as doors, doorframes and cable and pipe entry systems. In order to pass the test, the internal temperature must not exceed the starting temperature by more than 50 Kelvin, and – equally important – the relative humidity must not exceed 85%. Products that have successfully passed these and other tests required by EN 1047-2 are registered in the ECB•S database. Even if DIN 4102 [Ref. 6] and EN 1363 [Ref. 8] do generally describe component tests, complete system solutions such as safes and rooms can be tested in accordance with these standards.

Corrosive gases and smoke

Gas-tightness and resistance to smoke are important requirements that data centres and server rooms have to meet. For one thing, the factor of tightness matters when it comes to keeping the smoke from a fire within the server room and not spreading to other parts of the building.

Fires in IT environments are not extinguished with water but with inert gases or by oxygen deprivation, for example. This only functions reliably if the gases remain within the room and do not reach the rest of the building through leakage. Similarly, fire prevention by oxygen deprivation is bound to fail if fresh air is drawn into the room through doors, windows or structural defects. Tightness of seal plays an equally important role if there is a fire outside the data centre. The IT components in the data centre have to be protected from aggressive gases because the circuit boards in the servers, switches and other hardware could corrode.

Relevant standards for certification are DIN 18095 DIN 18095 [Ref. 9]/EN 1634 [Ref. 10]. Part 3 of EN 1634 specifies a test procedure and the corresponding test conditions for determining the leakage of hot and cold smoke from one side of a seal to the other. This "leakage rate" is measured for each test condition investigated. For data centres, tests are conducted on doors and pressure relief valves and flaps because these usually represent the only movable openings into the room. Due to the fire, a pressure of up to 50 Pa builds up on the side exposed to the smoke; the pressure difference between the two sides drives the smoke through all the gaps and openings that are present. A door that functions as part of the fire safety system must hinder the passage of smoke to ensure that the conditions on the other side of the door remain bearable.

Tests are carried out in a test chamber; the test piece is installed in the front of it. A blower system provides the necessary pressure while a heater generates temperatures of around 200°C to recreate the temperature of the smoke. Gaps due to the nature of the system, such as door thresholds or gaps between door wings are measured and recorded. Automatic closing mechanisms also have to be tried out a few times before the test. But this short test does not replace endurance testing of the mechanisms – it is simply aimed at making sure that the door can be properly closed. The real test for smoke resistance is performed at different pressure levels of up to 50 Pa and at room temperatures of 20°C and at 200°C. Successfully tested specimens must not exceed an air change rate between the inside and the outside as defined in the standard. During the tests, it is also important to record if (and which) elements of the door are deformed by the heat, and whether the door can still be opened after the test has been completed.

Falling debris

The dangers caused by falling debris also have to be considered. The forces so released can wreak great destruction on the hardware and infrastructure. In addition

to the fire tests for the security rooms and safes, the standards also set out impact und drop tests.

EN 1047-2 [Ref 7.] describes an impact test for high availability rooms. This test is conducted after the room has already been exposed to flames for 45 minutes. DIN 4102 also describes an impact test. A wall used as a firewall (fire resistance test according to DIN 4102 ETK [Ref. 6]) must be able to withstand a defined impact stress after exposure to flame. If the wall is a load-bearing one, compressive stress is also applied to the test piece.

This impact resistance is regulated in a separate standard, Norm EN 50102 [Ref. 11]. It is specified in the IK code and provides information on the level of external mechanical protection. The relevant product standard regulates how the test is performed. Five loads are carried out per area (evenly distributed, oscillating or free fall). The test piece must be mounted on a rigid frame and must not give way. Exposed areas such as hinges or locks are also subjected to stress. After testing, the test piece must be fully functional and, in particular, must not exhibit any adverse effects on its protection class.

IP protection categories: Protection against dust, water and solid particles

Dust is rarely seen as a physical danger and it will practically never cause any IT problems in a typical office environment. The situation is different in production plants where dust is generated in large quantities and extraction systems are unable to remove it completely. Here too, IT systems have to function and must not be exposed to dust without any protection. Water, however, is threat to IT equipment that everyone instantly recognises as such. During outdoor use, IT equipment must not be wet or even damp. Water damage from broken pipes or the like also has to be overcome. Depending on the application and the object concerned, there is a range of protection levels, which are defined by the IP (International Protection) categories in accordance with EN 60529 [Ref. 12]. Tests as per EN 60529 classify the protection of the electrical equipment up to a rated voltage of 72.5 kV in terms of enclosures, covers, and the like.

The IP protection classes use a simple combination of numbers to describe how the enclosure protects its contents. Generally, the aim is to protect people from coming into contact with hazardous parts inside the enclosure. Similarly, the equipment inside the enclosure must be protected from penetration by solid foreign objects and water. In this connection, the danger emanates from active parts, which can cause electric shock and mechanical parts that are dangerous if contact is made.

The protection category is specified in the form "IP XY". The first digits run from 0 to 6, with the respectively next highest number including all the ones below it. They define the level of protection against solid objects and dust.

Code	Protection property
IP 1x	Protected against solid foreign objects with a diameter of 50 mm and greater
IP 2x	Protected against solid foreign objects with a diameter of 12.5 mm and greater
IP 3x	Protected against solid foreign objects with a diameter of 2.5 mm and greater
IP 4x	Protected against solid foreign objects with a diameter of 1.0 mm and greater
IP 5x	Dust-protected
IP 6x	Dust-tight

Table 1: IP classification – protection against dust and solids

The second digit indicates the level of protection against water. They range from 0 to 8; up to 6, the same containment mechanism applies as for the first digit.

Code	Protection property
IP x1	Vertically dripping water
IP x2	Vertically dripping water, enclosure tilted by 15°
IP x3	Water spraying at an angle of 60° to the vertical
IP x4	Water splashing from any direction
IP x5	Water jets from any direction
IP x6	Powerful water jets from any direction
IP x7	Temporary immersion in water under standardised pressure and time conditions
IP x8	Continuous immersion in water

Table 2: IP classification – protection against water

In Germany, the tests are largely carried out by the TÜV and VDE bodies. In addition, the test laboratories at the manufacturers of such products are concerned with protection category testing. Thus, the Rittal QM test laboratory is accredited by the DAkkS (Germany's National Accreditation Body) and by the UL for protection categories, among other things. Besides the IP tests as per EN, protection category testing is also carried out in accordance with UL and NEMA specifications

Figure 3: Protection category testing

Testing is performed for a short time and without long-term exposure, such as may occur during periods of rain that last hours or days. This means that a high degree of protection is not equivalent to being suitable for installation in the open air. In the tests for the penetration by foreign bodies and dust, attempts are first made to penetrate the test piece with objects of a defined size. For the tests from IP 5x and up, a dust chamber is used with or without the possibility to generate negative pressure. Talcum powder is introduced as a test material; its presence on surfaces can be easily demonstrated. In the case of IP 5x, dust may only penetrate to the extent that the satisfactory operation of the device or safety are not compromised. The highest value as per DIN EN 62208 [Ref. 13] is one gram of dust per square metre of floor space. With IP 6x, no dust whatsoever may penetrate.

The tests are carried out with liquids through drip devices, as well as swivel pipes and showerheads with different nozzle diameters. Dip tanks are also used with IP x7 and up. All tests are judged by the same criterion: The water must not have any harmful effects.

Protection against unauthorised access

Normally, data centres inside buildings need to be well protected against intruders, because these first have to overcome all the other obstacles such as doors, reception area, cameras and observant staff. Nevertheless, it is important that a room containing expensive hardware and important data can resist even an attempted burglary. The Resistance Class (RC) states how well this can be done. The "RC" standard is defined in DIN V ENV 1627ff [Ref. 14]. The attack with tools is

made analogously to DIN EN 1630/2011-09 [Ref. 15] and a six-stage classification system is used.

A distinction is made, based on the capabilities of the offenders and the tools they are equipped with. The spectrum ranges from inexperienced offenders and vandals without tools through to experienced, highly motivated perpetrators, who have access to a large number of high-performance power tools. In each case, there are limits to the time that the test piece must withstand the attack for in order to pass the test.

For the category "RC 1", the components must have a limited-to-low level of basic protection against attempted burglaries involving physical force such as kicking, being jumped on, being shoulder-charged, or being pushed up and pulled out. In addition, a non-destructive manipulation test lasting up to three minutes is carried out to dismantle any screwed-on components that can be detached from outside with small tools. The duration of the attack applies for each point attacked. If, for example a complete safe is being tested, there are a number of points that may be attacked, such as the door (hinge side), door (frame side) and cable entry points. The total time is derived from the sum of all the points of attack. The remaining categories are summarised in the following table.

Code	Duration	Experience	Description / implements
RC 2	3 min	Occasional, inexperienced offender	Simple tools: screwdrivers, pliers and wedges
RC 3	5 min	Repeat offender	Additionally: second screwdriver and a crowbar
RC 4	10 min	Experienced offender	Additionally: Sawing and impact tools such as an axe, a crowbar, hammer and chisel, and a cordless drill
RC 5/ RC6	10 min	Experienced offender	Other hand-operated tools, up to and including a drill, jigsaw or reciprocating saw and an angle grinder with a wheel diameter of up to 250 mm.

Table 3: RC classification system – protection against unauthorised access

EM protection

Electromagnetic fields are an inevitable consequence when current flows. The energy that is irradiated, the electromagnetic radiation, is undesirable and in some cases harmful. Strong fields can have a negative effect on other electronic devices and make information accessible to unwanted eavesdroppers.

If they are planned and fitted out correctly, IT security rooms will protect hardware and data from the negative consequences of EM radiation. On the one hand, EMC describes how such devices can be protected against harmful interference from external sources. Here, some special measures are necessary.

A security room, in its basic state, does not offer any continuous and defined level of protection. However, EMC also involves preventing electromagnetic radiation from which unauthorised persons can tap valuable and sensitive information. IT security rooms from Rittal already have basic EMC protection when they leave the factory, and this can be increased with the aid of additional design measures.

The following table provides an overview of the relevant standards:

Area of application	EMI	Immunity
Information technology equipment	EN 55022 (P)	EN 55024 (P)
Residential environment	EN 61000-6-3 (FG)	EN 61000-6-1 (FG)
Industrial plants	EN 61000-6-4 (FG)	EN 61000-6-2 (FG)
Signalling on low-voltage electrical installations	EN 50065-1 (P)	EN 61000-6-2 (FG)
Electrical lightning	EN 55015 (P)	EN 61000-6-2 (FG)

Table 4: EMC standards for products and product families, and generic standards

The EMC standards set emission limits for products and surroundings areas in defined frequency and field strength ranges, see DIN EN 55022 (VDE 0878-22): 2011-12 [Ref. 16], for example.

By combining these threshold values with the tiered immunity requirements for IT equipment described in **EN 55024 (VDE 0878-24): 2011-09** [Ref. 17], it is possible to ensure – to a great extent – EMC between devices of all kinds and IT equipment in everyday operation.

Area of application / test	Standards
Absorber rooms, part 1: Screen attenuation measurement	EN 50147-1 : 1996
IEEE Standard Method for Measuring the Effectiveness of Electromagnetic Shielding Enclosures	IEEE Std 299-1997

Table 5: EMC test standards (for room shielding)

The EMC characteristics of IT security rooms have to fulfil two tasks. On the one hand, they must prevent IT facilities being intentionally or unintentionally hampered by radiated electromagnetic fields while on the other hand, they have to reduce the emission of safety-relevant information from the IT device. The shielding effect of the device housing and the enclosures in which the devices are accommodated can be

increased considerably by adding extra room shielding. However, there are no normative requirements regarding this.
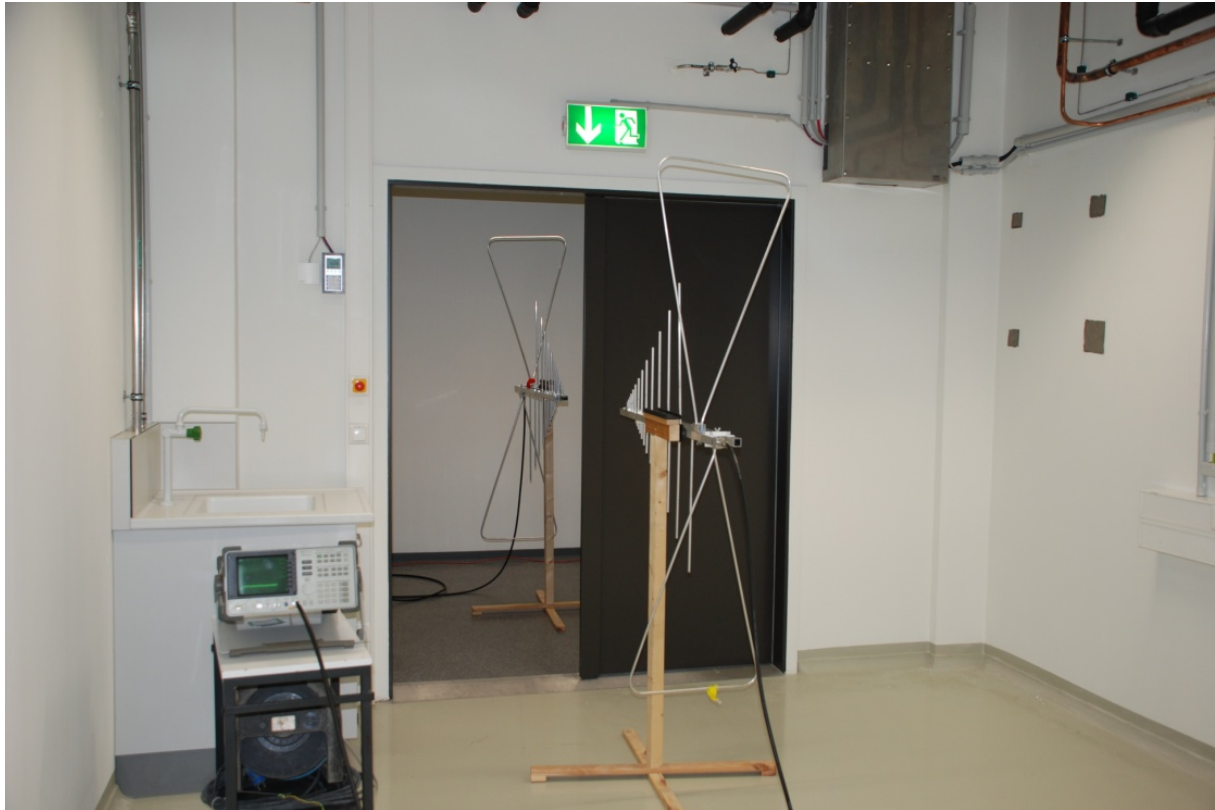

Figure 4: EMC testing

Here too, the ideal situation would be a slot-free, electrically conductive shell that neither lets signals in nor out. However, this is impossible in practice. This is because IT security rooms and data safes are composed of wall segments made of sheet steel, which enable a slot-free, conductive basic shell over wide-area, conductive connections. Openings or gaps must be shielded by suitable media, which involves a significant design effort, particularly with access doors. Just how well the shielding works determines the size of the necessary openings and the quality of the shielding elements used there, as well as their connection to the basic shell. One basic principle applies: the larger a poorly shielded opening (for rectangular openings/joints: the longest side; for round openings: diameter), the more likely there will be a loss in shielding effectiveness for the relevant frequency range.

The higher the frequency of the incident electromagnetic field, the more negative the effect of any openings in the shell. Therefore, some points such as the use of special gaskets and cable glands or the use of filter connectors must be observed. Basically speaking, the structural design of the sealing system largely determines the effectiveness of the shielding attenuation. The more attachment points for walls and hinges there are, as well as closure pressure points for doors, and the more uniform the contact pressure and the contact (low impedance) of shell and door/lid are along

the seals, the closer we will get to the ideal. Conductive special seals made of metal fabric on a foam body, as combination seals for EMC and IP protection categories, achieve high shielding attenuation values in the frequency range up to 1 GHz and beyond. They connect the bare metal interior surfaces of doors and removable side panels, roof and gland plates to the bare metal sealing edges of the enclosure body or frame.

With reasonable measures, shielding attenuation values of up to 60 dB can be implemented for security rooms in the frequency range of 30 MHz to 3 (10) GHz. The design effort required to increase shield attenuation above 60 dB for the relevant frequency range would be exceptionally high. The main applications of highly effective room shielding are for government agencies, such as the military, police, intelligence services and interior ministries. Rittal security rooms meet the basic requirements of EMC and can be upgraded at a reasonable cost to offer increased EMC protection.

You can find further information on the subject of EMC in a separate Rittal White Paper [Ref. 18].

Modular security rooms and safe solutions

In principle, any room can be used as a server room or converted to a data centre. Attention must be paid to various aspects of the IT infrastructure. Without cooling, for instance, the heat dissipation of the IT equipment quickly reaches its limits in the summer. This means that frequently, access cannot be controlled, while devices are often lying on the ground, where they can regularly be damaged by water. Modular IT security rooms or IT security safes are a sensible alternative if suitable space is available. A security room is installed in an existing room and provides everything that characterises a reliable data centre. It guards against physical dangers and offers system-proven protection for information technology.

Micro Data Centre

IT security safes, which are of smaller scale but no less professional, protect against physical hazards. These are fully equipped but compact data centres that only need to be connected to the appropriate supply lines on site. In addition to the Model A Micro Data Center (MDC) for basic protection requirements, Rittal's product range also includes the Micro Data Center B and the Micro Data Center E.

Figure 5: Micro Data Center product range: Level E, Level B, and Level A

The MDC Level A is a complete system with built-in cooling and a two-door system for simple installation and administration. It has been designed as a micro data centre for small and medium-sized businesses to protect server and storage applications, as well as business-sensitive data, and it can accommodate up to fifteen 19" units (U).

The MDC Level B is already fitted with the Rittal TS IT framework (including front and rear 19" levels) as a standard, and it is available in two different heights (42 or 47 U), as well as with two different interior depths (1000 mm and 1200 mm). The safe provides fire protection for over 90 minutes, and it has been tested in accordance with EN 1363. It provides RC 2 burglary protection and IP 56 protection class and has been tested by the "MPA" materials testing agency in Braunschweig for resistance to smoke in accordance with EN 1634.

The MDC Level E, as a safe for high safety requirements, provides fire protection for 90 minutes in accordance with DIN 4102 (compliance with the limits of EN 1047-2, ΛT 50 K, rel. humidity < 85% for 30 minutes), IP 56 protection, RC2 resistance class (optionally RC 3 or RC 4), as well as providing reliable protection against fumes.

Property	Level E	Level B	Level A
Usable U	42/47	42/47	15
Usable interior depth mm	1000/1200	1000/1200	1000
Fire protection	Fire resistance class F 90 (DIN 4102 Part 2) compliance with the limits ΔT <50 K, rel. humidity <85% for 30	Fire resistance class EI 90 / F 90 (DIN EN 1363-1: 1999/ in accordance with DIN 4102-2: 1997)	Fire resistance class F 90 (DIN 4102 Part 2) Compliance with limit values ΔT < 50K, relative humidity

	minutes		85% for 10 minutes
Burglar resistance	RC 2, optional RC 3, attack with tools analogous to DIN EN 1630/2011-09/RC 2. Optional RC IV tool attack analogous to DIN V ENV 1630/1999-04.	RC 2, attack with tools analogous to DIN EN 1630/2011-09/RC 2	RC II tool attack analogous to DIN V ENV 1630/1999-04
Protection category	IP 56 according to EN 60 529	IP 56 according to EN 60 529	IP 55 according to EN 60 529
Smoke protection	Analogous to DIN 18095-2: 1991-034)	Analogous to DIN EN 1634-3 2005-01	
Modularity	Yes	Yes	No
Enclosed during operation?	Yes	No	No
Extendibility	Yes	No	No

Table 6: Overview of MDC properties

The Micro Data Centre can be fully equipped as a compact data centre through adding modular and expandable pieces of equipment. These components from the Rittal product range include the Computer Multi Control III (CMC III) monitoring system, the DET-AC III fire alarm and extinguishing system, intelligent power distribution through the Power Distribution Unit (PDU) and the Power System Module (PSM) power distribution systems, as well as the Liquid Cooling Package (LCP) and a cooling unit.

Security rooms

A modular IT security room can be installed either in a new room or retrofitted in an existing one. Practically no dust or noise is generated during assembly; it can also be easily extended or even mounted at a different position. It frequently offers better protection against fires, water damage and EMC radiation than a conventional room does. Solutions can be selected for basic protection or for high availability requirements, depending on the level of availability required. Rittal's high availability room offers the maximum physical security for data centres and IT system locations. The system has been certified by the ECB according to the ECB S rules and fulfils the requirements of EN 1047-2 without restriction.

Figure 6: IT security room

As a rule, IT security rooms are equipped with security door systems. They can vary greatly in their design, depending on the requirements. In order to be prepared against vandalism and attempted burglary, the security door system should have a highly fire-resistant, multi-layer sheet steel door leaf with revolving door frame and all-round fire and sealing groove. Hollow rubber seals and expanding high-temperature gaskets, among other things, are mounted in the door rabbet. The closure technology represents another essential aspect. It needs to offer reliable protection from unauthorised access, and on the other hand, help people trapped in emergencies to leave the contaminated area for the open air quickly. To this end, the locks are equipped with a high-security bolt system, latch bolt and a panic release feature. The high security bolt system has a holder for the lock units. Anyone still in the room in the event of an alarm (while the door is closed) can leave at any time by using the standardised panic release. Automatic systems for closing the door need to have a variably adjustable delay.

Basic protection room GSR	Basic protection plus room GSR Plus	High Availability Room HVR
Basic protection Infrastructure of the rooms, Switchboards	**Extended basic protection** Data centres with medium security needs, back-up data centres	**High-MTBF protection** Main data centres with high security requirements, high availability solution

Table 7: Security room product range

It is almost always necessary to monitor status of the door at the entrance. Professional security rooms thus provide a door monitoring system that routes out floating contacts via a VdS-compliant interface distributor. This way, the door status can be linked to the central building management system. A door-monitoring contact is sufficient if it is only necessary to query the state of the door. With professional security rooms, the bolt itself can also be monitored, for example in order to connect it to a burglar alarm system or security centre. Doors in a system-tested security room ensure ideal protection against fire, water, burglary and other physical hazards.

A shelter that did not need any openings would be ideal. That is quite impossible because of the door alone, although the infrastructure in the security room and safe also need to be connected to climate control, power supply and network. This is the task of cable bulkheads, whose properties must not weaken the protective effect of the entire system. as hard duct systems that provide increased protection against manipulation in the field of cable entry, and as soft partitions filled with a flexible sealant, which is usually supplied as standard with security rooms. Round bulkheads, filled with sealing modules, are a different form factor. These are particularly suited for existing cables, pipes and cable trays within the building. Specialists authorised by the manufacturer should always be consulted on how to connect the bulkhead correctly. Only in this way can the full protection of the security room be guaranteed.

Criterion	Standards	GSR	HVR
System testing	Testing of the following values as complete system or design	Yes	Yes
Fire protection	ECB·S certifications to EN 1047-2, 50 K temperature increase and 85% rel. humidity up to 24 hours (reheating period), 60 minutes flame impingement time	No	Yes
	50 K temperature increase and 85% rel. humidity without reheating period, flame impingement time 30 minutes	Optional	-
	F 120 in accordance with DIN 4102	No	Yes
	F 90 in accordance with DIN 4102	Yes	-
Corrosive fire gases	Smoke gas resistance in accordance with DIN 18 095	Yes	Yes
Falling debris	Impact test at 200 kg	Yes	Yes
Water	IP x6 as per EN 60 529	Yes	Yes
	Protection against standing water	-	Yes
Dust	IP 5x as per EN 60 529	Yes	Yes
Unauthorised access	RC IV in accordance with DIN V ENV 1630, door system only	-	Yes
	RC III in accordance with DIN V ENV 1630, or DIN V 18103 (ET2)	Optional	Yes
	RC II to DIN V ENV 1630	Yes	-
EMC	Protection against high-frequency irradiation and radiation	Optional	Optional

Table 8: Overview of security room characteristics

The IT equipment in the security room has to be cooled. There are various methods of doing this; some require the supply of fresh air to the room through one or more suitable openings. In the event of a fire near the security room, such openings have to be sealed so that no smoke can enter the security room from outside. This is done by blocking the opening(s) by flaps or slide valves made of highly fire-resistant materials. In the event case of fire, the drives of such climate control slide valves or fire dampers must be independent of the power supply. Different types of drives can be realised, depending on the size, position and shape of the opening. Thus, climate control slide valves can be used to ventilate an electric drive system under normal circumstances. If there is a fire, the flap must close the opening in a purely mechanical way, for example, by using a spring or a magnet.

Another related component is the over-pressure slide valve. If a fire extinguishing system with an inert gas or a chemical extinguisher medium is activated, the excess pressure will have to be dissipated. This is done by a corresponding, highly fire-resistant slide valve that features an electro-pneumatic drive. In the event of an alarm, the excess pressure is discharged by opening the slide valve briefly. With purely mechanical fasteners in particular, the seals must be both perfectly adapted to the application and highly effective. This requires very flexible and tightly closing sealing tapes with very high temperature resistances.

To ensure security in the data centre and thus in security rooms and safes, a high-quality early-warning fire detection system (together with high-quality fire-fighting equipment) is essential.

In order to intervene as quickly as possible, an early-warning fire detection system is needed that reacts to even the smallest smoke emissions. Scattered light detectors are mainly used. The smoke density is measured by the way the light beam is scattered by the smoke particles present. Scattered light detectors operate both as a point-type detectors on the ceiling and in highly sensitive smoke extraction systems.

Due to the targeted air routing within a data centre, the smoke emitted only arrives at the detectors on the ceiling either very late or not at all. An active smoke extraction system is therefore unavoidable in order to ensure early detection.

Active extinguishing is usually triggered by a double-alarm or two-zone system, so that false alarms are prevented wherever possible. Inert gases or a chemical extinguishing gas are mainly used for extinguishing. In contrast, extinguishing foam and powder fire extinguisher systems must not be used because they would damage the information technology systems and their power supply units. Fires can be prevented by using an oxygen reduction system. This reduces the amount of oxygen in the data centre to such an extent that it is impossible for a fire to occur.

References

Ref. 1   BSI Grundschutzkatalog (*basic protection catalogue*), Link: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html

Ref. 2   Studie "Kritische IT-Systeme im Mittelstand", Techconsult im Auftrag von HP Deutschland, 2013, (*Critical IT systems in medium-sized companies, Techconsult on behalf of HP Germany*), Link: http://www.softexpress.de/Media/seite_hardware/ProactiveCare/HP_Ergebnispr%C3%A4sentation_Kritische_IT_Mittelstand_Handout_2013.pdf

Ref. 3   EMC study, 2014, Link: http://germany.emc.com/about/news/press/2014/20141209-01.htm

Ref. 4   ISO/IEC 17065, Link: http://www.iso.org/iso/catalogue_detail.htm?csnumber=46568

Ref. 5   BSI measure 1.6 „Einhaltung von Brandschutzvorschriften", (*Compliance with fire safety regulations*) Link: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m01/m01006.html

Ref. 6   DIN 4102 "Fire behaviour of building materials and building components"

Ref. 7   EN 1047-2, Link: http://www.beuth.de/langanzeige/DIN+EN+1047-2/113261910.html

Ref. 8   EN 1363 "Fire resistance tests - Part 1: General requirements"

Ref. 9   DIN 18095 "Doors; Smoke control doors; concepts and requirements"

Ref. 10   EN 1634 "Fire resistance and smoke control tests for door and shutter assemblies, openable windows and elements of building hardware"

Ref. 11   EN 50102 "Degrees of protection provided by enclosures for electrical equipment against external mechanical impact (IK code)"

Ref. 12   EN 60529 "Degrees of protection provided by enclosures (IP Code)"

Ref. 13   DIN EN 62208 "Empty enclosures for low-voltage switchgear and control gear assemblies – General requirements"

Ref. 14   DIN EN 1627 "Pedestrian doorsets, windows, curtain walling, grilles and shutters – Burglar resistance – Requirements and classification"

Ref. 15   DIN EN 1630 "Pedestrian doorsets, windows, curtain walling, grilles and shutters – Burglar resistance – Test method for the determination of resistance to manual burglary attempts"

Ref. 16   DIN EN 55022 "Information technology equipment – Radio disturbance characteristics – Limits and methods of measurement"

Ref. 17   DIN EN 55024 "Information technology equipment – Immunity characteristics – Limits and methods of measurement"

Ref. 18   Rittal – "IT white paper – EMC protection in security rooms"

List of abbreviations

BSI	Bundesamt für Sicherheit in der Informationstechnik (German Federal Office for Information Security)
CMC	Computer Multi Control (Rittal monitoring system for IT infrastructure)
DAkkS	Deutsche Akkreditierungsstelle (German Accreditation Body)
DETA-AC	Rittal fire alarm and extinguishing system
DIN	Deutsches Institut für Normung (German Institute for Standardisation)
ECB	European Certification Body GmbH
EMC	Electromagnetic compatibility
EN	European norm
ESSA	European Security Systems Association (ESSA) e.V.
GSR	Grundschutzraum (basic protection room)
HVR	Hochverfügbarkeitsraum (High Availability Room)
IEC	International Electrotechnical Commission
IK code	Degrees of protection against external mechanical impacts provided by enclosures for electrical equipment (IK code)
IP code	Protection classes provided by enclosures
ISO	International Organization for Standardization
IT -	Information Technology
MDC	Micro Data Centre
NEMA	National Electrical Manufacturers Association
NOAEL	No Observed Adverse Effect Level
PDU	Rittal's Power Distribution Unit
PSM	Power System Module (replaced by modular PDU)
RC	Resistance Class
RZ	Rechenzentrum (data centre)
TÜV	Technischer Überwachungsverein (German inspection and certification body)
UL	Underwriters Laboratories Inc. (certification in the USA)
VDE	Verband der Elektrotechnik, Elektronik und Informationstechnik (German Association for Electrical, Electronic & Information Technologies)
VDMA	Verband Deutscher Maschinen- und Anlagenbau (German Machinery and Plant Manufacturers Association)
VdS	VdS Schadenverhütung GmbH, Link: http://vds.de

WK   Widerstandsklasse (cf. RC = resistance class)

Rittal – The System.

Faster – better – everywhere.

- Enclosures
- Power Distribution
- Climate Control
- IT Infrastructure
- Software & Services

ENCLOSURES   POWER DISTRIBUTION   CLIMATE CONTROL   IT INFRASTRUCTURE   SOFTWARE & SERVICES

RITTAL

FRIEDHELM LOH GROUP