Reliable Data Centre

Guide

Version from December 2013

BITKOM

Reliable Data Centre

Guide

Version from December 2013

Legal Notice

Published by: BITKOM
Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e. V.
Albrechtstrasse 10 A
D-10117 Berlin-Mitte
Tel.: +49 (0)30 275 76-0
Fax: +49 (0)30 275 76-400
bitkom@bitkom.org
www.bitkom.org

Contact: Christian Herzog
Tel.: +49 (0)30 275 76-270
c.herzog@bitkom.org

Editorial team: Holger Skurk (BITKOM)

Graphics/Layout: Design Bureau kokliko/ Christine Holzmann /Astrid Scheibe (BITKOM)

Cover picture: Alejandro Mendoza, istockphoto.com

Table of contents

List of Figures

List of Tables

1 Introduction

The BITKOM “Reliable Data Centre" working group compiled this guide with the intention of providing clear and competent guidance on the planning, design and operation of IT infrastructures for vital company applications in data centres and other IT environments. It is therefore not just the choice of IT devices that is important – the layout and design of the data centre and the resulting requirements for:

- type and size
- electrical power
- heat dissipation
- wiring
- security and availability
- flexibility and energy efficiency
- purchase and running costs

are also decisive factors.

This guide offers up-to-date assistance in planning and setting up a data centre and IT environments in small and medium-sized companies. It supplements existing standards and specifications, which can also be referred to for support. These are often extremely general, however, whereas this guide is more in-depth and provides concrete instructions on how to design a data centre. It supplements the “Planning Guide for a Reliable Data Centre" matrix which, like the guide itself, is available to download free of charge on the BITKOM website.

Extracts of the matrix are also contained in sections of the guide.

This booklet and the planning guide are no substitute for expert advice and support from experienced advisers, specialist planners and consulting engineers, however.

2 Availability of a data centre

The rapid pace of development and the integration of information technology in all areas of business mean that today, even a small company cannot afford this technology to fail. Just a few years ago, many companies could "survive" the failure of their IT infrastructure, even for several hours. Today, the number of those for whom continuous availability of their IT is indispensable is growing dramatically.

These days, when creating, expanding or checking an IT concept, it is vital to find out how important the availability of a company's IT infrastructure is considered to be. Consequently, the question to be asked is this:

"What maximum IT downtimes can the company tolerate?"

As the demand for availability of the IT infrastructure grows, the requirements become increasingly stringent – not just for the IT systems themselves but, above all, for continually ensuring the ambient conditions and the power supply. As a result, redundancy in the air-conditioning and electricity supply, dual feed-ins and interruption-free maintenance of systems have established themselves as the norm for high-availability IT infrastructures.

But before you start work on the planning and layout of technical components for achieving the availability you desire, additional reflection based on risk analysis and the choice of site is imperative. This should cover possible risks associated with the area, which could influence the probability of potential failure geographically (air traffic, flooding, etc.), politically (war, conflict, terrorism, etc.). or from neighbouring sites (business premises such as service stations, chemical storage facilities, etc.). Furthermore, your considerations should also cover potential deliberate attacks by present or former employees of the company or by third parties.

However, the demand for high availability does not only entail getting to grips with possible technical solutions, but requires the owner to design and set up a comprehensive organisational structure. This includes the provision of trained service personnel, spare parts or a service agreement, for example. Precise instructions on the procedure in the event of failure or emergency must also be defined. In addition, this organisational structure must enable rapid, precise and targeted communication, with traceable documentation of events.

The term "availability" denotes the probability that a system can actually be used as planned at a given moment. Availability is therefore a measure that can be recorded and determined quantitatively. Different qualitative availability classes also exist, as shown in the following table, "Availability classes according to the 'HV-Kompendium' (High Availability Compendium) of the BSI". Here, the availability class of a service measures its quality in terms of availability in hours per year.

A system is regarded as available if it is capable of fulfilling the tasks for which it is intended. Availability is stated in percent and is calculated as 1 minus the relationship from downtime due to faults and the total time of a system.

Tier classification	Introduction	Explanation
Tier I	*1960s*	*Single power supply channel, single air-conditioning supply, no redundant components, 99.671% availability*
Tier II	*1970s*	*Single power supply, single air-conditioning supply, redundant components, 99.741% availability*
Tier III	*End of 1980s*	*Several power supply channels available but only one active, redundant components Maintenance possible without interruption, 99.982% availability*
Tier IV	*1994*	*Several active electricity and chilled water supply channels, redundant components, error-tolerant, 99.995% availability*

Table 1: Historic example of availability classes (according to the Uptime Institute, USA), source: US Uptime Institute: Industry Standards Tier Classification

Availability class	Description	Cumulated, probable downtime per year	Effects
AC 0 ~95%	*No availability requirements*	*Approx. 2-3 weeks*	*No measures are necessary as regards availability. Implementing the IT Grundschutz (formerly known as the IT Baseline Protection Manual) for the other basic values will have a beneficial effect on availability.*
AC 1 99.0%	*Normal availability*	*Less than 90 hrs.*	*Availability requirements are satisfied by the simple application of the IT Grundschutz (BSI 100-1 and BSI 100-2)*
AC 2 99.9%	*High availability*	*Less than 9 hrs.*	*The simple application of the IT Grundschutz has to be supplemented by the implementation of modules recommended for high availability requirements, e.g. modules B 1.3 Contingency Planning Concept and B 1.8 Handling Security Incidents, and a risk analysis on the basis of the IT Grundschutz (BSI 100-3).*
AC 3 99.99%	*Very high availability*	*Less than 1 hr.*	*Implementation of the measures recommended for selected objects in accordance with the IT Grundschutz, with particular emphasis on basic availability, e.g. measure M 1.28 UPS in the Server Room or M 1.56 Secondary Power Supply in the Data Centre, supplemented by HA (high availability) measures from the HA Compendium*
AC 4 99.999%	*Maximum availability*	*Approx. 5 min.*	*IT Grundschutz with additional modelling on the basis of the HA Compendium. The IT Grundschutz as the basis is increasingly supplemented and replaced by HA measures.*
AC 5 100%	*Disaster-tolerant*	*-*	*Modelling according to the HA Compendium. The IT Grundschutz continues to serve as a basis for the above areas and other safety/security values such as integrity and confidentiality.*

Table 2: BSI availability classes

If we calculate availability over the period of a year using the above formula, an availability of 99.99%, for example, would correspond to a downtime of 52.6 minutes.

$$\text{Availability (in percent)} = \left(1 \cdot \frac{\text{Downtime}}{\text{Production time + downtime}}\right) = 100$$

- 99 % * 87.66 hours per year
- 99.9 % * 8.76 hours per year
- 99.99 % * 52.6 minutes per year
- 99.999 % * 5.26 minutes per year
- 99.9999 % * 0.5265 minutes per year

The German Federal Office for Information Security (BSI) has defined availability classes as shown in Table 2 on page 9.

The BSI has developed a rating system for data centres: VAIR (Verfügbarkeitsanalyse der Infrastruktur in Rechenzentren – Availability Analysis of Data Centre Infrastructure). At www.vair-check.de, data centre operators can enter the details of their data centre anonymously and free of charge, and check the reliability of their data centre.

3 The influence of safety standards on the design of data centres

The planning and design of data centres is governed by a large number of safety standards. On the one hand, they provide planners and designers with assistance, but they also set out various requirements.

On the physical level of the data centre infrastructure, structural aspects, technical supply systems (electricity, air conditioning) and safety systems (fire alarm and fire extinguishing systems, intruder alarms, access control systems) are checked to ensure their suitability and correct use. As yet, no national or international standard exists for this subject area. In German-speaking countries, there are currently lists of tests from different certification authorities, which more (such as the TSI set of tests from the TÜV official German testing body) or less cover the requirements governing the physical infrastructure.

Here, we present the most important standards at organisational level, such as ISMS (Information Security Management Systems), ITIL (IT Infrastructure Library) and the Sarbanes-Oxley Act.

3.1 ISO 27001 / ISO 27002:2008

The ISO/IEC 27001 standards that came into force in October 2005 are intended to protect business information against threats. It is becoming increasingly important, as it provides companies with the necessary foundations for satisfying requirements from third parties. These can be legal requirements, for example (such as KonTraG, HGB and GoB, GoBS, GDPdU, BDSG, TMG, TKG, StGB), contractual requirements (e.g. from customers), and other requirements. The standard replaces the previous British standard BS 7799-2, which was annulled without replacement in February 2006.

The specialist business term used is 'compliance', which denotes both conformity to laws and guidelines, and voluntary codes of practice upheld by businesses.

The ISO/IEC 27001 helps companies to create a process for building and operating an Information Security Management System. This process of continuous improvement is achieved through the four well-known steps: “Plan, Do, Check, Act”, which will also be familiar to you from ISO 9001 (Quality Management).

Major assistance is also provided by the Grundschutz manuals (guides and catalogues), which have been developed and updated by the BSI over many years, and conform to “ISO 27001 based on IT Grundschutz”. The modules in the catalogues are extremely helpful for the creation of an Information Security Management System.

The PLAN phase entails the planning of the ISMS. Above all, the area of application and boundaries of the ISMS are defined here, and then approved by the management. A risk analysis is also carried out. This ascertains which systems and applications are important for maintaining a company’s business operations, and how great dependency on them is. Based on the results of this analysis, conclusions are drawn about the required level of protection, and the desired availability of systems and applications is determined.

The DO phase incorporates concrete measures to minimise and detect risks with the aid of a risk management plan. ISO 27002:2008 (formerly 17799) is a “Code of Practice for Information Security Management” and, as such, provides valuable tips for compliance with the “Controls/Measures” contained in ISO 27001. It is more or less a guide for putting the ISO 27001 into practice. Section 9, “Physical and Environmental Protection”, also sets out measures and suggestions for rooms

and infrastructures. Certification is only granted with reference to ISO 27001 or BSI ISO 27001, based on the IT Grundschutz.

During the CHECK phase, regular monitoring and periodic audits ensure that implemented measures are checked on a regular basis, in order that potential improvements can be flagged up (e.g. fire safety monitoring mechanisms, fire safety tests).

In the fourth phase (ACT), measures defined in advance as improvements are put into practice.

3.2 ITIL

"IT Service Management" is an important consideration during the planning and operation of a "Reliable Data Centre". Best practice recommendations for IT service management have been in existence since the end of the 1980s, when the British government's Central Computer and Telecommunications Agency (CCTA, now part of the Office of Government Commerce, OGC), published the first elements of the IT Infrastructure Library (ITIL). These guidelines, which have been set out in writing, range from detailed advice to individual processes within the ITIL, from rules of procedure to the newly published standard ISO 20000 (formerly BS 15000).

For existing data centres, customers also use a service management system that complies with ITIL as orientation. Computer service centres are often confronted by invitations to tender that require the participating companies to have ITIL. Two key areas are always included:

- Service support
- Service delivery

The set of rules applies to all IT organisations in all companies – no matter what their size.

To provide you with a quick overview of which processes are available in the data centre and which KPIs are used to monitor these, the working group has compiled a guide, "Processes and KPIs in Data Centres", which is available to download at www.bitkom.org/rechenzentren.

3.3 Sarbanes-Oxley Act and SAS 70

The Sarbanes-Oxley Act (SOX) that came into force in July 2002 is a US law intended to improve transparency in company reporting, and was introduced in response to the balance sheet scandals involving companies such as Enron and Worldcom. This law does not only apply to financial data, it also promotes security in the IT sector.

Initially, the law applied to all companies listed on the American stock exchange. However, its scope was subsequently expanded to cover non-US companies that have a parent company or subsidiary listed on the American stock exchange.

The Sarbanes-Oxley Act stipulates that company processes must be described and defined and internal monitoring procedures established, with the aim of minimising the risk of incorrect financial statements. Companies are monitored by approved auditors in accordance with the "SAS 70" audit. This in turn is largely based on the "Cobit 4.1" rules from the ISACA (USA). If a company that must comply with SOX has outsourced individual systems or its entire IT, for example, the SAS 70 audit must also be applied to the provider in question, although the responsibility always remains with the contractor. In this case, either the customer's auditors can carry out checks according to SAS 70 in the computer service centre, or the centre itself can arrange to have checks performed. The auditor's report must not be more than six months old from the time of the customer's annual financial statement. For this reason, SOX checks must basically be conducted twice a year, which entails considerable expenditure.

At international level, possible conflicts between the Sarbanes-Oxley Act and national regulations have been discussed. Any solution to these conflicts is still far from clear. A "Euro SOX" is in progress, however. In addition, the IDW (Institut der Wirtschaftsprüfer – German Institute of Public Auditors) currently bases its instructions for compliance with test requirements on Cobit 4.1.

3.4 Assessment of standards

The standards described above are frequently checked by customers, certification companies, auditors and other institutions. Whether the Sarbanes-Oxley Act and SAS 70 make a data centre more reliable is in dispute, but the stipulations for measures to improve security contained in ISO/IEC 27002:2008 and ISO/IEC 27001:2005 are thoroughly sensible and justified. ITIL and ISO 20000 demonstrably safeguard and improve processes in data centres. For contractors seeking public tenders, certification to BSI is often required. Here, however, the expenditure for documenting and running the ISMS is extremely high. The best combination is ISO 27001 with reference to the IT Grundschutz (where applicable), not certification by the BSI in Bonn.

4 The basis of IT infrastructure: the rack

Whether you have a separate data centre or an individual service cabinet, the individual rack is always the best means of securely accommodating IT systems. These include server racks, network racks and power supply/power distribution racks.

Since in most companies IT systems consist of (internationally) standardised 482.6 mm (19")[1] components, scalable, flexible rack systems in this design offer the best choice when putting together a stable and resilient IT infrastructure. They ensure perfect interaction between system and support components, such as the power supply, air conditioning and monitoring. A company's decision on whether to house its IT systems in a dedicated data centre or to have a standalone solution in individual server cabinets depends on the IT and the structural requirements. In both cases, however, the same fire safety and other security standards apply, for they are intended to protect ICT systems and – even more importantly – critical company data from the inside.

4.1 Server cabinet

4.1.1 Standard server cabinet (rack)

The modern server cabinet, referred to as a rack, should be designed to be as flexible as possible, so that it can easily be adapted to the future requirements of the IT equipment. A step-by-step design and modular expansion, from one rack to a whole row, from one aisle to an entire room, safeguards the value of current investments.

A multi-functional internal structure, high load-bearing capacity and air-conditioning concepts designed to suit the rack are the most exacting requirements for cabinet systems and racks in enclosures. Keeping components sufficiently cool is a necessary consideration when planning racks and their installation in a data centre. In a rack or row of racks, the air flow rate and a sufficiently low temperature (i.e. the difference in temperature from the desired maximum operating temperature of the components) must be designed such as to enable components to be operated within the desired temperature range. Monitoring and regulating air humidity within a safe range below dew point is also a prerequisite for trouble-free operation.

An easy-to-integrate power distribution system is also an important factor, because at the end of the day the power supply is what keeps the IT available. Fuse-protected low-voltage sub-distribution should also be available, as well as a flexible power distribution system in the rack itself, which can be supplied both from the electricity grid and from an uninterruptible power supply (UPS). Here, modern solutions deliver more than 88 kW to a rack. This is made possible by four independent, three-phase incoming feed ins, which guarantee a reliable power supply even in the face of more exacting requirements.

As server power and packing density in the rack have increased, the requirements for the ventilation system have become much more stringent, with demands for perforated doors with a free ventilation area of over 80%, and systematic isolation of hot and cold zones in the rack, for example. Other energy-optimised, performance-enhancing solutions can be achieved by hot or cold housing concepts that form part of the rack. In the case of extreme power losses in the rack, liquid-cooled solutions in the form of air/water heat exchangers are indispensable.

1 For stylistic reasons and ease of reading, the standardised 482.6-mm system is referred to hereinafter as the 19" system. The term "height unit" (HU) below signifies a height of 44.45 mm (1.75").

Sensors can be integrated in the infrastructure for monitoring both elements, power supply reliability and air conditioning. These probes record the servers' humidity and temperature, but also their power input. A modern, sensor-based monitoring system may also take on the task of access control and other parameters.

Here, incorporation of the servers and infrastructures in the monitoring process and simple bus wiring of the sensors themselves are decisive factors in determining the success of comprehensive monitoring at rack level.

The subject of stability is a vital aspect in all rack solutions. Due to the high packing density of modern server systems and storage solutions, server racks with a load-bearing capacity of up to 1,500 kg may be required, depending on the application. Consequently, the bases of units, sliding rails and snap-in functions must also be designed for high loads. A weight of up to 100 kg per base or 150 kg for special mounting rails can be anticipated in some cases.

Electricity and data cables should be routed separately to avoid any mutual influence. This is especially the case if the cabinet contains a great many copper-based cables.

4.1.2 A reliable server cabinet

A reliable server cabinet should, if possible, be modular in design. It provides the company with a reasonable degree of reliability at a manageable cost. A modular cabinet can be dismantled, converted or used in another location if necessary. This flexibility also offers advantages when choosing a location, during transport and re-erection if a company relocates.

Modularity is also advantageous when companies wish to expand enclosure systems or air-conditioning concepts. When planning a reliable server cabinet – just as for a reliable data centre – the following characteristics are essential for the continuous reliability and availability of systems:

- Constant temperature and air humidity through precision air conditioning
- A sufficiently reliable electricity supply by means of an uninterruptible power supply (UPS) and, if necessary, an additional, external backup power supply
- Protection against access from third parties through restricted-access lock systems, network monitoring of rack access, or even the acquisition of biometric data
- Adequate fire prevention, detection and reaction facilities
- Integration of modules or the architecture in a central monitoring and management system.

If necessary, the raised floor must be reinforced. The different methods of cable entry and internal cable routing are another important subject. Ever growing volumes of data and faster networks combined with copper-based wiring make the system sensitive to interference. Therefore, electricity and data cables should, as far as possible, enter the secure server cabinet separately. Consequently, attention must be paid to adequate cable routing options when selecting a rack.

If a three-phase backup power supply is used, it is possible to limit power input using motor-protective circuit-breakers, so as to prevent actual consumption of the theoretical amount of 88 kW per rack. For a single-phase backup, power could be limited using measuring instruments and limit values.

Well-structured wiring ensures order and clarity.
A prerequisite for this is a high level of flexibility in the cable routing and logical division into sections based on function.

Free areas (unused height units) should be sealed off by panels, so that as far as possible, cold air is conveyed only past the components that need cooling.

4.1.3 Making an inventory of the server cabinet

In data centres – particularly those of a certain size – it is difficult to maintain an overview of the available hardware components. Although today it is possible to communicate with any intelligent IT device, the equipment's physical connection to the rack and the relevant height unit is another matter. The layout of equipment in the individual cabinets, with servers, fans, UPS, etc. is often not transparent. As a result, making inventories and continually updating data about the arrangement of components in the data centre is expensive and mostly time-consuming as well. In many cases, existing, manually written documentation is not checked for accuracy. However, correct documentation is vital for making decisions, particularly in the event of failure.

Another problem is the half-life of the acquired information, for these records or updates still only ever represent a snapshot of the data centre inventory. Yet efficient rack assignment and transparent component management require continual, up-to-date and therefore reliable data.

To ensure constant access to up-to-date inventory data, modern inventory systems exist directly in the rack, which record the equipment of the 19" level completely and without contact.

Displays of rack configurations can be seen on the website of the respective monitoring system, or are transmitted in their entirety to a central management system as a data package.

4.2 Network technology

A complete examination of data centres, with special consideration of security aspects, cannot fail to include the subject of network technology. Many companies have already switched their telephone systems to Voice over IP (VoIP). Virtualised clients are the next step. This enables an increasing number of basic services critical to business to take place via data cables which, with Power over Ethernet (PoE), also supply power to the terminal devices. As network technology becomes increasingly important for problem-free business operations, security requirements are tightening up in this area, too.

As with the servers, for network technology the rack provides the basic housing. Since these active components are also designed as 19", network cabinets are generally based on the same platform. Requirements are also comparable in terms of stability, fire safety and access control. However, since the network infrastructure installed in the building tends to be designed to last more than 10 years, long-term planning is recommended when purchasing network cabinets, and flexibility of accessories is desirable. This way, future developments will also be taken into account. It must be borne in mind that the interior structure of racks differs greatly from one to the next.

Frequent switching between the various connections of the network components means that cables in network cabinets have to be rerouted considerably more often than is the case in server cabinets. These modifications, also known as MACs (Move, Add, Change), and increasing port density, lend special importance to the task of cable management. This starts with the roof panels and bases. Simple cable entry at these points facilitates retrofitting and keeps cable runs short. Routing ducts and guide panels ensure orderly fine distribution in the rack. At the same time, cable management, in particular, must place great importance on component stability, for modern current-carrying network cables are much more expensive and rigid than their Cat-5 predecessors.

One subject that is currently gaining in importance when it comes to network cabinets is air conditioning. Switches and routers are becoming ever more powerful, and produce more and more waste heat. Therefore, here too, possibilities for expansion have to be considered. The spectrum ranges from passive air conditioning via roof panels, ventilation attachments and dual-walled housings to fans and roof cooling units.

4.3 A reliable data centre

In addition to the basic requirements for a reliable data centre mentioned above, numerous project details have to be clarified in relation to construction.

First of all, a precise analysis of risks and weak points in the company must be compiled, flagging up possible risks for IT systems. This must cover the responsibility for planning and building a data centre, access authorisation and regular safety checks by independent auditors.

Various individuals are responsible for the planning, construction and operation of a data centre. In addition to IT specialists, these include building experts such as architects and construction engineers, specialist planners for air conditioning, energy and active defence, the department in charge of organisation and, last but not least, the management board.

The physical requirements facing a data centre do not apply merely to IT-related matters, such as the number and type of servers and network and storage devices, but also to active and passive defence.

A modular (and hence extendible/modifiable) fireproof security room, certified as far as possible, may form part of the equipment of the data centre. The use of a stable, multilayered fire safety door with the same protection values as the security room is also compulsory. Other structures such as a hermetically sealed ceiling, wall and floor system to protect against the ingress of smoke or water, for example, or a multistage very early fire detection system with multiple sampling points, including in the raised floor, are now the state of the art. These are joined by an appropriately dimensioned, autonomous fire extinguishing system with pressure relief and ventilation duct dampers, personal access control using card readers or biometric technology, and data centre periphery monitoring via LAN video technology.

To ensure the flexible expansion of data centres, it is a good idea to work with planners and suppliers who can ensure the long-term availability of the required products.

5 Energy supply

5.1 Power supply companies (PSCs) – Electricity feed-in and distribution in the company

5.1.1 Current situation

The electricity supply is of major importance for the operation of server cabinets or entire data centres.

The power supply chain commences at the power plants of the PSCs, which generate electricity from various forms of primary energy. The electricity is then transported through cables across high-voltage pylons to medium-voltage stations. From these stations, the electricity is often conveyed to the transformer stations on the various medium-voltage levels (10, 20 or 30 kV) via underground cables. Transformer stations are frequently situated in large buildings and on the roadside, on specially designed premises.

Large data centres with a surface area of several thousand square metres often have two medium-voltage feed-ins, ensuring complete redundancy – i.e. duplication to increase availability – all the way to the power plants.

Past examples show how dramatically situations can escalate if the power supply fails for longer periods and no backup solution is available. The general power supply can succumb to failure for several days over large areas. From reports of the damage caused in such cases, it is easy to see how essential an autonomous power supply is, particularly in areas of critical importance to companies, such as IT.

Possible causes of an interruption to the power supply could be:

- Technical faults in equipment (e.g. servers and their components)
- Technical faults in the power distribution (e.g. cables, sub-distribution boards)
- Faults in alternative power supply solutions (e.g. standby generating systems, also known as emergency diesel generators, battery-backed uninterruptible power supply (UPS) systems)
- Process-driven faults (e.g. design faults in the power supply, logistical errors)

For building a data centre, ready-made power supply solutions cannot simply be pulled out of a hat. However, basic principles have been set out, which must be adapted to individual circumstances. The challenge facing the planner lies in putting these principles into practice in a manner that suits the customer, his requirements and wishes and, last but not least, his budget.

5.1.2 Method of operation of the infrastructure

Different methods exist for transporting the electricity supply through the network. It is conveyed through ring mains and spurs. It must be ensured that the building is connected via a ring mains. The latter is connected to at least two medium-voltage distribution systems, so that the supply of electricity is safeguarded in the event that one system fails. The medium voltage is lowered to 400 V in the transformer stations and conveyed to the data centre through the low-voltage main distributor and normal mains sub-distribution via cables or busbars. The normal mains sub-distribution also supplies electricity to the uninterruptible power supply (UPS) systems.

5.1.3 Recommended equipment for different downtimes

The output from the UPS systems is routed via the UPS sub-distributors, and from there to the individual server cabinets. Junction boxes or distribution boxes are installed in the raised floor for this purpose. From these branches or junctions, more cables feed the electricity to the power supply units of the servers in the cabinet. If only one UPS system is installed, power supply units A and B have a joint supply; if there are two UPS systems, their supply is separate. A 2 x N supply therefore increases availability.

Category A is currently in place in many small to medium-sized businesses, often without any possibility of feed-in for a mobile standby generator. When examined more closely, however, this version does not provide any real security, and places its trust solely in the electricity suppliers. We are always hearing the old saying "It hasn't happened yet. So it won't happen to me...". But if a single link in the supply chain fails, this interrupts the entire supply from the PSC, and electricity has to be supplied by the UPS system. Moreover, the backup time of a UPS system is generally severely limited. It depends on the number of batteries installed, and the power that has to be provided. A UPS is generally unable to bridge a power cut lasting more than 30 minutes. In this case, a functioning computer shutdown routine should automatically be initiated, which sends out notifications, saves data, closes applications and, finally, powers down the computers in an orderly fashion. During planning therefore, it is especially important to make sure that the backup time of the UPS system is longer than the time required to transport and connect up a mobile standby generator. As a rule, batteries are used for the above arrangements.

Category B offers greater security. Here, the power supply is redundant, with a second UPS all the way from the low-voltage main distributor. If a supply channel upstream of the low-voltage main distributor fails, electricity is automatically supplied via the second, redundant channel. If the medium-voltage feed-in fails, the power supply is still assured by the mobile standby generator.

With Category C, the second UPS is joined by a second UPS sub-distributor. This ensures a redundant supply from the UPS systems to the server power supply units.

DC category	Electricity feed-in from PSC			Permitted DC downtime
	Server cabinet	Server cabinet	Data centre/server room	
	up to 7 kW	from 7 kW to up to 40 kW	500 up to 2500 W/m2	
A	*Standard*			*12 h*
B	*Redundant feed-ins*			*1 h*
C	*Redundant feed-ins*			*10 min*
D	*Redundant feed-ins from various transformer substations*			*< 1 min*

Table 3: From the BITKOM matrix "Planning Guide for a Reliable Data Centre" – Feed-in from PSCs

Category D represents the “gold standard”. Not only does it offer additional redundancy via a second standby generator, it also provides an additional feed-in from another independent medium-voltage substation. However, the energy supplier nearly always has to install the second cable route from another medium-voltage substation first. This can mean that several kilometres of new cable must be routed to the data centre premises, which is extremely cost-intensive and should be taken into account during costing.

Maintenance, that is, regular inspection and servicing of the entire infrastructure by qualified personnel, and compliance with regulations and guidelines on operation of the systems are indispensable for maintaining availability.

5.2 Power distribution in the company

5.2.1 Current situation

Power distributors convey the power of the normal electricity grid, the generator and the UPS to the equipment, systems and lighting. Two distributors can be employed to ensure higher availability.

5.2.2 Method of operation of the infrastructure

For power distribution, the normal electricity grid supplies the building infrastructure including lifts, lighting – except for safety lighting to VDE 0108 – compressors in DX air-conditioning systems (DX = direct expansion), chillers and other installations. In the event of power failure, this electricity supply is interrupted until an available generator starts up and an automatic switch causes it to restore the electricity supply.

All power distributors must be equipped with an input fuse. The size and type of power distribution system depends upon the power output to be distributed, the desired number of circuits and the power output per circuit. Please refer to the table below.

Phases	Max. amperage	Max. output
1	*16 A*	*3.6 kW*
1	*32 A*	*7.2 kW*
3	*16 A*	*11 kW*
3	*32 A*	*22 kW*

Table 4: Overview of power output classes

Overview of power output classes:
(Further combinations with two phases are also possible but are uncommon in Germany).

Ideally, fuse protection is effected selectively within the power strip, i.e. the outputs are monitored not by an overall fuse but by several fuses, either separately or as a group. As a result, in the event of failure only the affected output or group is disconnected from the mains, instead of the entire power strip. Either fuses or circuit-breakers may be used. A cabinet typically contains two separate power strips, which permit redundant operation of IT systems.

Modern power distribution units (PDUs) also feature measuring or switching functions, as well as a network connection for extended energy management. In addition, various models offer environmental monitoring with a range of sensors for measuring temperature and air humidity, for example.

Since most IT units in data centres are installed in 19" cabinets, the question arises as to where the PDU should be situated, and how the power supply should be routed to the 19" cabinets. PDUs are either installed in or surface-mounted on the wall, are separate cabinets or are integrated in a 19" cabinet. In many cases, the power supply is routed under the raised floor, which is also used for cold air conduction, however. This can adversely affect the flow of air, and access to the power supply is tricky. Alternatively, PDUs can be routed along the ceiling or walls, so that they have to enter the 19" cabinet from above. Integrated PDUs have the advantage of already being located near the point of use, and so being within easy reach of the 19" cabinets. Cables can also be routed on the roof of the 19" cabinets, provided that power and data cables are routed separately.

Special attention must be paid to the PDU strips in the cabinets. Thanks to the modern, compact design of units today, many systems can be installed in one cabinet. In extreme cases, a cabinet may have 42 height units (HU) each with 42 servers, and two power supply units per server, for example. For such a cabinet, a total of 84 sockets would have to be available.

5.2.3 Intelligent multiple outlet strips

For management at rack level, transparency, order and ease of handling are vital. Ideally, the multiple outlet strips used in a data centre will have different, easily changeable plug-in modules, e.g. for country-specific systems. In this case, international organisations have the option of using the same type of multiple outlet strip in all their branches, without having to assign specialist personnel to convert their systems. Today’s multiple outlet strips allow modules to be replaced during ongoing operation. High-end systems such as this generally also feature HTTP or SNMP monitoring and management options, and user administration that makes sure only authorised personnel can configure the outlet strip. These modular systems permit basic equipment of the racks by means of a vertical mounting rail with three-phase feed-in. The various plug-in modules can simply be inserted in this rail, considerably reducing wiring and assembly time and expenditure.

Finally, hosting companies, for example, which must demonstrate a high degree of accuracy in the distribution of energy costs per server (in one rack), can now benefit from officially calibrated socket modules. Calibrated measuring instruments of this kind are also available for the PDU.

5.2.4 Recommended equipment for different downtimes

The form redundancy takes depends on the number of power supply units in the IT devices. A good basis for high availability would be two power supply units per device, which are redundant. Then, in the event that one power supply unit fails, the remaining unit is able to continue supplying the IT device normally. These two power supply units per device should be supplied by the PDU via two separate PDU strips in two separate circuits. Availability can be further increased by using two separate PDUs, which receive power from two separate UPS systems via two separate transformers and two separate generators.

5.2.5 Protective measures and high availability

Data centres are subject to maximum requirements regarding availability. The energy supply must be permanently secure to reflect this. It therefore goes without saying that the power supply to the data centre itself and all areas in the same building to which data cables are routed must take the form of a TN-S system[2]. Structuring equipotential bonding to ensure good EMC is absolutely essential. To achieve optimum equipotential bonding, it is best to employ a separate functional protection earth (FPE) and protective earth (PE). Continuous self-monitoring of a “clean” TN-S system (e.g. with residual current monitoring (RCM)) and forwarding messages to a constantly manned point, e.g. the control centre, are fundamental prerequisites for reliable operation. Messages then inform the electrical engineer about what action needs to be taken, so that he can take appropriate service measures to prevent damage.

For line protection, too, all PDUs must be equipped with an input fuse. The size and type of PDU depends on the power output to be distributed, the desired number of circuits and the power output per circuit (see Table 4 on page 20: Overview of power output classes).

2 Separate neutral and PE conductors from the transformer to the current-using equipment

DC category	Distribution			Permitted DC downtime
	Server cabinet	Server cabinet	Data centre/server room	
	up to 7 kW	from 7 kW to up to 40 kW	500 up to 2500 W/m2	
A	*Standard, connection of servers via UPS and normal electricity grid is recommended*			*12 h*
B	*Redundant (A and B)*			*1 h*
C	*Redundant (A and B)*			*10 min*
D	*Redundant (A and B)*			*< 1 min*

Table 5: From the BITKOM matrix "Planning Guide for a Reliable Data Centre" – Distribution

A particularly difficult subject is that of "selective fuse co-ordination", which enables a short circuit or short to ground of a device in a cabinet to be safely isolated without any ill effects on other cabinets or IT devices.

Where personal protection is concerned, there are new requirements for additional protection for final circuits with sockets. Since 01.06.2007, DIN VDE 0100-410:2007-06, "Protection Against Electric Shock", applies to newly erected systems. Modifications and extensions to existing systems must also be carried out in accordance with this standard.

The above standard stipulates additional protection by means of residual current devices (RCDs) for all sockets in a.c. voltage systems, if the system in question is to be used by laypeople or is for general use. Care must be taken to ensure that faults/damages are eliminated immediately by an electrical engineer, including in connected electrical units/current-using devices/equipment. This requires a permanent monitoring system, plus organisational measures to ensure rapid troubleshooting.

A continuous residual current monitor (RCM) satisfies the current standard governing protective measures and also offers increased fire protection, even without switch-off by an RCD.

5.3 Uninterruptible power supply (UPS)

5.3.1 Current situation

It is not just total power outages – even simple voltage fluctuations or transient failures in the electricity grid can be enough to damage hardware or software, or to interfere with it to such an extent that severe errors occur in IT processes. Irregularities in the grid may be rare, but they are more frequent than many people assume.

UPS systems are employed to prevent the possible negative consequences of brief power failures. They filter out disturbances, such as surges and dips in voltage, and bridge interruptions in the mains supply. This reduces transmission errors, computer crashes and the loss of data.

5.3.2 Different UPS system technologies

Various technologies are employed for UPS systems. The most common is the static UPS system. Here, rechargeable (secondary) cells (batteries) are used to store energy. When two or more connected cells are linked in a circuit, this is known as a secondary battery, or simply a rechargeable battery. In the event of power failure, the energy from the battery is kept ready for critical loads by a static transformer (inverter) at the output of the UPS system. The backup time is determined by the load and the capacity of the batteries, but is typically within the range of 10 to max. 30 minutes.

The second type of technology used is the dynamic UPS system, either with or without reciprocating internal combustion engine. Depending on the design, the energy is stored by a kinetic bulk storage device or, as above, a rechargeable battery system. The dynamic UPS system makes the battery's energy available to critical loads by means of a rotating transformer (generator) at the output of the UPS system. With kinetic storage, the backup time depends on the load of the IT devices and the kinetic energy of the storage device (mass and speed), and is measured in seconds.

The dynamic UPS system with combustion engine combines a UPS system with a standby generator, and is therefore capable of bridging power failures over a longer period.

5.3.3 Method of operation

Static types of UPS are divided into three categories. The classification and associated methods for determining static UPS systems are defined and described in European standard EN 62040-3. We also distinguish between several types of mains fault (see Table 6 below).

Dynamic UPS systems with and without combustion engine are subject to DIN 6280-12.

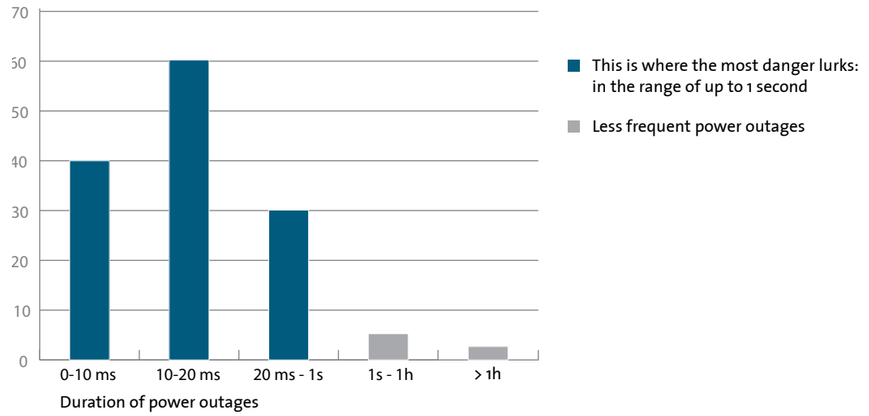

Figure 1: Frequency of mains faults in relation to their average duration

In data centres, static UPS systems with the classification "VFI" to EN 64040-3 or diesel UPS systems to DIN 6280-12 should always be used.

Static UPS systems with this classification are available with a power output range of 10 kVA to 1600 kVA, and can be connected in parallel up to a power output of 4800 kVA, depending on the make.

Diesel UPS systems are available with a power output of 200 to 1750 kVA. They can cover the low and medium-voltage range, and can be connected in numerous parallel circuits.

5.3.4 Basic construction of static UPS systems

Single block systems contain all the components required for system function, such as

- Rectifier
- Dedicated battery DC link with battery
- Inverter
- Electronic bypass
- Possibly a mechanical bypass

These systems are fully functional standalone units. For smaller power outputs and short backup times, the battery can be integrated in the system. Where higher power and longer backup times are required, it can be housed in external battery cabinets or on battery racks. The battery system is fused by means of special DC fuses or circuit-breakers.

Mains faults	Time	EN 62040-3	UPS solution	Deflector solution
1. Power outages	*> 10 ms*	*VFD Voltage + Frequency Dependent*	*Classification 3 Passive standby operation (offline)*	-
2. Voltage fluctuations	*> 16 ms*			-
3. Voltage peaks	*4 ... 16 ms*			-
4. Undervoltage	*Continuous*	*VI *) Voltage Independent*	*Classification 2 Line interactive operation*	-
5. Overvoltage	*Continuous*			-
6. Surges	*< 4 ms*	*VFI Voltage + Frequency Independent*	*Classification Double conversion operation (online) delta converter*	-
7. Effects of lightning	*Sporadic*			*Protection against lightning strikes and overvoltage IEC 60364-5-534*
8. Bursts	*Periodic*			-
9. Voltage harmonics	*Continuous*			-
10. Frequency fluctuations	*Sporadic*			-

Table 6: Types of mains faults and suitable UPS solutions according to EN 62040-3 (ref.: "Uninterruptible Power Supplies, European Guide"; Hsgr. ZVEI 2004

Single block systems have a power output range of approx. 300 VA to approx. 900 kVA.

Modular block systems contain all the components of a single block system, plus an interface for communication with a modular block of the same type.

Each of these systems constitutes a fully functional standalone unit, and is equivalent to a single block system. Thanks to the communications interface, modular block systems can be connected in parallel to create redundancy or increase the power output. Via this interface, all the parameters required for the synchronised operation of inverters and the electronic bypass are exchanged between the systems connected in parallel. Up to 10 modular block systems can be connected in parallel, depending on the manufacturer. When modular block systems are connected in parallel to increase the power output, an external mechanical bypass and a tie switch for isolating the entire UPS system from the loads are indispensable.

Modular block systems have a power output range – depending on the manufacturer – of approx. 10 kVA to approx. 900 kVA.

Custom solutions, such as a central electronic bypass or a central battery for several UPS blocks, are not discussed here. Custom solutions such as this limit redundancy and produce a single point of failure (SPOF).

Like single block systems, rack-mounted modular UPS systems are equipped with all the necessary components for function (see above). They function in the same way as the modular block system. The individual active components (rectifier, inverter, electronic bypass – as one unit or separate modules – plus battery sets in some cases) are modular in design and can be added to as necessary with no need to modify existing installations. The system cabinets of these systems are already equipped for a defined final expansion stage. All the interfaces required for possible future expansions are already in place and can be used without further preparatory work.

Installations upstream and downstream of the UPS system must also be designed to cope with the power output of this future stage.

In practice, there are two principal reasons why these systems are used:

They are primarily used for creating N+1 redundancy within a system cabinet. In the case of modular block systems, a considerable amount of space and major investment may be necessary in order to ensure redundancy.

Examples:

- Load capacity: 64 kW
- Modular system: 5 x 16 kW = 64 kW + 16 kW = 1 system cabinet
- Modular block system: 2 x 64 kW = 64 kW + 64 kW = 2 system cabinets
- Modular block system: 3 x 32 kW = 64 kW + 32 kW = 3 system cabinets

Data centres/server rooms often begin with a low power output. As a rule, the planned final power is output only achieved years after the initial installation. With a rack-mounted modular system, a good operating point (high efficiency) can be ensured by adapting the system in line with the load capacity, with no need to modify the installation or shut down the systems in operation. The higher cost of these systems is generally offset after a few years, thanks to energy savings.

These systems are available in module sizes of approx. 4 kVA to 200 kVA and can – depending on which modules are used – be expanded to up to 1600 KVA. They can also be connected in parallel in some cases, although in most cases this does not make sense, as the mean time between failures (MTBF) decreases as the number of modules connected in parallel grows.

The operating principles vary from one manufacturer to another. Some manufacturers use one central battery system for all UPS modules; others have the option of operating each module with its own, separate battery system. If, after several years, a central battery system is expanded, irregular charging/discharging may occur due to different internal resistance, resulting in reduced backup times and a shorter useful life. What is more, a central battery system is an SPOF.

Where the electronic bypass is concerned, too, some manufacturers prefer one central bypass for all modules, while others employ a decentralised bypass for each UPS module. This system behaves similarly to the central battery approach. Availability is reduced by an SPOF.

5.3.5 UPS redundancy

Redundancy takes the following forms with UPS systems.

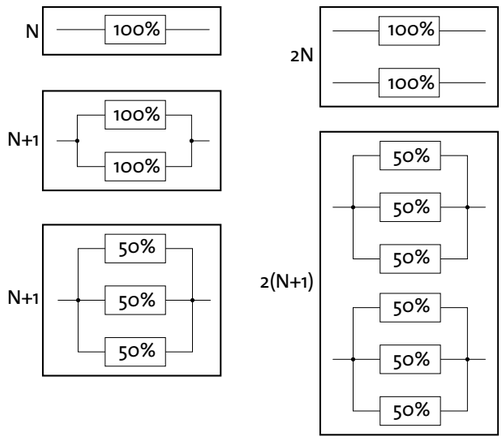

Figure 2: Redundancy in UPS solutions

5.3.6 Electronic/manual bypass

The task of the electronic bypass is to switch the loads without interruption from the mains to the inverter of the UPS system (safe busbar) and back. In the event of faults during inverter operation or in the event of high overload, the electronic bypass switches the consumers back to the mains without a break. Depending on its design, the electronic bypass can either be integrated in the UPS system (single block and modular block) or be an external component (parallel block with external electronic bypass). A second electronic bypass can be connected in parallel to create redundancy (N+1).

Every UPS system should be equipped with a manual bypass. The latter switches off the voltage of the UPS system for the purpose of service and maintenance work. If the manual bypass is integrated in the system, voltage is present in the input and output terminals of the UPS system even in bypass mode. The system cannot be replaced without cutting off the consumers. However, when an external manual bypass is used, the UPS system can be replaced without the need to switch off the consumers. If the manual bypass takes the form of modular blocks connected in parallel, or parallel blocks, it must be designed for maximum consumer load.

5.3.7 Energy storage units

Kinetic energy storage units are designed or dimensioned almost exclusively by manufacturers of UPS systems. The achievable backup times are limited to a few seconds, so that their use is restricted to diesel UPS systems or in combination with fast-starting standby generators.

The electrochemical storage units used in connection with UPS systems include lead and nickel cadmium batteries. Use of lithium ion batteries has not yet become widespread. Nickel cadmium rechargeable batteries are relatively insensitive to increased ambient temperatures, but their use is contentious because of environmental pollution.

The energy storage unit most commonly used in UPS systems is the lead battery. Lead batteries are very sensitive to temperature. Low temperatures reduce the battery capacity and therefore the backup time or power, while high temperatures reduce the battery's service life, or useful life. The optimum ambient temperature is 20°C.

The useful life of battery systems varies depending on the technology, the materials used and other factors. According to Eurobat, useful life is based on an ambient temperature of 20°C and laboratory conditions. The following useful life specifications are in place:

- 3 – 5 years – Standard Commercial
- 6 – 9 years – General Purpose
- 10 – 12 years – High Performance
- 12 years or more – Longlife

To ensure a reliable power supply, the battery system must be inspected regularly and replaced before the useful life has elapsed. In addition, it must be borne in mind that the battery loses capacity over its life. Designing the system for very short backup times carries the risk that the already ageing system may no longer be able to provide the required power and may therefore cut off the UPS system. In areas of importance to safety, overdimensioning (factor 1.25) is required, to ensure that sufficiently high capacity is still available at the end of the battery's useful life.

If the operator decides to dispense with redundancy in his UPS system, the battery system should at least be divided into two sections. The achievable backup time of a section is just one part of the planned backup time. This ensures that power outages, at least, are backed up for a few seconds. This is not a suitable approach for high availability data centres, however.

5.3.8 Recommended equipment for different downtimes

The most important factors to bear in mind when designing a UPS system is the required electrical power of connected, critical consumers, and the particular installation conditions. In order to bridge power failures, it is vital to include in planning an energy storage unit such as a battery system (cabinet or rack with isolating and safety devices) or a flywheel storage unit that is suitable for the power supply environment in question. Furthermore, the redundancy strategy and options for input and output supply play an important role.

A whole range of different concepts is available for selection for constructing the UPS system. Smaller, individual UPS devices are popular for safeguarding the supply of a few servers and IT storage systems. Different versions are the UPS cabinet or tower unit with integrated battery, the external battery pack, and the rack version for installation in a 19" cabinet. Larger UPS systems as single block or parallel systems, mostly with external battery cabinets, battery racks or flywheel storage systems, are mostly set up and operated in dedicated operating rooms. Here, a modern, liquid-cooled UPS system offers low-cost, efficient and direct UPS air conditioning without any special room air conditioning. Further advantages of operating rooms dedicated to UPS are the avoidance of thick power cables in computer rooms, and of batteries, which also represent a fire hazard. Modular UPS systems combine service friendliness with rapid adaptability to frequently changing maximum power requirements. However, the number of modules used has to be considered, as availability decreases the more complex the system becomes. When UPS systems are installed in server cabinets or take the form of a dedicated UPS rack in rooms shared with IT equipment, the additional fire hazard posed by the rechargeable batteries must be taken into consideration in the design of alarm and fire safety devices.

Ventilation units, chilled water pumps and cooling units/compressors may need to be supplied via a UPS system, depending on the energy density and selected backup time. The amount of energy required for cooling can also be made available via a storage unit, instead of cooling units/compressors. No cooling at high power densities results in overheating, causing IT devices to shut down without the possibility of using the established backup time for a planned shutdown.

5.3.9 Special features

Important planning features for dimensioning and installing a UPS system are:

- Output power rating at the required load power factor (these days min. 0.95)
- Connection values such as input/output voltage and frequency
- Current, wire cross sections and options for connecting UPS inputs and outputs
- Efficiency and power loss for the various load ratios during typical operating cycles (e.g. day/night, weekday/weekend), consideration of energy efficiency
- Details on UPS fuse protection for the various operating modes
- Effects on the mains input and input power factor. However, the effects of the connected load when the UPS is in bypass mode must also be taken into consideration
- Available backup time of a battery system or flywheel storage unit under actual load
- Maximum available backup time of a battery system or flywheel storage unit under actual load
- Information on the energy storage unit and charge/discharge behaviour
- Permitted ambient parameters, such as operating temperature and humidity; implemented degree of protection, fire safety and air-conditioning requirements

DC category	UPS			Permitted DC downtime
	Server cabinet	Server cabinet	Data centre/server room	
	up to 7 kW	from 7 kW to up to 40 kW	500 up to 2500 W/m²	
A	*Standard, min. backup time 10 minutes (incl. ventilation), minimum duration dependent on controlled shutdown time of servers*		*Standard, min. backup time 10 minutes, minimum duration dependent on controlled shutdown time of servers*	*12 h*
B	*Redundant (N+1), min. backup time 10 minutes*			*1 h*
C	*Redundant (2N), min. backup time 10 minutes*			*10 min*
D	*Redundant 2 (N+1), min. backup time 10 minutes*			*< 1 min*

Table 7: From the BITKOM matrix "Planning Guide for a Reliable Data Centre" – UPS

- Noise
- Electromagnetic compatibility (EMC)
- Dimensions and weights

This guide cannot offer a precise analysis of these individual features, because the circumstances of the data centre power supply will always required detailed planning. Some interdependencies to be considered are mentioned here as examples:

- The importance of the connected battery/flywheel storage unit for the backup time during a power outage if an emergency generator is available
- Consideration of the input power factor when dimensioning an emergency generator. Operation via UPS power electronics and operation via the bypass must also be taken into account here.
- The influence of the UPS output power factor on the possibility of supplying modern switching power supply units with electricity, including at full load
- Restricted power during operation at high altitudes
- The importance of considering efficiency over a typical operating cycle (fluctuations in capacity utilisation), in order to obtain realistic estimates of running costs

The price of a UPS depends on equipment details such as filters, transformers, fans, electronic bypass, integrated or external manual bypass and different switching concepts. Calculating the price of best-practice solutions is extremely complex for UPS systems, and requires time-consuming analysis of the circumstances, boundary conditions and interdependencies, and consideration of numerous individual parameters.

5.4 Backup power

5.4.1 Generating sets for supplying backup power (emergency power) in the event of power failure

Electricity suppliers cannot guarantee an undisturbed power supply at all times and all places, and power supply companies always waive any liability in their standard contracts. Therefore, brief interruptions or sustained power failures must be bridged by backup power systems, in order to maintain the operation of a data centre and its technical systems, such as air conditioning, electricity and safety.

The amount of permitted downtime has maximum priority when planning emergency power systems. In this connection, standby generators are divided into various groups:

- Generators without a required load transfer time. Systems are put into operation manually. These systems are unsuitable for automatic operation in data centres.
- Generators with a required load transfer time. Here, there may be an interruption of no more than 15 seconds before the generator assumes the task of supplying power after automatically being brought into operation. A DIN standard sets out the requirements for generating sets with combustion engines for safety power supplies in hospitals and in buildings and premises intended for gatherings of people. This standard should also be regarded as a minimum requirement for generating sets in the data centre sector.
- Generators with auto-reclosing in the form of standby power supply units. Here, the interruption time must be less than one second. These systems are no longer used in data centres, as an interruption time of less than one second is not necessary.

- Generators for an uninterruptible power supply in the form of diesel UPS systems. Here, the load is transferred without interruption on power failure.

5.4.2 Emergency power supplies

In the two last cases, special versions of generating sets are required, which are standby units with an energy storage unit. The latter must be continuously fed. The resulting operating costs mean that the consumer pays for his more reliable supply.

Various versions of standby units exist, as combinations consisting of a diesel engine, flywheel, electric motor and the necessary couplings.

Standby units are required whenever an interruption time, such as that caused by the use of simple standby generators, would not be a feasible option for reliably continuing ongoing operation of the load.

The most commonly used systems in the data – those mentioned second – are versions with a required load transfer time. The information below refers to these systems

5.4.3 Designing the emergency power system

The factors below are decisive when designing the output power of the generator:

- Sum total of connected loads
- Demand factor
- Starting currents and starting cos phi of loads
- Circuit feedback of loads (rectifier technology of UPS systems or frequency converters)
- Permitted dynamic behaviour
- Reserve for expansions
- Supplement for different ambient conditions

Load capacity

When adding together the load capacity, bear in mind that the apparent power and real power have to be stated.

Demand factor

In data centres, the generator output power must be set up with a demand factor of 1, as operation of the data centre must be maintained in both summer and winter.

Switch-on behaviour

The starting and switch-on behaviour of electric motors, transformers and large lighting systems with bulbs has an influence on generator output power. Where asynchronous motors are used, the apparent power can reach 6 times nominal power, and real power 2–3 times nominal power. Phased switch-on can considerably reduce the required generator output power. All available measures to limit starting power should be used to the full.

Dynamic behaviour

The dynamic behaviour of the generator when the full load is switched on and upon expected load changes during operation must be adapted to the permitted values of the loads. The motor, generator or both may have to be overdimensioned in order to satisfy the required values.

Ambient conditions

According to DIN 6271, the motor reference temperature is 27°C. If operating temperatures exceed this, the motor must be of larger dimensions. The motors' reduction factors must be established.

5.4.4 Recommended emergency power supply as a function of the permitted downtimes

It is possible to hire generating sets from your power supply company, which guarantee the emergency power supply during maintenance and repairs via an external connection. But hired generators are no answer to unforeseen power outages, as you cannot be certain that they will actually be available at the moment of occurrence.

Room planning/detailed planning for emergency generators

The following points must be considered during room planning/detailed planning:

- Compliance with the following regulations (DIN VDE, VDS, WHG, TA Noise, TA Air, VAws, TRbF, VDN...)
- Basic construction/version of generator (stationary built-in, container or hood-type generator)
- Design of the tank system (day tank and storage tank)
- Design of the exhaust system
- Engine cooling (front-mounted radiator, table cooler and the use of heat exchangers)
- Backup power control/switchgear
- Immission control

Basic room requirements

The room in which an emergency generator is erected is an electrotechnical operating room. It must be protected to F90 quality, and is a fire zone in its own right. Ventilation apertures must be provided to supply the cooling and combustion air, and for removing heated cooling air. These apertures must lead directly to the outside. Rooms without exterior walls are unsuitable because of the cross sections required for ventilation. If necessary, ventilation ducts in F90 quality must be built, which lead directly to the outside. In order to avoid short circuits of air, supply and extraction apertures must not be situated immediately next to one another. The generator room must take the form of a catch basin, with a circumferential barrier of 10 cm with 3 coats of oil-resistant paint, for protection against flooding and for environmental protection. This basin must be monitored for leaks. The room must be sufficiently large to allow an escape route 1 m wide. The doors of the room must be of at least T30 quality with a panic lock.

DC category	Backup power			Permitted DC downtime
	Server cabinet	Server cabinet	Data centre/server room	
	up to 7 kW	from 7 kW to up to 40 kW	500 up to 2500 W/m²	
A	*Optional*			*12 h*
B	*Availability in 15 seconds, fuel reserve: 24 hours*			*1 h*
C	*Redundant, availability in 15 seconds, fuel reserve: 72 hours*			*10 min*
D	*Emergency generator per power supply channel, optionally redundant, availability in 15 seconds, fuel reserve min. 72 hours, refuelling management, optional fuel purification system*			*< 1 min*

Table 8: From the BITKOM matrix "Planning Guide for a Reliable Data Centre" – Emergency Power

Applicable regulations

The regulations and laws listed here ensure the correct function of the system, operational reliability and protection of the environment. Approval authorities may impose further restrictions and requirements. In all cases, dialogue with the authorities should be initiated at an early stage of the planning phase.

Noise protection is an especially important consideration. Below is a list of continuous emission reference values for emissions sites outside buildings.

The residual noise level is assessed at an appropriate distance, not at the site of emission.

Industrial estate	*70 dB(A)*	
Business park	*Daytime 65 dB(A)*	*Night-time 50 dB(A)*
Core regions, villages and mixed regions	*Daytime 60 dB(A)*	*Night-time 45 dB(A)*
Residential areas and small housing estates	*Daytime 55 dB(A)*	*Night-time 40 dB(A)*
Purely residential areas	*Daytime 50 dB(A)*	*Night-time 35 dB(A)*
Areas with hospitals/clinics/ care facilities	*Daytime 45 dB(A)*	*Night-time 35 dB(A)*

Table 9: Continuous emission reference values for emissions sites outside buildings

Basic generator construction/version

There are three possible generator constructions/versions. With a built-in generator, the entire system is installed in the building. Interfaces to the outside are the air supply and extraction apertures, the exhaust system and, if necessary, an external table cooler. In this version, power can range from a few kVA to many MVA.

Container generators are frequently used when insufficient space is available in the building, or installation in the building is unsuitable for other reasons. As with a stationary built-in generator, power can range from a few kVA to many MVA. The third type is the hood-type generator. This is mostly employed when power of a few

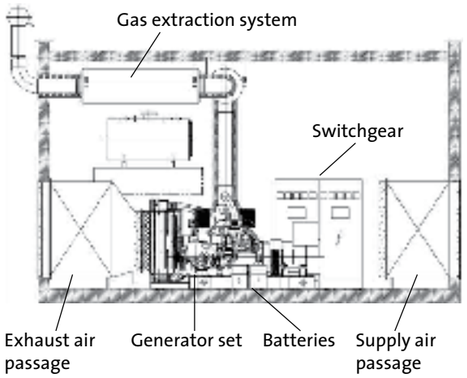

Figure 3: Standby generator in a building

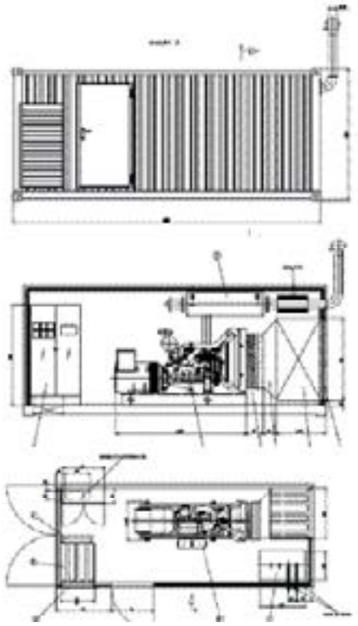

Figure 4: Standby generator in a container

kVA to several hundred kVA is required. Its advantage lies in its space-saving design. A disadvantage is the difficulty of access to all system components in the event of service or repair. The diagrams below show standby generators in a building and in a container.

Design of the tank system

The key factor that determines tank size is the necessary operating time and the system output power.
A quantity of fuel of less than 5000 litres can be stored in the generator room. If more than 5000 litres are required, a separate storage room in F90 quality, a tank for above-ground storage outside the building or an underground tank must be provided. The day tank is a single-walled tank with catch basin. It must be fitted in such a way that static pressure is applied to the engine's injection system. The storage tank must have double walls, or the storage room must be designed as a catch basin for the entire tank contents. If fuel pipes are installed between the day tank and the storage tank, which cannot be seen in places, they must have double walls. These double-walled pipes, the catch basins and the jacket of double-walled tanks must be monitored for leaks.

Due to the increased use of biofuels, fungi or micro-organisms may alter the composition of the fuel and render it unfit for purpose. Total failure of the power supply is not improbable. These fungi and micro-organisms can be removed to a very large extent by suitable fuel filtering systems, keeping the quality of the diesel stable for a longer period. A uniformly low temperature without the major seasonal fluctuations encountered in underground storage tanks, for example, has a positive effect on fuel storability.

Using only fuel specified by the engine manufacturer is a fundamental prerequisite. Most manufacturers base their recommendations on EN 590. As a rule, heating oil does not satisfy the requirements of this standard.

Design of the exhaust system

The nominal width of the exhaust system is based on the nominal power of the emergency generator, the planned pipe length, the number and type of changes in direction and the required sound absorption. Exhaust systems of emergency generators are pressure systems, and reach temperatures of up to 500°C. They must be restricted in such a way as to exclude any danger to people and valuables.

Design of the engine cooling

Engine cooling using a front-mounted radiator is possible up to an output range of approx. 1150 kVA. This means that all the cooling air has to be conveyed through the generator room. At an output of approx. 800 kVA and above, part of the heat from the engine can be dissipated via a table cooler. This reduces the amount of cooling air that has to be conveyed through the generator room. If there is a difference in height between the diesel engine and the table cooler in excess of 10 m, a heat exchanger must be used to reduce the pressure on the engine's cooling circuit.

Design of backup power control/switchgear

Each generator must be equipped with at least one backup power controller, which assumes the following tasks:

- Monitoring the mains power for compliance with the permitted tolerances
- Communication with the engine management system
- Starting and stopping the diesel engine
- Monitoring the generator network for compliance with the permitted tolerances
- Monitoring the engine parameters and controlling the necessary parameters
- Managing and controlling the required auxiliary drives (motor-driven ventilation flaps, supply and extractor fans, fuel pumps, solenoid valves, leakage sensors, pipe heaters, coolant preheating, starter battery charging, control battery charging, etc.

- Managing the necessary mains and generator tie switches for automatic mode
- Charging and monitoring the battery

The following options exist for the power unit:

- The mains and generator switches are located in the backup power controller
- The mains switch is located in the low-voltage main distributor, the generator switch in the backup power controller.
- The mains and generator switches are located in the low-voltage main distributor, the generator power is monitored by means of external voltage taps, and the generator is protected by a star-point current transformer.

Here is an example power supply diagram:

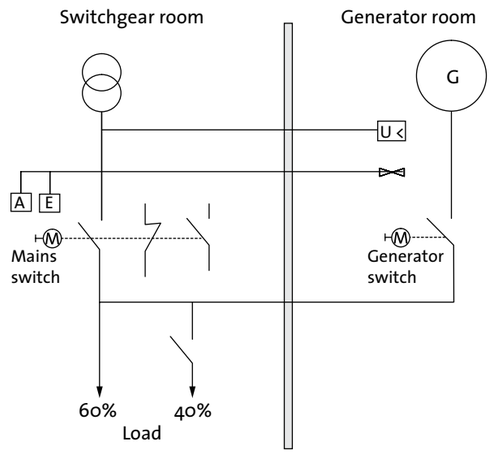

Figure 5: Power system monitoring/switchover

5.5 Service/maintenance

5.5.1 Service/maintenance of UPS systems

Maintenance in accordance with the manufacturer's instructions by specialist personnel authorised by the manufacturer is a prerequisite for maintaining proper function. Wearing parts must be replaced before their service life expires, in accordance with the manufacturer's instructions.

Less emphasis is placed on maintenance, as maintenance-free sealed lead batteries are commonly used. The term "maintenance-free" refers to the interior of the battery, however, and means that distilled water does not have to be topped up. On the other hand, all connections and battery connection screws have to be checked to ensure they have the correct torque. The voltages of the individual batteries must be recorded and logged in the charge holding and discharging phases. The condition of the battery can only be evaluated on the basis of this data. Just as important is regular cleaning of the battery system, to prevent leakage current or short circuits.

The availability of appropriate specialist personnel to remedy problems is another safety aspect that should not be ignored.

5.5.2 Service/maintenance/test runs of the emergency generator

Maintenance in accordance with the manufacturer's instructions by specialist personnel authorised by the manufacturer, and monthly test runs, are prerequisites for maintaining proper function. To ensure correct function, these monthly test runs must last at least one hour and operate at 50% of nominal load. They may be performed by the plant operator himself if he has received adequate instruction on the system. During a test run, the system must reach its operating temperature. A fixed, installed resistor, which supplies the consumers or the available network in parallel mains operation when backup power is required, may be employed as a load.

This requires agreement and acceptance testing on the part of the power supply company, however.

As with the UPS system, the availability of appropriate specialist personnel to remedy problems must also be considered.

5.5.3 Maintenance/testing of the electrical installation

Electrical systems must be inspected and serviced at regular intervals in accordance with the applicable regulations (VDE 0105) and stipulations of the professional association. To this aim, the systems must be offload, and appropriate repeat measurements and tests conducted. If necessary, an A/B supply must already be incorporated when planning the infrastructure. This enables the necessary isolation and testing to take place.

6 Air conditioning

6.1 Requirements

The air conditioning of ICT systems is an important criterion for their availability and operational reliability. The increasing integration and packing density of processors and ICT systems produces quantities of waste heat which, just a few years ago, would have been unimaginable in such a restricted space. And this trend is set to continue in the future.

After decades during which a cooling capacity of 1 to 3 kW per 19" cabinet was fully adequate, in the past decade the heat load per rack has increased dramatically. Modern IT devices in a 19" cabinet with 42 height units can consume over 30 kW of electrical power, and so also emit over 30 kW of heat. Further increases can be anticipated due to demands for ever increasing performance in a smaller installation space.

The "cooling" function is the most important requirement for the air-conditioning system: each kilowatt (kW) of electrical power that is consumed by ICT devices is released once more as heat. This heat must be conducted out of the ICT equipment, the cabinet, the room and the building, to keep operating temperatures constant. Since practically all ICT systems currently in use are air-cooled, the above task involves providing sufficient quantities of cold air and extracting the corresponding quantities of heated air. Other functions of air-conditioning systems are filtering, reheating, humidifying and dehumidifying the air, in order to comply with requirements for air temperature and humidity.

Different air-conditioning solutions are available on the market, to suit the thermal output of the equipment, i.e. the expected waste heat. Measurements and experience from the field show that power losses of up to around 8 kW in a rack or housing can still be tackled with traditional raised floor air conditioning, still commonly used in almost all data centres. However, the raised floor in the classic data centre cannot always keep pace with the sometimes high demands that prevail today. In recent years, raised floor air conditioning has been optimised to cope with these high heat loads, and a variety of so-called high-density air-conditioning solutions have been developed.

6.1.1 Compliance with ICT operating conditions

In the past, the requirements for air conditioning IT rooms involved maintaining a room temperature of approx. 21°C ± 1K and a relative humidity (r.h.) of about 50% ± 5%. Today, however, racks are overwhelmingly arranged according to the cold aisle/hot aisle principle, so that room temperature requirements in the conventional sense are now extremely rare. Nowadays, therefore, we no longer refer to a room temperature, but to supply air and exhaust air conditions.

The most important requirements for air conditioning concern the supply air temperature; the exhaust air temperature is not relevant to the reliable operation of ICT systems. Today, the recommended range for supply air in the cold aisle is extremely broad and covers a temperature from 18 to 27°C and humidity between 5.5°C dew point and max. 60% r.h./15°C dew point (to ASHRAE TC9.9 – 2011). The short-term permitted range is much broader still.

6.1.2 Recommended air-conditioning technology

Optimum conditions in terms of temperature and relative humidity can only be achieved with closed-circuit air-conditioning units – so-called precision air-conditioning units. These systems are the only ones designed for 24/7 operation, and use energy efficiently, i.e. primarily for cooling the return air (lowering the temperature = sensible cooling). A further challenge for the air-conditioning technology is operation all year round. The outdoor units must extract the heat in all seasons, at the ambient temperatures expected at that location. Here, the maximum expected ambient temperature must be set as the design parameter.

In contrast to this are comfort air-conditioning units for homes and offices, such as split or multi-split versions, for example, which permanently use a large proportion of the energy to dehumidify the circulating air (lowering the air humidity = latent cooling). This creates critical room conditions, but also considerably higher operating costs. Therefore, it is uneconomical to use comfort air-conditioning units in data centres and ICT rooms.

6.1.3 Redundancy

All technical systems can fail – including air-conditioning units. Therefore, a failure probability must always be considered in calculations, due to the numerous electromechanical components in air-conditioning systems. For this reason, one or more additional, redundant units are installed in most system sections, depending on the required availability, in the minimum number needed to cope with the occurring heat load. These redundant units safeguard the generation of cooling capacity in the event of failure, and so provide the required degree of availability. If a unit fails, the air-conditioning system no longer has full redundancy, and corrective measures (repairs) must be initiated immediately, to restore the conditions for reliable operation.

6.1.4 Energy efficiency

With sharply increasing energy costs, the energy efficiency of the air-conditioning system is particularly important during the planning phase. When reflecting on the overall costs, the total investment cost for the new system and the expected operating and maintenance costs throughout the system's service life must be ascertained and evaluated. If an air-conditioning system has a service life of 10 to 15 years, the energy costs – which make up the largest proportion of operating costs – generally exceed the investment cost and therefore constitute the most important decision-making criterion.

Some basic principles must be applied in order to minimise energy costs:

- Optimised operating conditions (as high temperatures as possible for the supply air and so also for the chilled/cooling water circuit)
- Use of Direct or Indirect Free Cooling
- Energy-efficient units and components (fans with EC drives, power-regulated compressors with a high COP, etc.)
- Adequately sized and, if possible, modular subsystems (closed-circuit air conditioning, refrigeration)
- Integrated closed-loop control of all subsystems, which automatically adjust dynamically in line with the fluctuating ICT load

Thanks to the considerably lower operating costs, the extra investment cost is paid back in the short to medium term.

6.1.5 Scalability

In many data centres, the ICT systems only reach their maximum final expansion stage after several years. Therefore, the air-conditioning system must be scalable and consist of a growing solution of modular units. Moreover, the subsystems must permit adjustment – preferably infinite – in line with the fluctuating ICT load, over a wide range. An air-conditioning system of this kind can then run with high operating and cost efficiency, even in partial load mode.

6.1.6 Service concept

In an air-conditioning system, wearing parts, e.g. filter mats and steam cylinders, are used, but so are numerous mechanically moved components. Therefore, preventive maintenance at regular intervals is a must. The tasks to be undertaken are described in DIN 31051 and VDMA 24186, among others. However, the relevant directives

for the operation of refrigeration systems must also be observed, as legislation requires plant operators to perform scheduled leak tests and complete system logbooks.

Suitable service contracts are available, depending on individual requirements for air-conditioning availability. These contracts differ in terms of the services offered:

- Repair contract
  - Comes into force after a failure or fault. System operability is restored by downstream corrective service measures
- Service contract
  - Regular work that ensures system availability through preventive service measures
- Maintenance contract
  - Combination of repair and service, which combines preventive and corrective service work
- Full maintenance contract
  - Complete maintenance, with budget security thanks to constant costs throughout the term of the contract

These contracts can sometimes also be combined with a 24/7 emergency service, and offer contractually fixed visiting times. This ensures that corrective measures are initiated by specialist personnel immediately, and the availability of the system is fully restored as quickly as possible.

6.2 Closed-circuit air conditioning

The overwhelming majority of ICT systems in use today are air-cooled, which is why the heat load is initially dissipated using air as the medium. Traditionally, this is achieved by closed-circuit air conditioning at room level. With higher heat loads, however, air at room level is a poor heat conductor, and is no longer up to the task. Then, better conductors such as water or refrigerant can be conveyed closer to the heat loads, i.e. right into the row of cabinets or, sometimes, even inside the cabinet. This ensures that the high heat loads are transferred to the air-conditioning systems right at the point of occurrence, and do not have to be transported long distances through the air.

6.2.1 Room cooling

The supply of cold air and the extraction of warm air is achieved using closed-circuit air-conditioning units, which are generally situated at the ends of server rooms (in the room or outside, in an air-conditioning compartment). The supply air is distributed around the room through a raised floor, and the exhaust air mostly returns freely through the room to the closed-circuit air-conditioning units. Then, in these air-conditioning units, the heat is transferred to a different carrying medium (coolant or refrigerant). As a rule, a small proportion of ambient air is supplied to the ICT room, for the purpose of air exchange and to maintain the air quality.

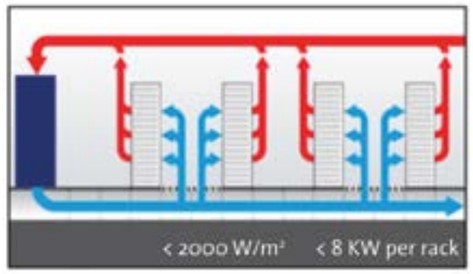

Figure 6: Room air conditioning via the raised floor with cold/hot aisle layout

The cabinets containing the ICT systems are now almost completely arranged in hot and cold aisle rows in the so-called “front-to-front” and “back-to-back” configuration. This prevents ICT systems in one cabinet from receiving hot exhaust air from another cabinet, and so being insufficiently cooled. This layout is an important prerequisite for efficient air conditioning.

However, classical systems of this kind are frequently prone to mixed supply and exhaust air, to a greater or lesser extent. This causes closed-circuit air-conditioning units to reach an exhaust air temperature that is often only a few degrees higher than that of the supply air. The result is that large quantities of air have to be transported to dissipate the heat load, considerably diminishing the cooling capacity of the closed-circuit air-conditioning units.

Therefore, a few years ago, isolation (enclosures) was introduced between hot and cold parts of the room, which counter the above disadvantages and prevent short circuits in the air flow (the mixing of supply and exhaust air).

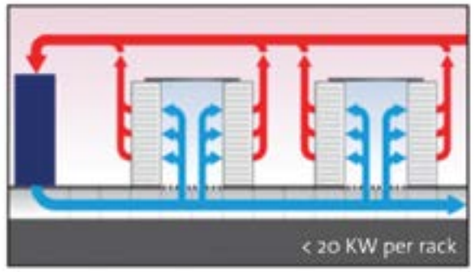

Figure 7: Room air conditioning via the raised floor and enclosed cold aisles

This isolation offers several advantages:

- There is a greater difference in temperature between the supply and exhaust air, which improves the performance capabilities of the air-conditioning solution
- The cabinets are exposed to the same supply air temperature over their entire height, temperature stratification no longer occurs, and ICT systems in the top part of cabinets are no longer more prone to failure
- The energy efficiency of air-conditioning systems is considerably improved

A complete enclosure consists of several components:

- Complete isolation inside cabinets
- Hot or cold aisle enclosure
- Raised floor sealing; no openings are permitted in hot areas (hot aisle and beneath the cabinets)

In such an arrangement, the flow of air is more or less forced to absorb heat from the ICT components on its way from the raised floor back to the air-conditioning unit.

6.2.2 In-row cooling

As soon as the room exceeds a certain heat density, air as a conductor of heat is no longer sufficient for managing the transport of heat over long distances to the closed-circuit air-conditioning units. The technical complexity required to manage the necessary quantities of air is no longer feasible. The height of the raised floor that would be needed for such high heat loads is structurally impossible in most data centres.

Therefore, in cases such as this air-conditioning units are integrated in the rows of cabinets or racks, either of adequate size for the heat load, or as additional units to the existing closed-circuit models. In this way, the transfer of heat from air to water or refrigerant takes place closer to the actual heat loads, and it is no longer necessary to convey all the cold air through the raised floor.

When the air is conducted in front of the server racks in the optimum way, the enclosure illustrated here can also be dispensed with.

6.2.3 Cabinet cooling

When heat loads exceed 25 kW per rack, direct cooling of the racks is necessary. This direct cooling is achieved by heat exchangers in the immediate vicinity of the servers. As a rule, these are liquid-cooled and are situated

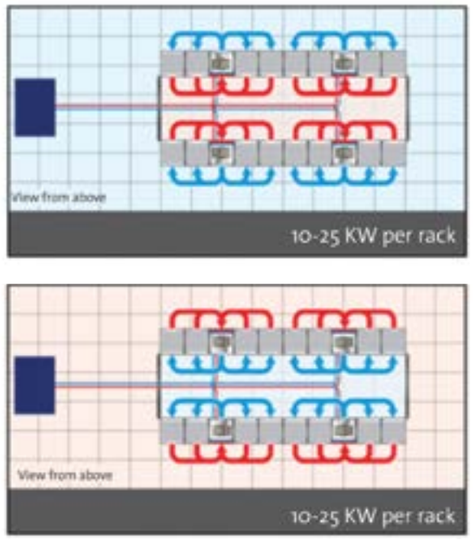

Figure 8: Air conditioning with air-conditioning units in rows of racks in enclosed hot/cold aisles

either below or next to the 19" racks. This method allows the removal of up to 40 kW or more per rack.

A chilled water infrastructure must be established around the racks for this purpose. Liquid-cooled racks ensure the right climatic conditions for each server cabinet, and are therefore autonomous in terms of room air conditioning.

In existing buildings with a low ceiling height, liquid-cooled server racks represent a good method of reliably dissipating high heat loads without the use of a raised floor.

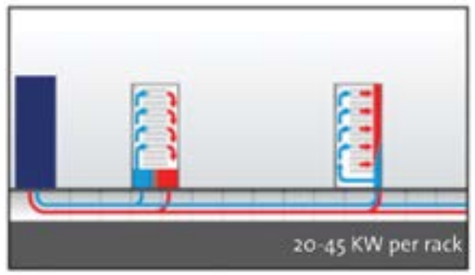

Figure 9: Cabinet cooling with liquid-cooled rack

6.3 Refrigeration

Closed-circuit air-conditioning systems differ considerably in design, and the selected system must take account of, among other things, the anticipated heat loads, exterior climatic conditions and the structural possibilities of the ICT room. The sections above dealt with the supply of the air flow; we now go on to describe in detail the required cooling of this air flow.

Efficient air-conditioning systems use Free Cooling to cut the refrigeration running times to a minimum, and so make a considerable contribution to energy-efficient air-conditioning operation. Systems can be divided into versions with Indirect Free Cooling, with Direct Free Cooling, and without Free Cooling.

Indirect Free Cooling

With Indirect Free Cooling, the air flow in the ICT room is separated from the ambient air flow. The heat load is transferred from the air flow in the ICT room via the closed-circuit air-conditioning unit to a water/glycol heat transfer medium, and the heat is transferred to the ambient air in the outdoor dry cooler. Indirect Free Cooling is particularly suitable where the supply air is subject to exacting requirements concerning temperature and relative humidity.

Direct Free Cooling

A characteristic of Direct Free Cooling is high flow rates of ambient air into the ICT room. The heat is absorbed directly from the incoming ambient air, and transported out of the ICT room. There is no water/glycol heat transfer medium in between, which is why this system is referred to as Direct Free Cooling. Direct Free Cooling is especially suitable when the requirements for the supply air temperature and relative humidity are less stringent.

6.3.1 Indirect Free Cooling

Indirect Free Cooling with refrigeration in the closed-circuit air-conditioning units

Indirect Free Cooling with refrigeration in the closed-circuit air-conditioning units is employed for data centres with a heat load of up to approx. 500 kW. The air-conditioning units contain refrigeration circuits that ensure refrigeration at high ambient temperatures.

When ambient temperatures are low, it is just a water/glycol mixture that circulates between the Free Cooling heat exchanger in the closed-circuit air-conditioning cabinet and the dry cooling unit installed outdoors. This method of operation greatly reduces the operating hours required for refrigeration, and so improves the system's energy efficiency. A higher ambient temperature causes the activation of the refrigeration circuit, and at very high ambient temperatures, energy-intensive refrigeration is carried out solely by cooling compressors.

The design parameters for the system as a whole are a decisive factor for the energy efficiency of an Indirect Free Cooling system. A higher permissible temperature in the ICT room results in longer Free Cooling running times, which aids energy efficiency. The use of Free Cooling mode for the longest possible period is desirable, and up to the highest possible ambient temperature.

In these systems, refrigeration is integrated in the closed-circuit air-conditioning cabinet, and therefore in or near the ICT room.

Indirect Free Cooling with refrigeration via chillers

Here, refrigeration takes place in chillers, which are generally installed outdoors. A water/glycol mixture circulates in the building. The heat from the return air is transferred to the cold water/glycol mixture in the closed-circuit air-conditioning cabinet, which is cooled by chilled water. The heated water/glycol mixture is cooled once more in the chiller, and returns to the closed-circuit air-conditioning cabinet.

For Indirect Free Cooling mode to be achieved, here too, an additional Free Cooling heat exchanger is required, which is either in the chiller outdoors or takes the form of a separate dry cooler.

At low ambient temperatures, the water/glycol mixture circulates between the chilled water-cooled air-conditioning units and the Free Cooling heat exchanger. In the air-conditioning unit, the heat is taken from the circulating air and emitted outside. At high ambient temperatures, the water/glycol mixture is cooled by refrigeration in the chiller.

Figure 10: Indirect Free Cooling

Further basic conditions for achieving maximum energy efficiency are described above in section 6.3.2.1, and also apply to Indirect Free Cooling with refrigeration using chillers.

Refrigeration is generally integrated in chillers installed out of doors. This system tends to be used for medium to large ICT rooms.

6.3.2 Direct Free Cooling

Direct Free Cooling has been used for smaller telecommunications facilities for many years. The telecommunications (TC) systems used here do not have exacting demands as regards air humidity. Today, the tolerances for air humidity (see 6.1.1) enable Direct Free Cooling to be used in data centres, too, and therefore in larger ICT rooms.

The air-conditioning units contain refrigeration circuits that ensure refrigeration at high ambient temperatures or in adverse environmental conditions.

The ambient air enters the ICT room via a multistage air filter unit with a large surface area. The air is conveyed in front of the ICT systems, and directly absorbs the heat. The heated air exits the room via exhaust air ducts. Additional fans may need to be fitted, depending on distances in the building and the possible cross sections of the air ducts.

At low ambient temperatures, some of the heated air is mixed with the cold ambient air in order to maintain the desired supply air conditions. At high ambient temperatures, the system switches to circulating air mode and refrigeration by refrigerant circuits is activated.

The humidity of the room is of lesser importance for these systems, and varies throughout the year from approx. 15–20 % r.h. min. to 80–85% r.h. max. A narrow tolerance band for humidity would entail considerable operating costs for humidification and dehumidification.

With Direct Free Cooling, too, the operating conditions influence the system's energy efficiency. The highest possible temperature of supply air in the cold aisle helps to achieve long Free Cooling periods, making a direct contribution to energy efficiency.

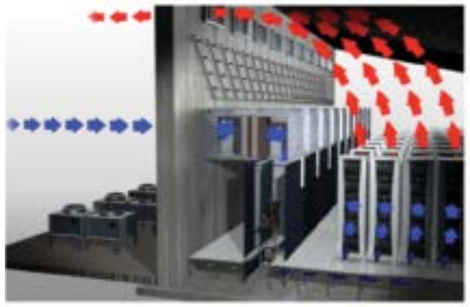

Figure 11: Direct Free Cooling

6.3.3 Air-conditioning systems without Free Cooling

In systems without Free Cooling function, energy-intensive refrigeration via refrigeration circuits is necessary all year round. These systems give rise to much higher operating costs, and are only considered for use in new systems in exceptional circumstances.

Moreover, it is worth checking whether existing smaller systems, which in the past were partly fitted with comfort air-conditioning systems, can be retrofitted with Direct Free Cooling.

6.3.4 Recommended equipment for different downtimes

DC category	Air conditioning			Permitted DC downtime
	Server cabinet	Server cabinet	Data centre/server room	
	up to 7 kW	from 7 kW to up to 40 kW	500 up to 2500 W/m²	
A	*Air conditioning required, redundancy optional*	*Air conditioning required, redundancy required, UPS support*	*Precision cooling, redundancy, cold/hot aisle separation, UPS support if necessary*	*12 h*
B	*Air conditioning required, redundancy required*	*Air conditioning required, redundancy required, UPS support*	*Precision cooling, redundancy, cold/hot aisle separation, UPS support*	*1 h*
C	*Air conditioning required, redundancy required, UPS support*	*Air conditioning required, redundancy required, UPS support*	*Precision cooling, redundant devices and pipes, cold/hot aisle separation, UPS support*	*10 min*
D	*Air conditioning required, complete redundancy required, UPS support*	*Air conditioning required, complete redundancy required, UPS support*	*Precision cooling, redundant devices and pipes, cold/hot aisle separation, UPS support, emergency cooling functions via an additional air-conditioning system*	*< 1 min*

Table 10: From the BITKOM matrix "Planning Guide for a Reliable Data Centre" – Air Conditioning

6.4 Conclusion

The technical solutions for energy-efficient, reliable air conditioning are many and varied, and must be individually explored within the framework of a project and specialist planning in the light of the ICT requirements, structural constraints and economic factors.

During these considerations, the aspects of scalability – i.e. whether the air-conditioning systems can grow alongside the ICT requirements – and future modifications to ITC systems, play a major role.

Exacting requirements concerning the availability of the air conditioning necessarily result in a more sophisticated technical solution and higher investment costs, whereby the return on larger investments in energy-efficient air conditioning will be achieved in shorter and shorter periods due to anticipated rises in energy prices.

7 Fire safety

"Experience shows that we must expect the outbreak of fire at practically any time. The fact that in many buildings there has been no outbreak of fire for decades does not prove that there is no risk, but is rather a piece of luck for the inhabitant, which he can expect to come to an end at any time." Even today, there is nothing to be added to this statement by a Higher Administrative Court (Oberverwaltungsgericht of North Rhine-Westphalia 22.07.2002, 7 B 508/01) from the year 1987. Therefore, reliable and effective fire protection is an indispensable prerequisite for reliable data centre operation.

Water as an extinguishing agent mostly has no place in a data centre, however. Today, specialist firms in the industry offer suitable fire protection solutions for every requirement and situation. When constructing a new data centre or retrofitting fire safety measures, precise planning and design of these systems is vital. Existing data centres with CO_2 systems in areas with personnel should be changed to gas suppression technology, which is safe for staff, immediately.

7.1 Technical fire safety

Fire, smoke and aggressive fumes represent a latent danger for data centres. To ensure safety, fire alarms that conform to requirements, combined with fire extinguishing technology, are vital. One alternative is oxygen reduction (fire prevention).

Foam or powder extinguishing systems are unsuitable for data centres. These will successfully fight a fire, but simultaneously damage or destroy equipment, e.g. sensitive servers or power supply units. Sometimes, this damage is worse than the actual fire damage. Therefore, automatic extinguishing systems or oxygen reduction systems using gaseous media are the "recognised state of the art" for data centres.

7.1.1 Method of operation of the infrastructure

Smoke detectors

Smoke detectors that work on the principle of scattered light are primarily used for fire detection in data centres. Here, the scatter of a ray of light on smoke particles in the optical chamber of the smoke alarm provides a measure of the smoke density. This technique is employed both in conventional, point smoke detectors (optical smoke detectors, point detectors) and in highly sensitive smoke extraction systems (aspirating detectors, active detectors). In contrast, the ionisation detector commonly in use years ago has now almost completely disappeared from the European market.

Whether a point smoke detector is more suitable, or aspirating detectors (smoke extraction system) depends on the area of application. In areas without special detection requirements, e.g. offices, point smoke detectors are generally adequate.

In air-conditioned rooms or areas with high ceilings, point smoke detectors rapidly come up against their limits. Cushions of warm air or a strong flow of conditioned air prevent sufficient quantities of the smoke reaching the point smoke detectors quickly enough. In these cases, the use of highly sensitive extraction smoke detectors (smoke extraction systems) is recommended for early fire detection.

If the automatic fire extinguishing system is triggered in the data centre by point smoke detectors, the latter must be installed in a so-called dual detector dependency system to prevent false alarms. If a point smoke detector in the room monitoring system is activated, an internal alarm is initiated, but the automatic fire extinguishing systems are only triggered when a second point smoke detector also goes off.

For the protection of individual, air-conditioned IT equipment, the VdS (Verband der Sachversicherer – German Association of Property Insurers) points out that early fire detection using point smoke detectors is difficult, to say the least, or even impossible.

A fire in live components in cabinets can be produced by smouldering fires at any time, caused, for example, by overloaded components or faulty contacts. If not detected in good time, a smouldering printed circuit board leads to rusting and possibly corrosion in other components not affected by the smouldering fire. In addition, in air-conditioned cabinets, early smoke detection is rendered more difficult by the high air change rates of the air conditioning. Any occurring smoke is immediately diluted, and is then scarcely detectable by smoke detectors in the very early stages of a fire.

To protect individual, air-conditioned IT equipment in the data centre, highly sensitive smoke extraction systems are reliable and enable early intervention focusing solely on the individual affected IT device.

Closed server cabinets present a new challenge for fire safety in data centres, as they have an integrated cooling system and work in a closed circuit. Then, smouldering fires are virtually undetectable from the outside, as only a very small quantity of smoke escapes to the outside. Similarly, gaseous fire suppression agents are unable to penetrate these cabinets from the outside.

For server cabinets of this kind, compact fire detection and extinguishing systems should be used, which can be integrated in the form of a 19" slide-in module.

As with early fire detection in air-conditioned IT rooms, smoke extraction systems for monitoring individual air-conditioned IT devices have advantages. Here, samples of air may be taken from the air-conditioning air flow directly inside the IT cabinets, for example. Nowadays, these systems for the integrated protection of IT devices are modular in structure and offer fire detection and fire extinguishing, for example, in a compact 19" slide-in module. Alternatively, an external fire extinguishing unit can be activated.

Fire extinguishing systems

The effectiveness and reliability of fire extinguishing systems for data centres are determined by project design, specialist planning, execution and maintenance that takes account of all the risks of that particular case. Suppression gases are preferred, because they are not electrically conductive, do not leave behind any residue and operation of IT equipment can be maintained even if the fire extinguishing system is triggered.

When planning a fire extinguishing system using gaseous suppression agents, a pressure relief system for the room must also be included, in order to counter the resulting brief rise or drop in pressure. The required aperture for pressure relief and the integrity of the room with a view to the holding time of the suppression gas concentration are determined by means of tests (door fan test method). The minimum holding time of the gas concentration should be at least 10 minutes.

Gas suppression systems for data centres are basically divided into those with inert gases and those with halogenated hydrocarbons (chemical suppression gases).

Inert gases

Inert gases extinguish fire by reducing the proportion of oxygen in the air.

Rooms are flooded with inert gases within 120 seconds. The air in the room therefore mixes with the inert gas, producing a low-oxygen atmosphere. The oxygen content of the air in the room is reduced to such an extent as to halt a combustion process.

- Argon (Ar)
  Argon is an inert gas, it is chemically very stable and does not combine chemically with any other element. Argon is taken from the ambient air at low cost, and is employed in numerous other technical processes (e.g. as shielding gas during welding), as well as for extinguishing fires. Argon is non-toxic

and is heavier than air. At a concentration of argon required for extinguishing a fire, persons can be in danger from a lack of oxygen. Therefore, and also because of the danger posed by smoke during a fire, rooms are only flooded with argon after an alarm has already sounded, so that persons can leave the area in question safely.

- Nitrogen (N_2)
  Nitrogen makes up 78% of the atmosphere. Like argon, it is extracted from the ambient air and used in numerous ways. It is an inert gas and only combines chemically with other elements at very high temperatures. Nitrogen is colourless, odourless and tasteless, non-toxic and lighter than air. At the nitrogen concentration required for extinguishing a fire, persons can be in danger from a lack of oxygen. Therefore, and also because of the danger posed by smoke during a fire, rooms are only flooded with nitrogen after an alarm has already sounded, so that persons can leave the area in question safely.

- Chemical fire suppression gases: HFC227ea, trade name e.g. FM-200 and FK-5-1-12, trade name Novec 1230 Chemical fire suppression gases extinguish the fire by absorbing the heat in the flame. The advantage of chemical fire suppression gases is their highly effective extinguishing effect at low concentrations. The fire extinguisher cylinders therefore take up much less space than those of inert gases. In some cases, the cylinders can also be installed right inside the areas of the data centre that require protection, e.g. when retrofitting fire safety measures. Chemical gases have a flooding time of only 10 seconds until the concentration needed to suppress the fire is reached.

Oxygen reduction systems

An oxygen reduction (fire prevention) system creates a permanently low-oxygen atmosphere in a data centre by introducing nitrogen. This eliminates the possibility of naked flames developing. Permanent oxygen reduction is maintained without interruption by high-precision regulation of a nitrogen reserve or nitrogen generator.

At the reduced oxygen content necessary to prevent fire, the protected areas of the data centre can still be accessed by persons in accordance with Information BGI/GUV-I 5162, "Working in oxygen-reduced atmospheres" by the German Social Accident Insurance.

7.1.2 Recommended equipment for different downtimes

Data centres

If maximum downtimes of 24 hours can be tolerated, sensitive fire detection in the data centre is sufficient. If there are more stringent availability requirements for the data centre, in addition to the above an automated fire extinguishing system with gaseous suppression agents, or an oxygen reduction system, are recommended.

The most important criteria for selecting an automated fire extinguishing system with gaseous suppression agents, an oxygen reduction system or a combination of the two are the requirements regarding the data centre's availability. The higher the required availability, the more it makes sense to install an oxygen reduction system, or an innovative combination of fire extinguishing and oxygen reduction technology.

With fire extinguishing systems with gaseous suppression agents, pressure relief via pressure relief vents is required to prevent positive and negative pressures that may occur if the system is triggered. The applicable regulations stipulate that the calculated maintained concentration must be upheld for 10 minutes. The power supply must be switched off throughout the data centre in order to prevent re-ignition.

Server cabinets

A compact, integrated unit with fire detection detects the outbreak of fire in the early stages. This provides a time advantage for organisational measures (e.g. automatic alarm texts, pagers etc.), and the initiation of automatic measures, e.g. the "soft shutdown" of IT systems, data backup in another location, selective shutdown or targeted fire suppression of network and server cabinets.

In the event of a fire, IT units that are switched off and have no power supply are the most reliable countermeasure to widespread propagation of a fire or aggressive fumes. However, a "soft shutdown" does not mean that the power supply is immediately cut off. Instead, the early fire detection system triggers a shutdown management function, which diverts data to IT units that are not at risk. The definitive cut-off of the power supply only takes place when the data transfer is complete.

7.2 Structural fire safety measures

The aim of structural fire safety measures is to save human lives. This demands maximum quality of materials and workmanship, and strict adherence to regulations and procedures.

The basics of structural fire safety are set out in national building regulations, and provisions governing technical fire safety equipment, fire safety plans, firewalls and emergency escape routes. The fire characteristics of building materials and components are regulated by DIN 4102, which does not, however, cover the necessary objectives of fire safety measures, such as are vital for IT data centres.

Further aspects to be considered carefully are the fire resistance ratings of load-bearing structures and fire protection in electrical installations and power supply systems. When planning a data centre, the fire resistance rating and escape routes must also be considered with a view to fire fighter access and safety. Fire fighting lifts and safety stairwells must be included. Data centres are also subject to industry-specific fire safety directives.

DC category	Technical fire safety			Permitted DC downtime
	Server cabinet	Server cabinet	Data centre/server room	
	up to 7 kW	from 7 kW to up to 40 kW	500 up to 2500 W/m²	
A	*Monitoring unit with early fire detection and extinguishing technology (with passive reserve of fire extinguishing agent)*	*Fire alarm system, monitoring unit with early fire detection and autonomous extinguishing technology (with passive reserve of fire extinguishing agent), or oxygen reduction (fire prevention) system*		*12 h*
B	*Monitoring unit with early fire detection and extinguishing technology (with passive reserve of fire extinguishing agent)*	*Fire alarm system, monitoring unit with early fire detection and autonomous extinguishing technology (with passive reserve of fire extinguishing agent), or oxygen reduction (fire prevention) system*		*1 h*
C	*Fire alarm system, monitoring unit with very early fire detection and autonomous redundant fire extinguishing technology (fire extinguishing system), or oxygen reduction (fire prevention) system*			*10 min*
D	*Fire alarm system, monitoring unit with very early fire detection and autonomous redundant fire extinguishing technology (fire extinguishing system), or oxygen reduction (fire prevention) system*			*< 1 min*

Table 11 from the BITKOM matrix "Planning Guide for a Reliable Data Centre" – Technical Fire Safety

Fire fighting, extinguishing agents and smoke extraction must also be incorporated in planning. This would include mobile fire extinguishers, the possibility of extinguishing agent retention, etc.

7.2.1 Fire safety objectives

When planning a data centre, it is of the utmost importance to define the fire safety objectives. During the planning phase you must clarify whether the regulations, guidelines and fire safety objectives themselves can be put into practice. The use of experienced planners is recommended, because structural and technical fire safety measures must be brought into balance with interruption-free data centre operation. Subsequent installations and conversions devour huge sums of money or lead to a spectacular rise in premiums for insurance relating to fire and electronic systems.

7.2.2 Method of operation and room requirements

Structural elements are categorised in fire resistance classes according to their fire behaviour. The fire resistance stages are mostly set at 30, 60, 90 and 120 minutes. So, F30 means, for example, that during a fire test, at least 30 minutes must pass before the wall gives way. The building authorities denote the class F60 as "fire-retardant" and F90 as "fire-resistant".

Walls, floors and ceilings must be constructed with at least fire resistance class F90. Doors must conform to T90 quality as a minimum, i.e. doors must be resistant to fire for 90 minutes. Protection against fumes and spray water is also indispensable.

Cable and installation ducts from and to the data centre must be effectively protected. Flame-retardant cable ducts can have protection with E30 or even E90 quality. Installation ducts must be in I30 or I90 quality, and independent ventilation ducts in L90. If electric cables are routed through fire-resistant ceilings and walls, the cable bushings must also be fire and fume-resistant – in other words, sealed off. This isolation may in some cases be achieved by means of intumescent fire pillows.

Cable runs constitute a very high risk in the event of a fire, and should be coated or designed to be water and moisture-resistant. This will make them intumescent, capable of reliably preventing fire from spreading along the cables. The cables themselves should consist of flame-retardant material, which also does not produce aggressive fumes (e.g. PCV-free insulation).

Fire spreads rapidly and uncontrollably through flammable pipes, which are routed on and in ceilings and walls. Pipe shielding or flame-retardant materials provide fire-resistant and fume-proof barriers.

However, simple testing of structural elements is in no way adequate for complex, high-availability data centres. When high availability is required, it is essential for the rooms or modular safety cells to be constructed to undergo a European standardised system test to EN 1047-2, as must the structural elements of the ceiling-wall and wall-floor connections, the cable entries, overpressure relief and the doors and surrounding areas. This current European standard for the structural data centre infrastructure specifies both the intensity and the duration of precisely defined loads. With the ECB-S certificate issued by the VDMA, the user is safe in the knowledge that his entire system – not just one wall or the door – is fire-resistant.

7.2.3 Recommended equipment for different downtimes

Special features

Aspects to be taken into consideration during project planning are:

- Determination of fire safety objectives, under consideration of the special requirements of the IT infrastructure
- Determination of structural characteristics

DC category	Structural fire safety measures			Permitted DC downtime
	Server cabinet	Server cabinet	Data centre/server room	
	up to 7 kW	from 7 kW to up to 40 kW	500 up to 2500 W/m²	
A	*Walls, floors, ceiling, fire resistance class min. F90, protection against smoke and spray water, min. T90 doors, cable sheaths with same protection rating*	*Walls, floors, ceiling, fire resistance class min. F90, protection against smoke and spray water for 30 minutes, min. T90 doors, cable sheaths with same protection rating*		*12 h*
B	*System test of structural fire protection of walls, floors, ceiling, doors: to European standard EN 1047-2, cable sheaths with the same protection rating, protection against smoke and spray water for 60 min*	*System test of structural fire protection of walls, floors, ceiling, doors: to European standard EN 1047-2, cable sheaths with the same protection rating, protection against smoke and spray water for 60 min*		*1 h*
C	*System test of structural fire protection of walls, floors, ceiling, doors: to European standard EN 1047-2, cable sheaths with the same protection rating, protection against smoke and spray water for 60 min*	*System test of structural fire protection of walls, floors, ceiling, doors: to European standard EN 1047-2, cable sheaths with the same protection rating, protection against smoke and spray water for 60 min*		*10 min*
D	*System test of structural fire protection of walls, floors, ceiling, doors: to European standard EN 1047-2, cable sheaths with the same protection rating, protection against smoke and spray water for 60 min*			*< 1 min*

Table 12: From the BITKOM matrix "Planning Guide for a Reliable Data Centre" – Structural Fire Safety

- Planning the building work – by professional planners if possible
- Compilation of specifications for the individual elements to be offered for tender
- Collection of incoming quotations, comparison, evaluation
- Drawing up a contract-awarding proposal for the decision-makers

7.3 Preventive and organisational fire safety measures

In the Federal Republic of Germany, preventive fire safety is of a high standard in international terms. Despite today's safety standards, however, experience in recent years shows that it is the human factor that determines the occurrence, effect and extent of a fire.

Preventive and organisational fire safety measures are frequently neglected. But the correct behaviour of the people involved, and optimised fire safety organisation, can hugely limit the impact of a fire.

If a company fire safety organisation system is put in place, this is a managerial task and should motivate employees to actively participate in fire prevention measures. When establishing a fire safety organisation system, technical fire safety equipment and procedures must be shown and explained to employees. Organisational rules for fire safety should be incorporated in company processes. Only motivated, well-informed and involved employees can make an active contribution to minimising the risk of fire.

For existing buildings and systems, organisational fire safety measures supplement existing preventive structural and technical fire safety measures.

For new buildings, organisational fire safety helps to define the structural and technical fire safety strategy in the planning phase.

The following aspects need to be considered when planning and operating a data centre:

- Emergency shutdown plan
- IT restart plan
- Fire safety regulations
- Ground plan for fire fighters
- Fire safety diagram
- Plan of escape routes, company instructions
- Signage/identification
- Avoidance of unnecessary fire hazards
- Ban on smoking
- Ban on food
- Special permits:
  - Work involving an increased risk of fire
  - Instruction of people from other companies
- Plant security
- Procedures for visitors
- Training

All planning must take account not just of current circumstances, but also of foreseeable future developments.

8 Design of premises and safety zones for data centres

Security of information technology is a sweeping term that covers logistical data security, the physical safety of systems and the organisational reliability of processes. The objective of a comprehensive security concept is to take all areas into consideration, to recognise and assess risks early on and to initiate measures in such a way that a company's competitiveness on the market is not jeopardised.

Through an overall examination of the IT infrastructure and various functional areas of the IT, a well thought-out plan can reduce or even eliminate major risks to physical safety. Decisive roles are played by the premises in which the IT is located on the one hand, and the spatial arrangement of the various functions in relation to one another on the other hand.

Location of IT rooms

The design of an IT infrastructure and thus the selection of a site for a data centre must be based on the company's data security principles, which reflect availability requirements and the company's strategic direction.

The following criteria should be taken into consideration when examining the physical safety of a site:

- Low risk potential from neighbouring usage, adjacent parts of the building or functions
- Avoidance of risks from media and power supply lines, tremors and chemicals, which would compromise the physical safety of the IT systems
- Avoidance of possible dangers posed by elementary risks (water, gales, lightning strikes, earthquakes), risk assessment of aspects peculiar to the region
- The data centre as a separate, independent functional zone
- A "protected" location to ensure protection against sabotage
- Assessment of potential threats on the grounds of the company's social policy

If all risk factors and the constraints specific to the company are taken into consideration, potential danger and the resulting time and expense can be eradicated in advance during the design of the IT infrastructure.

Structure of a data centre

When designing and planning a data centre, the various functional zones are arranged in accordance with the requirements for their safety and security, and their importance for maintaining the function of the information technology.

The different functional zones can be divided as shown in Table 13 on page 52.

Layout of safety zones

A schematic presentation of the various safety zones produces something like the example illustrated in Figure 12: the IT zone (red) is situated in the interior and is protected by the adjacent zones 3 and 4 (yellow/blue). Safety zones 1 and 2 (white/green) form the outer layers. The individual safety zones are divided by safety lines.

Safety zones	Function	Identification (example)
1	*Plot*	*White*
2	*Semi-public area, neighbouring offices*	*Green*
3	*Operating areas, rooms adjoining IT*	*Yellow*
4	*Technical systems for operating IT*	*Blue*
5	*IT and network infrastructure*	*Red*

Table 13: Functional areas of a data centre

Figure 12: Safety zones in the data centre

The safety lines represent the monitored, safe transition from one zone to another, and are set up in conformity with the company's safety requirements.

A fitting solution for avoiding possible sabotage is to separate the functional zones by ensuring limited access to sensitive areas. For example, a maintenance technician for the air-conditioning systems or UPS has access only to the technical zones (blue), not to the company's IT zone (red).

The locations of the different functional areas and the division of the safety zones or safety lines are important for guaranteeing the safety of the IT infrastructure. However, continuous IT availability can only be achieved through a comprehensive safety plan, which takes account of all aspects of IT security and safety.

9 Wiring

9.1 Current situation

The primary, original task of data centres is to run IT applications on mainframes and servers, to maintain data and save it on storage systems.

From an IT point of view, the principal requirement is availability, i.e. the ability of IT applications that are generally critical for companies to remain operational, as far as possible without any interruption. These typically include ERP systems, production applications in industrial companies, databases, office applications and their operating systems, and also access to provider networks (MAN, WAN) and to the internet.

The ISO-OSI 7 Layer Reference Model applies to the IT, and this defines the application as the uppermost layer, and the physical infrastructure required for transporting the data, the IT wiring and data transport devices as the lowest, or first, layer, e.g. layer 1 switches.

Therefore, the IT wiring is of fundamental importance for the availability of IT applications in a data centre: without functioning IT wiring, IT devices such as servers, switches and storage devices cannot communicate with each other or exchange, process, hold or save data.

It is frequently the case, however, that IT wiring has simply grown over time, and only satisfies today's requirements, such as

- high duct densities
- high transmission speeds
- interruption-free hardware modifications
- service support, and
- ventilation issues

with difficulty.

The structuring of IT wiring and meticulous, anticipatory planning are therefore key tasks for a data centre operator. Legal principles such as Basel II or SOX also demand rigorous and comprehensive transparency.

9.2 Underlying standards

State-of-the-art wiring in conformity with DIN EN 50173-5 (VDE 0800-173-5) satisfies the requirement or written stipulation for structured IT wiring that is not tied to a specific application. In addition, this standard expresses clear recommendations for setting up redundant IT wiring, for ensuring high-level reliability of the data centre.

The planning, installation and acceptance testing of IT wiring in data centres is described in the DIN EN 50174 (VDE 0800-174) series of standards. Important contents include the quality plan, safety distances, the distances between copper IT wiring and other electrical sources for the prevention of electromagnetic interference, plus the documentation and acceptance testing of the entire data centre. DIN EN 50310 (VDE 0800-2-310) is the required standard for equipotential bonding in buildings containing IT equipment.

9.3 Quality, selection of components/ systems

Requirements for maximum availability and ever faster data transmission rates mean that the quality requirements facing IT wiring components for data centres are many times more exacting than those for products used in LANs. When it comes to selecting systems, quality principles should be included in the very early planning phase, with a view to satisfying performance requirements for

- Cable design for copper and fibre-optics

- Bandwidths for copper systems and fibre-optic cables
- Insertion and return loss budgets for fibre-optics
- EMC immunity for copper systems
- Update capability in line with higher speed classes
- 19" cabinet design.

Whether fibre-optic or copper cables are used, the IT wiring components may take the form of factory-assembled, turnkey systems for plug & play installations.

Preassembled systems have the best possible, reproducible quality, and therefore promise very good transmission characteristics and high reliability. Only screened systems may be used in copper systems, due to the demanding availability requirements. DIN EN 50173-5 (VDE 0800-173-5) stipulates at least Class EA for copper wiring.

Sufficient priority must also be lent to the selection of IT wiring suppliers. Besides the quality of the wiring components, the chief requirements for a reliable supplier are specialist data centre expertise, experience with data centre IT wiring and lasting ability to supply. Ideally, the supplier should also offer comprehensive planning, installation and maintenance services

9.4 Structure

Data centres are the company's central nervous system. They are therefore subject to continuous change, driven by the short lifecycles of the active components. In order to avoid fundamental or far-reaching changes to the IT wiring with every new piece of equipment, a physical IT wiring structure that is clearly arranged, transparent and isolated from the surrounding "device pool" is highly recommended.

It should connect the respective device locations to a uniform, consistent IT wiring structure.

In DIN EN 50173-5 (VDE 0800-173-5) [or ISO/IEC 24764], this fixed device wiring is divided into main area distribution and area distribution wiring, at the end of which is the device connection, or interface. The active devices

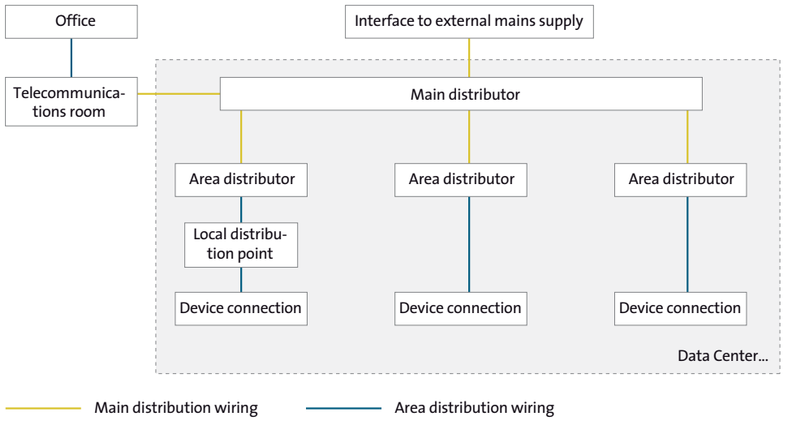

Figure 13: Schematic EN wiring configuration to DIN EN 50173-5

are connected to the "generic" area distribution wiring via the device connection interface by means of device-specific connecting cables that are as short as possible. Consequently, when a device is replaced – which often requires the replacement of the connection face on the device – only the cable specific to this connection has to be replaced. There is no need to carry out work on or strip the area distribution wiring.

Areas with a high packing density are worthy of particular attention in this context.

The above technique ensures that any rewiring involved during equipment replacements are reduced to a minimum both financially and in terms of time – while the defined structure is fully preserved.

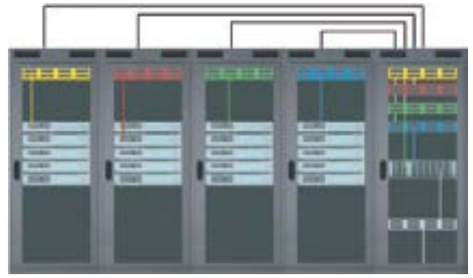

Figure 14: Area distribution wiring (Cu and fibre-optic with area distributor and server/storage cabinets with device connection)

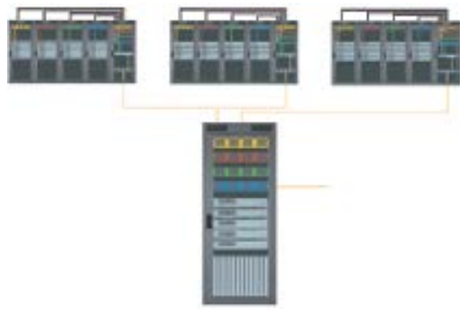

Figure 15: Main distribution wiring (fibre-optic) with main distributor and connection to area distribution wiring (Cu and fibre-optic) with area distributor and server/storage cabinets with device connection

Where necessary, the area distribution wiring must be formed from copper and fibre-optic cables, so that different types of device can be connected. The main distribution wiring should take the form of fibre-optic and copper cables, and offer redundancy.

Suitable plug-in systems must be selected for the device connection interfaces, in accordance with the required packing density of the connected devices. Standards DIN EN 50173-5 (or ISO/IEC 24764) specify suitable plug-in systems.

9.5 Redundancy and reliability

The requirement for high availability means that connections and components must be redundant. Hence, it must be possible to replace hardware during ongoing operation, and an alternative component must take over the running of the application without interruption if a cable fails.

It is therefore obvious that an appropriate, all-inclusive IT wiring platform must be provided, which ensures the correct bending radii, safeguards performance and can be fitted quickly and reliably during operation.

The availability of applications can be increased through the use of preassembled IT wiring systems. This reduces to a minimum the time that installation personnel have to spend in the safety zone of the data centre, both during initial installation and eventual hardware modifications, and also promises additional operational reliability. In addition, care must be taken to ensure that all products are inspected and documented as part of quality management.

For the mutual connection of data centres, e.g. redundant data centres, backup data centres, or simply for backing up and saving data at a different site, the incorporation and security of MAN and WAN provider

networks (data transport services or so-called dark fibres), or dedicated fibre-optic cable runs, is of enormous importance for reliability and availability and, like the IT wiring inside the data centre, must be redundant.

9.6 Installation

Engineers and technicians must be trained in the specifications of the systems in order to ensure the safe, reliable operation of fibre-optic IT wiring in the data centre, particularly in the matter of installation and work with patches. Due to the required wiring, when selecting a 19" server or IT wiring cabinet, and under consideration of item 4.1.2, "Secure server cabinet", the use of cabinet systems at least 800 mm wide is recommended. These enable the installation of an integral cable management system in the vertical and horizontal direction. As a rule, the depth of the cabinet is determined by the passive and active components to be installed inside. Cabinet systems 800 mm deep have proven their suitability for passive distributors. A depth of 1000 to 1200 mm is recommended for cabinet systems destined to accommodate active components. DIN EN 50174-2 (VDE 0800-174-2) contains detailed requirements and recommendations on this topic.

The possible advantage of factory-preassembled IT wiring systems already mentioned in the section on safety principles comes to the fore during installation in the form of time savings. When these systems are employed, it is worth mentioning that when data centre capacity is expanded due to an increase in IT equipment, these devices and hence the IT applications themselves can be wired to one another and brought into operation at the greatest possible speed – and the same applies to hardware modifications.

9.7 Documentation and identification

Painstaking, continually updated documentation is an important means of ensuring the simple management of IT wiring and reliable planning of conversions and upgrades. A large range of possibilities exist in this respect, from "individual" Excel worksheets to proven, software-based documentation tools. Important requirements for system management and documentation are described in DIN EN 50174-1 (VDE 0800-174-1). What is important is that the documentation is always kept up to date, and reflects the actual, installed IT wiring. The choice of tool is at the user's discretion.

Closely linked to documentation is the requirement for clear, easily legible identification of cables, including in poor lighting. Here, too, numerous identification methods are available, e.g. from cable tags with replaceable labels to barcode labels. The type selected will depend on individual requirements. What matters is ensuring identical nomenclature throughout the company. Central management of the data is recommended to ensure clear, unambiguous cable identification.

10 Certification of a reliable data centre

10.1 Introduction

At the level of the infrastructure, the reliable data centre combines various engineering disciplines, such as electrical, mechanical and civil engineering, fire safety, safety technology, etc. The IT level takes account of virtually every facet of information technology, while at organisational level, various management techniques are employed for monitoring and controlling processes.

On the matter of data centre reliability in terms of data availability, confidentiality and integrity, certification procedures based on standards and lists of tests have been established in the following three areas:

- Physical infrastructure
- Information technology
- Organisational procedures

Certification is a process whereby an impartial third party demonstrates that there is sufficient confidence that a product, system, service or process conforms to a particular national and/or international standard or normative document. DIN EN 45020 describes the term "standard" as follows: "A document, established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context."

If no underlying standard exists, the acceptance of the certificate and, in particular, a normative document, depends on the extent to which it has been compiled by experts, there is consensus about its stipulations among other expert groups, and how widespread its requirements find application in the market. The certifying partner is another factor in its acceptance. This partner should be able to offer expertise on the test subject, to have defined certification processes and made them accessible, and be accredited as a certification body.

Due to the complexity of the "data centre system", different certification approaches exist, which test and confirm different areas or selected characteristics of a data centre. Item 3 of this guide sets out the various standards.

10.2 Possible types of certification for data centres

On the physical level of the data centre infrastructure, structural aspects, technical supply systems (electricity, air conditioning) and safety systems (fire alarm and extinguishing systems, intruder alarms, access control systems) are checked to ensure their suitability and correct use. The TSI set of tests devised by the TÜV with this area in mind has asserted itself as the industry standard for the certification of the data centre infrastructure. The series of European EN 50600 standards (some of which are still in development) lays down requirements for the technical infrastructure of data centres and the systems operated within. The TSI list is expected to cover these requirements in future.

Where information technology is concerned, certification generally takes place in the product environment, i.e. on the premises of the manufacturers of IT systems (hardware and software). Since the end of the 1990s, ISO 15408 – also known as the Common Criteria – has established itself in this domain. This international standard defines extensive requirements for safety features and mechanisms, and sets out stipulations for the test methodology.

In the matter of organisational procedures, an array of certification options exists. These concern the certification of the Information Security Management System (ISO 27001 – ISMS), or the evaluation of typical data centre operating processes (ISO 20000 – ITIL), or the examination of measures to maintain operability (BS25999 – Business Continuity). Auditing bodies also offer test services based on their own lists of requirements, e.g. SAS 70 or IDW 951. The results and the procedure are ranked rather differently in this case, as no certificate is granted and, as a rule, the dual control principle (test institution and certifying body) is not applied.

10.3 The certification process

If the data centre is in operation and if the technical concepts and/or organisational procedures and rules are documented and effectively implemented in the company, it can be certified by an independent, neutral, accredited body (i.e. one authorised to grant certification). This institution first inspects the documentation, then the system on site. The auditor possesses the necessary qualifications and professional experience. A positive result leads to certification, which is generally valid for 2–3 years.

The certification procedure follows a set pattern, which can be subject to slight variations depending on the test programme.

A certification meeting should be held before a certification body is selected.

Certification meeting

The subjects under discussion basically include questions about certification and auditing, organisational procedure (e.g. scope and schedule) and costs.

Certification order

By placing an order for certification, the contracting company places itself under obligation to provide the certification body with the necessary documentation. Alternatively, the documentation may sometimes be inspected on site. A preliminary audit may be conducted, if the company so desires.

Performing a preliminary audit

The aim of the preliminary audit is to ascertain whether the basic prerequisites for certification are met. It determines whether the certification audit can be carried out on the planned date with success as the likely outcome.

Preliminary auditing entails an inspection and initial assessment of the documentation. The preliminary audit is basically a random sample test, and does not claim to be complete.

Certification process

During the certification audit, the auditors check whether the documented technical concepts or procedures and routines satisfy the requirements of the relevant rules, and whether the technical installations and the processes and agreements defined by the company conform to the documentation. The process generally has three stages, starting with the perusal of the documentation provided and an initial assessment for adherence to the rules. This is followed by an on-site audit and inspection of the technical concepts in operation, and concludes with the certification process itself, whereby the result recorded in an assessment report is submitted to the certification body.

This is the basis upon which the certification committee of the certification body decides whether or not to grant a certificate.

Routine surveillance audit

During the period of validity of the certificate, annual surveillance audits may take place, depending on the certification procedure.

Routine surveillance audits entail a random sample test of whether:

- Negative finding(s) from the previous audit has/have been remedied
- Organisational changes have been introduced in the company
- The recipient of certification has changed
- The certificate and certification logo are being used correctly
- Recent changes to relevant standards, laws and regulations have been taken into consideration
- The recipient of certification continues to satisfy the requirements.

If the routine surveillance audits are successful, a complete inspection takes place in a new certification procedure after two or three years. TSI certification largely monitors changes since the last certification.

Recertification

For management systems, recertification is carried out after three years. TSI certification does not prescribe routine surveillance audits; instead, recertification takes place after two years.

10.4 The advantages of certification

Certification is neutral proof of compliance with test requirements (industry or other standard), and can offer the following advantages:

- Acquiring new customers, opening the door to new markets
- Strengthening competitiveness
- Eradicating weak points (failure prevention)
- Enhancing interested parties' trust in the effectiveness and efficiency of the organisation
- Improving the company's ranking and creditworthiness
- Reducing the time and cost of quality verification
- International recognition and acceptance
- Making it possible to classify the availability characteristics of a data centre
- Demonstrating that a data centre is being operated in line with the state of the art
- Providing proof for supervisory bodies

10.5 Selecting the right certification partner

The selection of the right certification partner is decisive for the success of the process. As with any service, the price varies, so obtaining several quotes is recommended.

In certain cases, whether a certification body is sufficiently international may be an important cost factor if, for example, company sites in other countries are to be included in the certification process.

Auditors are similarly qualified between one certification body and another, as the authorisation of auditors is dictated by the certification body and monitored by the accrediting agent. However, it is worth noting that different certification procedures with varying depth of testing are employed depending on the focus of investigations (physical infrastructure, information technology, organisational procedures), and there can also be differences in the composition of auditors.

It is therefore not possible to make a general statement about what constitutes the right certification partner. A correctly chosen certification partner is one who supports the objectives pursued by certification to the best of his/her abilities, and specialises in the relevant area (physical, IT, organisational). References from the certification body, accreditation and recognition by third parties can also be important pointers.

For certain standards, approved audit firms can be found on the websites of accrediting agents, see www.dakks.de.

11 Annex

Selection of important rules and regulations:

Part 1	General definitions
Part 2	Power ratings and power rating plates
Part 3	Limiting values for the operating behaviour of the engine, the generator and the generating set
Part 4	Speed governing and speed behaviour of reciprocating internal combustion engines; definitions
Part 5	Operational behaviour relating to synchronous alternators for generating sets
Part 6	Operational behaviour relating to asynchronous alternators for generating sets
Part 7	Controlling and governing equipment for generator operation
Part 8	Operational behaviour relating to generating sets; definitions
Part 9	Acceptance test
Part 10	Small power generating sets; requirements and tests
Part 11	Measurement and assessment of mechanical vibrations in generating sets with reciprocating internal combustion engines
Part 12	Generating sets – Uninterruptible power supply – Dynamic UPS systems with and without reciprocating internal combustion engine
Part 13	Generating sets – Generating sets with reciprocating internal combustion engine for emergency power supply in hospitals and public buildings
Part 14	Combined heat and power system (CHPS) with reciprocating internal combustion engine – Basics, requirements, components and versions
Part 15	Combined heat and power system (CHPS) with reciprocating internal combustion engine – Tests

German Federal Control of Pollution Act:

4.	Regulation for the Implementation of the German Pollution Control Act (BimSchG), Regulation for Systems Requiring Approval
9.	Regulation for the Implementation of the German Pollution Control Act (BimSchG), Principles of the Approval Procedure
TA	Air German Technical Guidelines on Air Quality Control
TA	Noise German Technical Guidelines on Noise Prevention
BS ISO 8528-1: 2006-02-10	Title (German): Stromerzeugungsaggregate mit Hubkolben-Verbrennungsmotoren – Anwendung, Bemessungen und Ausführungen
ISO 8528-2: 2006-02-10	Title (German): Stromerzeugungsaggregate mit Hubkolben-Verbrennungsmotoren – Motoren
BS ISO 8528-3: 2006-02-10	Title (German): Wechsel-Stromerzeugungsaggregate mit Antrieb durch Hubkolben-Verbrennungsmotoren-Wechselstrom-Generatoren für Stromerzeugungsaggregate
BS ISO 8528-4: 2006-02-03	Title (German): Stromerzeugungsaggregate mit Hubkolben-Verbrennungsmotoren – Steuer- und Schalteinrichtungen
BS ISO 8528-5: 2013-04-30	Title (English): Reciprocating internal combustion engine driven by alternating current generating sets. Generating sets
BS ISO 8528-6: 2006-02-03	Title (German): Stromerzeugungsaggregate mit Hubkolben-Verbrennungsmotoren – Prüfverfahren

DIN ISO 8528-7: 1997-11	Title (German): Stromerzeugungsaggregate mit Hubkolben-Verbrennungsmotoren – Teil 7: Technische Festlegung für Auslegung und Ausführungen (ISO 8528-7:1994)
DIN 6280-13: 1994-12	Title (German): Stromerzeugungsaggregate – Stromerzeugungsaggregate mit Hubkolben-Verbrennungsmotoren – Teil 13: Für Sicherheitsstromversorgung in Krankenhäusern und in baulichen Anlagen für Menschenansammlungen
DIN EN 50173-5 (VDE 0800-173-5)	Information technology – Generic cabling systems – Part 5: Data centres
DIN EN 50174-1 (VDE 0800-174-1)	Information technology – Cabling installation – Part 1: Installation specification and quality assurance, information technology
DIN EN 50174-2 (VDE 0800-174-2)	Information technology – Cabling installation – Part 2: Installation planning and practices inside buildings
DIN EN 50310 (VDE 0800-2-310)	Application of equipotential bonding and earthing in buildings with information technology equipment
DIN EN 50600-1 (VDE 0801-1)	Information technology – Data centre facilities and infrastructures – Part 1: General concepts
E DIN EN 50600-2-1 (VDE 0801-2-1)	Information technology – Data centre facilities and infrastructures – Part 2: Building construction
E DIN EN 50600-2-2 (VDE 02/02/0801)	Information technology – Data centre facilities and infrastructures – Part 2-2: Power distribution
DIN VDE 0100-551 (VDE 0551)	Low-voltage electrical installations – Part 5-55: Selection and erection of electrical equipment – Other equipment – Section 551: Low-voltage generating sets
DIN VDE 0100-560 (VDE 0560)	Low-voltage electrical installations – Part 5-56: Selection and erection of electrical equipment – Safety services
DIN VDE 0100-710 (VDE 0710)	Low-voltage electrical installations – Requirements for special installations or locations – Part 710: Medical locations
DIN VDE 0100-718 (VDE 0718)	Low-voltage electrical installations – Requirements for special installations or locations – Part 718: Communal facilities
PSC	Connection conditions of PSCs
VDEW	Guidelines for emergency generating sets by the German Electricity Association (VDEW)
VDEW	Parallel operation with the low-voltage network by the German Electricity Association (VDEW)
EltBauVO	Ordinance governing the construction of operating rooms for electrical installations
VDS	Regulations from the German Association of Property Insurers
WHG	German Water Resources Act
German Law on the Taxation of Mineral Oil	(Operation of stationary systems with fuel oil)
DIN 31051	Maintenance

12 Glossary

- **19" cabinet**
  Rack with approximately 40 height units, overall height approximately 2 metres, installation width 483 mm, installation height is measured in height units (HU), 1 HU = 44.45 mm
- **CW**
  Chilled Water; air-conditioning systems with chilled water
- **Data centre**
  Server room and/or data centre
- **DX**
  Direct eXpansion; air-conditioning systems with refrigerant
- **EMC**
  ElectroMagnetic Compatibility
- **Emission**
  Influences emitted by a device that affect the environment
- **IT**
  Information Technology (formerly EDP – Electronic Data Processing)
- **Immission**
  Influences originating from the environment that affect a particular location
- **Modular**
  Describes a system that is constructed of several modules (assemblies)
- **PDU**
  Power distribution unit or low-voltage distribution system
- **PSC**
  Power Supply Company
- **Parallel operation**
  Two or more installations jointly supply connected consumers
- **Precision air-conditioning system**
  Air-conditioning system that is able to keep both the temperature and the air humidity constant. The parameters of the air at the inlet openings of the IT units should be between 22 and 27°C and 40 and 60% r.h.
- **Redundant**
  Duplicate arrangement to increase availability (error tolerance)
- **Scalable**
  Step-by-step adaptability to requirements
- **Standby generator**
  (mostly an emergency diesel generator)
- **UPS**
  Uninterruptible power supply

13 Acknowledgements

This “Reliable Data Centre” guide was compiled in consultation with the BITKOM “Data Centre & IT Infrastructure” working group.

We wish to express our sincere thanks to all members of the working group for the valuable discussions we had with them, and our particular thanks go to the following for their involvement:

- Harald Becker
  Rosenberger-OSI GmbH & Co. OHG
- Dr. Gerald Berg
  Rosenberger-OSI GmbH & Co. OHG
- Klaus Clasen
  Notstromtechnik Clasen GmbH
- Peter Clauss
  Wagner Group GmbH
- Joachim Faulhaber
  TÜV Informationstechnik GmbH
- Helmut Göhl
  O2 GmbH
- Christian Leu
  Minimax GmbH & Co. KG
- Matthias Lohmann
  TÜV Secure
- Wilhelm Lorz
  Atos IT-Solutions and Services GmbH
- Helmut Muhm
  Dipl.-Ing. W. Bender GmbH & Co.KG
- Torsten Ped
  Notstromtechnik Clasen GmbH
- Achim Pfleiderer,
  Stulz GmbH
- Dr. Jörg Richter
  I.T.E.N.O.S GmbH
- Harry Schnabel
  Schnabel Consult GmbH
- Christian Schneider
  Siemens AG
- Michael Schumacher
  Schneider Electric GmbH
- Peter Wäsch
  SCHÄFER Ausstattungs-Systeme GmbH
- Thomas H. Wegmann
  DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE
- Manfred Willnecker
  Emerson Network Power Systems EMEA
- Ralph Wölpert
  Rittal GmbH & Co. KG
- Ingo Zimmermann
  AXA

In addition, the following people kindly helped to work on earlier versions:

- Silvia Bader
  DEKRA certification GmbH
- Aykut Güven
  DEKRA certification GmbH
- Frank Hauser
  Server Technology International
- Dieter Henze
  Rittal GmbH & Co. KG
- Dr. Siegbert Hopf
  Masterguard GmbH
- Peter Koch
  Emerson Network Power Systems EMEA
- Knut Krabbes
  QMK IT-Security+Quality
- Stephan Lang
  Weiss Klimatechnik GmbH
- Ingo Lojewski
  Emerson Network Power GmbH
- Hans-Jürgen Niethammer
  Tyco Electronics AMP GmbH
- Thorsten Punke
  Tyco Electronics AMP GmbH
- Zeynep Sakalli
  euromicron solutions GmbH
- Dr. Sandra Schulz
  Giesecke & Devrient GmbH
- Jürgen Strate
  IBM Deutschland GmbH
- Karlheinz Volkert
  Orange Business Germany GmbH
- Judith Wagener
  Bull GmbH
- Eckhard Wolf
  AEG Power Supply Systems GmbH

We extend our particular thanks to Harry Schnabel, Chairman of the BITKOM Data Centre & IT Infrastructure working group for many years.

You can find information on the topics mentioned, and the activities and members of the working group, on the internet at: www.bitkom.org/rechenzentren

The Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. represents more than 2,000 companies, over 1,200 of them direct members with turnover of approx. 140 billion euros and 700,000 employees. These are almost all global players, plus 800 high-performing medium-sized companies and numerous creative, founder-run companies. Members are suppliers of software and IT services, telecommunications and internet services, manufacturers of hardware and consumer electronics, and companies from digital media and electricity grid management. BITKOM's principle mission is the modernisation of the education system, an innovative economic policy and a future-oriented electricity grid policy.

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstrasse 10 A
D-10117 Berlin-Mitte
Tel.: +49 (0)30 27576-0
Fax: +49 (0)30 27576-400
bitkom@bitkom.org
www.bitkom.org