

Rittal – The System.

Faster – better – everywhere.

► The world of IT infrastructures

Background information and decision-making criteria



Rittal – The System.

Faster – better – everywhere.

► The world of IT infrastructures

Background information and decision-making criteria



FRIEDHELM LOH GROUP



The author Martin Kandziora, born 1967, has been Vice President Market Communications at Rittal in Herborn since 2004. On completing his studies in electrical engineering in Stuttgart, he started his career as a project engineer. Subsequently, he changed course and worked in the media sector as a specialist journalist, during which time he spent five successful years developing the Elektro Automation trade magazine. In 2000 he began his marketing career at a software company in Munich. Martin Kandziora is involved with various professional associations and committees. He also writes numerous articles for both the German and English-language press.

The Rittal technology library, volume 4

Editor: Rittal GmbH & Co. KG
Herborn, September 2014

All rights reserved.
No duplication or distribution
without our express consent.

The publisher and authors have taken
the utmost care in the preparation of all text
and visual content.

However, we cannot be held liable for any
content that is incorrect, incomplete or out-of-
date. Under no circumstances will the publish-
er and authors accept any liability whatsoever
for any direct or indirect damages resulting
from the application of this information.

Copyright: © 2014 Rittal GmbH & Co. KG
Printed in Germany

Produced by:
Rittal GmbH & Co. KG
Martin Kandziora, Dagmar Liebegut
Graphics: Günter Muhly Grafik, Marketing-
und Werbeberatung GmbH, Allendorf (Lumda)
Printed by: Wilhelm Becker
Grafischer Betrieb e.K., Haiger



ENCLOSURES

POWER DISTRIBUTION

CLIMATE CONTROL

Preface

As the company and the digitalisation of its business processes grows, so too does the need for commensurate physical IT hardware. The rooms and IT infrastructure in which the computers or data storage systems are housed also have to be aligned with the technology. At the same time, the demand for improved security, higher availability and better energy efficiency in modern data centres is constantly growing. The aim is also to construct or modernise data centre infrastructures on a sustainable basis. Scalable, modular and efficient IT infrastructure solutions realise these requirements. This overview is a criteria catalogue and reference work aimed to help you determine your individual needs. The compact guide takes into account the various aspects of IT infrastructure, ranging from power supply and distribution to network technology, and from effective cooling methods to key performance indicators, monitoring and the rack in the data centre. Different approaches to delivering solutions provide you with useful perspectives for your own IT infrastructure.

We – the IT experts from Rittal – hope you enjoy reading it.

Special thanks for the invaluable technical support and constructive feedback go to Heinrich Styppa, Hartmut Lohrey, Bernd Hanstein, Michael Nicolai, Günter Muhly and Burkhard Weber.

Wishing you every success.

Yours
Martin Kandziora

Rittal – The System.

Faster – better – everywhere.



ENCLOSURES

POWER DISTRIBUTION

CLIMATE CONTROL

Contents

	Page
Basic principles for IT infrastructures	21
System components for IT infrastructures	65
Solutions for IT infrastructures	95
Expert knowledge	111

Rittal – The System.

Faster – better – everywhere.

» nextlevel

for data centres

Rittal opens up brand new perspectives for the IT world. Be it the standardised RiMatrix S data centre module or efficient individual components – everything is available off the shelf with short delivery times.

Rittal – The System.

- Rittal – Series-produced modular and standardised data centres with RiMatrix S
- Rittal – System components for individual IT solutions



ENCLOSURES

POWER DISTRIBUTION

CLIMATE CONTROL



nextlevel

for data centres

IT INFRASTRUCTURE

SOFTWARE & SERVICES



Rittal – The System.

Faster – better – everywhere.

IT infrastructure from the smallest to the largest

- RiMatrix S
- IT enclosure systems
- IT enclosures
- IT power
- IT cooling
- IT monitoring
- IT security solutions



ENCLOSURES

POWER DISTRIBUTION

CLIMATE CONTROL

- RiMatrix S – the first standardised data centre as a turnkey infrastructure solution
- IT security rooms – certified to ECB-S



IT INFRASTRUCTURE

SOFTWARE & SERVICES



Your benefits with RiMatrix

Unique IT system solutions from Rittal provide state-of-the-art data centre infrastructures. You can select standardised components from the RiMatrix system components, IT enclosure systems/enclosures, IT power, IT cooling, IT monitoring and IT security solutions. This ensures the IT infrastructure is tailored perfectly to your requirements – leaving plenty of flexibility for future expansion.



ENCLOSURES

POWER DISTRIBUTION

CLIMATE CONTROL

Faster – Precise-fit data centre infrastructures with “Rittal – The System.”
Better – Standardised, coordinated system components
Everywhere – Installation and commissioning carried out internationally by our 1,000 service engineers



IT INFRASTRUCTURE

SOFTWARE & SERVICES



Your benefits with RiMatrix S

RiMatrix S is the revolutionary alternative in data centre construction. Based on pre-configured, complete data centre modules, it supports the creation of standardised data centre infrastructures. The data centre modules already contain all the essential components, such as IT enclosure systems, power back-up and distribution, cooling, monitoring and security solutions. All data centre modules are pre-configured, available off-the-shelf and permit rapid configuration of a customer solution.



ENCLOSURES

POWER DISTRIBUTION

CLIMATE CONTROL

Faster – pre-configured data centre modules available off the shelf

Better – tested, pre-certified data centre modules with outstanding efficiency

Everywhere – can be installed in system-tested security rooms, standard rooms or containers



IT INFRASTRUCTURE

SOFTWARE & SERVICES



Rittal – The System.

Faster – better – everywhere.

RiMatrix S Selector

Your solution is configured on the basis of standardised data centre modules.

- The planning phase, delivery and commissioning times are significantly reduced.
- A precise efficiency calculation (including consumption figures) based on the data sheet is always included as part of our consulting service.
- Standardisation leads to significant savings potential.
- The data centre modules are complete functional units (including power, cooling and monitoring).
- The modules are completely configured, have a data sheet and can therefore be ordered off the shelf using a Model No.



ENCLOSURES

POWER DISTRIBUTION

CLIMATE CONTROL

The first series-produced data centre. Simply plug in and it's ready to use.

RiMatrix S App

Your configurator for standardised data centres for SMEs, branch concepts and flexible cloud applications.

An intuitive user interface will guide you to your complete data centre in five easy steps:

1. Requirements and peripheral conditions
2. Technical specifications
3. Standardised module selection
4. Optional packages
5. Your RiMatrix S solution



IT INFRASTRUCTURE

SOFTWARE & SERVICES



Rittal – The System.

Faster – better – everywhere.

2014/2015 catalogue

Our 2014/2015 catalogue contains the latest order information for the entire Rittal product portfolio. Clearly structured and with useful cross-references to matching accessories, alternative products and important information. See for yourself!



- Complete order information, structured according to your requirements
- Clear allocation of accessories
- Further information on the Internet

RiMatrix S

RiMatrix S Single & Double 8

- 8 server enclosures
- 1 network enclosure
- Two separate, supported climate zones for server and technology zones
- UPS, battery case and distribution enclosures
- Space-saving climate control in the raised floor

- Consistent separation of cold air intake and warm exhaust air integrated into the mechanical concept
- Cable routing above the racks
- In the Double 8, the second module is a mirror image with integral cold aisle

RiMatrix S Single 9/Double 9

- 9 server enclosures
- 1 network enclosure
- 1 climate zone for server racks
- Other using a pre-existing UPS
- Distribution enclosures
- Space-saving climate control in the raised floor

- Consistent separation of cold air intake and warm exhaust air integrated into the mechanical concept
- Cable routing above the racks in the Double 9, the second module is a mirror image with integral cold aisle

Standard room

	Single 8	Double 8	Single 9	Double 9
External dimensions (mm)				
height	2750	2750	2750	2750
depth	1000	1000	1000	1000
Internal dimensions (mm)				
height	2750	2750	2750	2750
depth	700	700	700	700
Module No.	7000_108	7000_107	7000_408	7000_407
Physical security				
Fire protection				
Burglar resistance				
Anti-jam system				
Lock and master protection				
Safe fire detection				
Non-intrusive system				
Identification and identification system			Optional	Optional
Identification			Optional	Optional
Climate				
Climate in raised floor (R10) + R1000	4 zones	10 zones	4 zones	10 zones
R10 + R1000 + R1000	1 zone	2 zones	1 zone	2 zones
Power protection, see also 10 pages 401	80 kW + 20 kW	2 x 80 kW + 20 kW	--	--
Net. capacity	1 x 20 kW	2 x 20 kW	--	--
Net. power	1 zone	2 zones	10 modules	--
Net. power (max. capacity)	10 kW	20 kW	10 kW	20 kW
Net. power (R1000)	10 kW	20 kW	10 kW	20 kW
Net. power (R1000 + R1000)	100 kW + 20 kW	200 kW + 20 kW	100 kW + 20 kW	200 kW + 20 kW
Net. power (R1000 + R1000 + R1000)	100 kW + 20 kW	200 kW + 20 kW	100 kW + 20 kW	200 kW + 20 kW
Net. power (R1000 + R1000 + R1000 + R1000)	100 kW + 20 kW	200 kW + 20 kW	100 kW + 20 kW	200 kW + 20 kW

ENCLOSURES

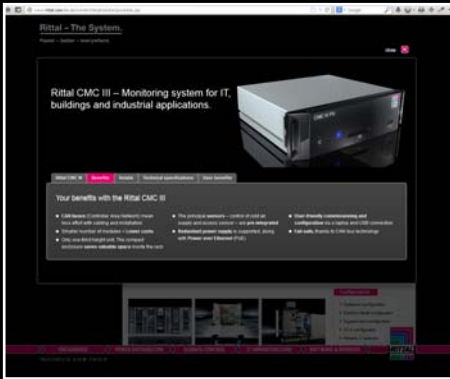
POWER DISTRIBUTION

CLIMATE CONTROL

Get to know the benefits

Internet

Sometimes pictures say more than words. With this in mind, we have prepared web pages or selectors/configurators for many of our products, outlining the benefits in a clear and transparent way, and making it easier for you to select the right one. Take a look for yourself!



Web pages

- Clearly demonstrate the benefits
- Elucidation of arguments
- Offer special background information
- Provide handy tips



Selectors/ configurators

- Simple to configure
- Test out various solution options
- Request a binding quote

IT INFRASTRUCTURE

SOFTWARE & SERVICES



Rittal – The System.

Faster – better – everywhere.

Technical details – Technology Library

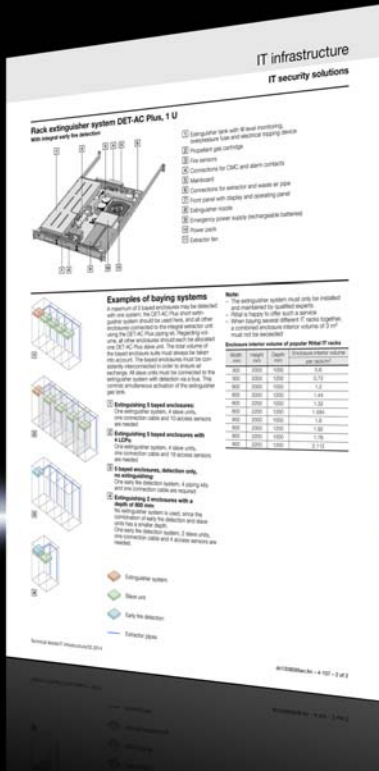
Do you need detailed technical information on your desk, in the workshop or at the construction site?

If so, request a copy of our comprehensive compendium, “Technical Details”.

Looking for tips on the project planning and operation of enclosure systems? Look them up in the Rittal “Technology Library”. This is a high-quality series of technical literature in compact form for industry and IT users.

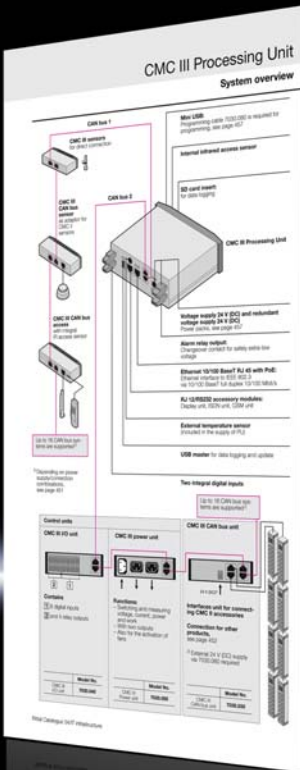
Current publications:

- Standard-compliant switchgear and controlgear production
- Enclosure and process cooling
- Technical aspects of enclosures



Technical system catalogue in PDF format

Looking for a simple solution for your task? Take a look at our technical system catalogue, available to download from our website in PDF format. You will soon recognise the infinite possibilities afforded by “Rittal – The System.”.



- Clear presentation of the benefits
- Unequivocal product advantages
- Intelligible explanation of principles
- Handy application tips



IT INFRASTRUCTURE

SOFTWARE & SERVICES



Rittal – The System.

Faster – better – everywhere.

Make **IT** easy.

ENCLOSURES

POWER DISTRIBUTION

CLIMATE CONTROL

Basic principles for IT infrastructures

	Page
Introduction	22
Availability as a matter of cost	24
Examples of the interdependency of output, availability and costs	25
Capacity	26
Capacity and sustainability	26
Availability	28
Individual availability requirements	28
Levels of availability (tiers)	29
Availability classes (VK)	30
IT availability checklist from TÜV Rheinland	32
Factors affecting availability	34
Availability through thermal safety	35
The comprehensive power supply and power back-up	36
Availability through physical protection	45
Availability planning criteria	46
Efficiency	48
Factors for efficient IT	48
Calculation formula for data centre energy efficiency	50
How to increase the efficiency of a data centre	52
Data Centre Infrastructure Management System (DCIM)	54
Location	56
Location factors	56
The future	62
Options for future IT infrastructures	62

■ Introduction

Corporate IT

Regardless of whether it's a small, medium or large company, practically every business, service organisation or public institution requires a functioning information technology system. The data centre is complex, as we want to use it to implement technical innovations and organisational changes. The answer to this challenge, as well as the increasing demand for availability, security and a high level of energy efficiency, is the IT infrastructure solution of the future.



The IT infrastructure

Irrespective of the size of the data centre, the IT infrastructure covers the following areas:

- 1 Racks and housings for server and network components
- 2 Power distribution and back-up
- 3 Cooling using cooling transport and distribution
- 4 Monitoring and remote management using hardware and software components
- 5 Security components for detecting and extinguishing fires
- 6 Security solutions through certified security areas or safes

ENCLOSURES

POWER DISTRIBUTION

CLIMATE CONTROL

A trend towards all-in-one data centres, e.g. as a container solution, is also emerging. These units have a modular and flexible structure, can be implemented quickly and are adaptable.

In this case, a distinction is often made between the productive unit and the cooling container (see RiMatrix S, page 100, as an example).



The economic factors of the IT infrastructure

The key requirements of modern IT infrastructures are capacity, availability, security and energy efficiency. These are the main factors behind acquisition and operating costs. The following are decisive in shaping the design of the data centre:

- Flexibility
- Location selection
- Type and size
- Security and availability
- Electrical power
- Heat dissipation
- Cabling
- Energy efficiency
- Future-proof with regard to scalability
- Investment and operating costs

Availability as a matter of cost

Interactions

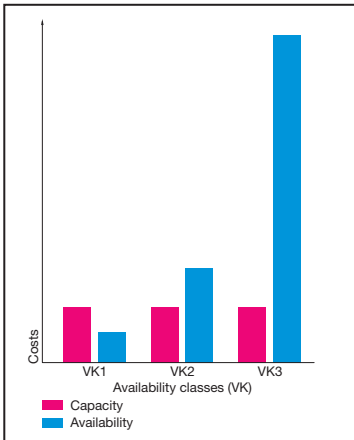
Continuous operation is the key to a reliably functioning information processing system. Insufficiently protected information represents a risk that is often underestimated and can ultimately threaten the survival of the company.¹⁾

Data centres form the physical basis of the IT infrastructure. Essential pillars of the economy, such as banks, insurance companies, car manufacturers and suppliers, would not be able to operate today without permanently available and secure IT infrastructures. The backbone of the Internet itself is

also to be found in data centres. The national economy depends on having IT services with a high level of availability, a challenge that is met by data centres.

The main goal is availability

Linking the physical data centre infrastructure to server and application management ensures the continuous monitoring of IT services. Detecting malfunctions at an early stage enables you to act in time and ensures that the defined levels of availability are maintained.

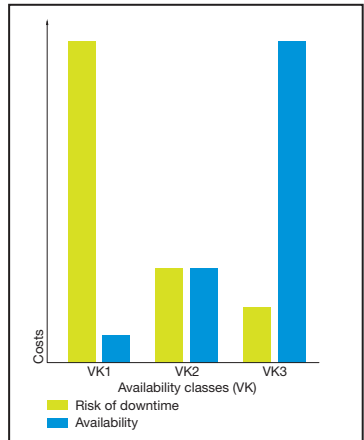


The higher the level of availability required, the greater the investment and operating costs, assuming the same level of data centre productivity.

The following mathematical formula for IT availability can be used:

$$\text{MTBF}/(\text{MTBF} + \text{MTTR})$$

The MTBF (Mean Time Between Failures) is the amount of time between



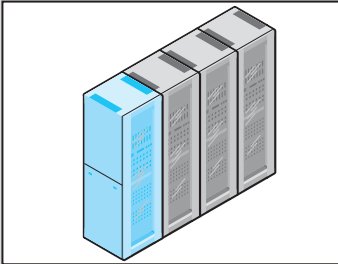
The risk of a damaging loss of productivity is minimised by increasing availability.

one failure and the next. MTTR (Mean Time To Repair) is understood to be the average time required to repair the data centre and/or the integrated components.

¹⁾ www.bsi.bund.de

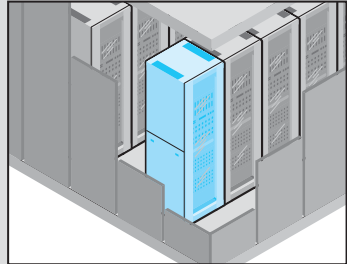
Examples of the interdependency of capacity, availability and costs

As shown in these two examples, it is crucial to precisely determine the availability requirement. An increase in availability from 99% (VK 1) to 99.99% (VK 3) results in a significant reduction in downtime. However, an increase in availability incurs significantly higher costs for the IT infrastructure and its operation.



Example 1 (VK 1: 99%) Downtime of 88 hours per year

If an SME builds and uses a data centre, as a rule it will mainly be used during working hours from Monday to Friday. During this period, the availability demand is high, and it may also be high during the night if the company is an international organisation. Availability is usually less of a concern at the weekend.



Example 2 (VK 3: 99.99%) Downtime of 52 minutes per year

If a bank or an online department store is planning its own IT cluster or a trading cluster, the overriding priority is reliability. The entire infrastructure must ensure maximum availability. However, the redundancies required for this purpose drive up investment costs. When compared with the potential costs of downtime, however, redundancy is worthwhile and a wise investment.

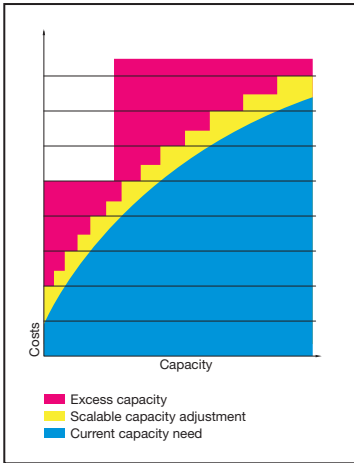
■ Capacity

Capacity and sustainability

Whether your company is small, medium-sized or large, the requirements on IT performance and services are growing.

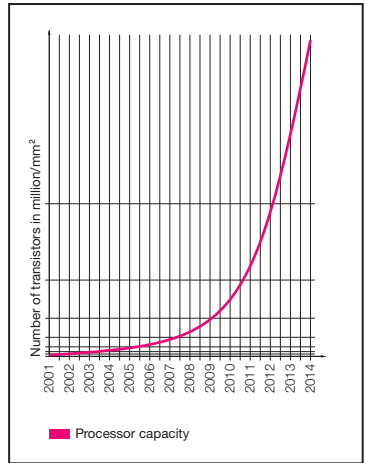
- Ongoing server development and server consolidation
- Implementation of new applications for automating business processes and thereby increasing load capacity of the IT network
- Introduction of new technologies and centralisation of IT and therefore the “IT traffic”
- Greater number of users
- Virtualisation of IT solutions
- Modernisation and use of cloud-based applications, thereby distributing the load
- Availability requirements

The aim is to deliver a scalable and flexible data centre solution so that the IT itself can continue to be developed in a highly dynamic manner.



“Pay as you grow” – Changing to meet current need

A data centre has to be continually updated to meet the growing capacity requirements of the hardware. High levels of excess capacity drive up costs.



Development dynamics

The current development dynamics show that processor capacity doubles every 18 months. New data centres should therefore account for this development trend through flexible and modular expansion concepts.



The most compact unit in a data centre is the IT rack with cooling, monitoring, UPS, servers and network

■ Availability

Individual availability requirements

Fundamental aspects need to be considered and decisions made if a successful emergency restoration plan is to come to fruition. This includes looking at availability and the potential impact of system downtime on the running of an organisation. The following questions help identify the availability requirements:

- What are the requirements in terms of availability? During which period must your client security service be online each day?
- What costs will the company incur in the event of a failure?
- How much downtime would be acceptable if a medium (e.g. a storage device) were not available?
- How much client security service downtime would be acceptable in the event of an emergency, e.g. loss of servers following a fire?
- How important it is that data must never be lost?
- How easy would it be to restore lost data?
- Are there any system administrators in the company and what role do they play?
- Who is responsible for the back-up/restore processes?
- What qualifications do the relevant employees have?¹⁾

The ongoing development and integration of information technology in all areas of business means that: not even the smallest company can afford to have its IT system to go down.

Even just a few years ago, a few hours downtime for a company's IT system would have been tolerable. Today, the number of companies for whom continuous availability of their IT systems is crucial is increasing rapidly.



Availability expectations vary according to user and application.

That is why the availability of the IT infrastructure within a company is a key factor when creating and expanding or monitoring the IT concept. The ensuing key question is therefore:

“What are the maximum tolerable downtimes of the company's IT systems?”²⁾

¹⁾ Microsoft TechNet Library

²⁾ BITKOM, Reliable Data Centre

Levels of availability (tiers)

Data centres are complex systems; it is the interaction between all their active and passive IT components that influences availability. The actual required availability of an IT infrastructure must be estimated during the concept phase. An assumption has to be made as to the maximum tolerable

downtime per year of a company's IT infrastructure.

The renowned US Uptime Institute has defined a number of availability classes, which are referred to as the Industrial Standards Tier® Classification¹⁾:

Tier I

1960s:
Single power supply path, single cooling supply, no redundant components

**99.671%
availability**

Tier II

1970s:
Single power supply path, single cooling supply, redundant components

**99.741%
availability**

Tier III

End of 1980s:
Several paths available, though only one active, redundant components, maintenance possible with no operational interruptions

**99.982%
availability**

Tier IV

1994:
Several active power and cold water distribution paths, redundant components, fault-tolerant

**99.995%
availability**



These have risen sharply due to the Internet and the prevalence of IT-based processes.

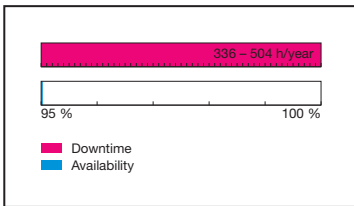
¹⁾ BITKOM, Reliable Data Centre

Availability classes (VK)

As the demands made on the availability of the IT infrastructure have grown, so too have the requirements placed on IT systems. What is now commonplace in high-availability IT infrastructures is redundancy of the climate control and power supply systems. Redundancy in these cases is provided by duplicated infeeds and interruption-free maintenance of the systems. Availability is calculated from the downtime and the overall productive time of the system (data centre).

$$\text{Availability} = (1 - \text{downtime} / \text{productive time} + \text{downtime}) \times 100$$

An IT system is deemed to be available when it is able to carry out the tasks for which it was designed. Availability is expressed as a percentage and is categorised by availability classes.

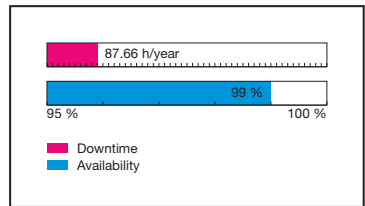


**AC 0: ~ 95%
downtime = 2 – 3 weeks**

- No requirements in respect of availability
- No measures to be implemented with regard to availability.
- The implementation of IT baseline protection for the other fundamental values is beneficial in terms of availability.

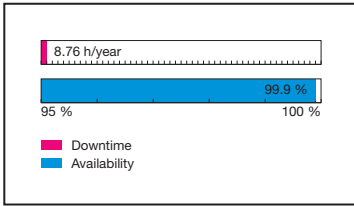
Bundesamt für Sicherheit in der Informationstechnik (Federal Office for IT Security – BSI):

- The BSI has developed an assessment system for data centres called VAIR (from the German “Verfügbarkeitsanalyse der Infrastruktur in Rechenzentren” – Availability Analysis of Infrastructure in Data Centres). Data centre operators can visit www.vair-check.de and enter their infrastructure data anonymously and free of charge and check the fail-safe results for their data centre.
- The BSI defines:
 - Availability class
 - Designation
 - Cumulative, probable downtime per year/impact



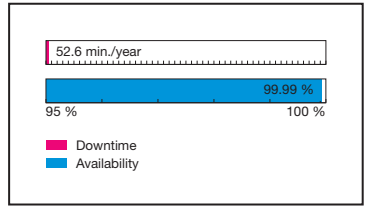
**AC 1: 99.0%,
downtime = 87.66 hrs/year**

- Normal availability
- With regard to availability, the simple use of IT baseline protection (BSI 100-1 and BSI 100-2) satisfies the requirements.



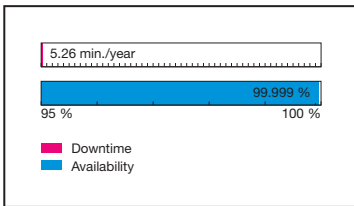
**AC 2: 99.9%
downtime = 8.76 hrs/year**

- High availability
- The simple use of IT baseline protection is to be extended by the use of the modules recommended for high-availability requirements, e.g. an emergency power supply, dealing with security incidents and the use of risk analysis based on IT baseline protection (BSI 100-3).



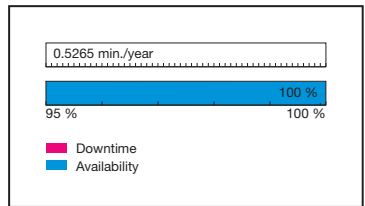
**AC 3: 99.99%
downtime = 52.6 minutes/year**

- Very high availability
- Implementation of the recommended measures as per IT baseline protection that have a significant impact on the basic availability figure for selected objects, e.g. UPS (Uninterruptible Power Supply) in the server room or a secondary power supply for the data centre, supplemented by further high-availability measures from the high-availability compendium.



**AC 4: 99.999%
downtime = 5.26 minutes/year**

- Maximum availability
- IT baseline protection supplemented by modelling according to the HV compendium.
- Using IT baseline protection as a basis is increasingly being replaced and supplemented by high-availability measures.



**AC 5: 100%
downtime = 0.5265 minutes/year**

- “Disaster tolerant”
- Modelling according to the high-availability compendium. IT baseline protection continues to serve as a basis for the above areas and for other desirable aspects, such as integrity and confidentiality. ¹⁾

¹⁾ BITKOM, Reliable Data Centre

IT availability checklist of TÜV Rheinland

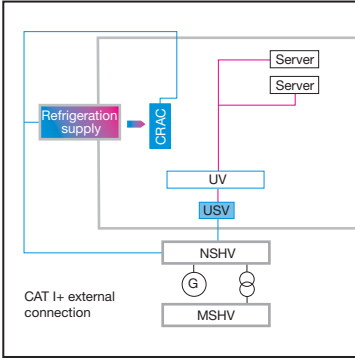
Server room/data centre	n	n+1	2n	2(n+1)
< 400 kVA/to 320 kW/200 m ² CAT	1	2	3	4
Electricity supply				
Medium voltage infeed/mains supply (MV)	■	■	■	2
Transformers	■	■	■	2(n+1)
Low-voltage distribution centre (NSHV)	■	■	■	2(n+1)
Emergency power unit (diesel)	–	■	■	2(n+1)
Uninterruptible power supply (UPS)	■	■	2	2(n+1)
Electrical distribution board in data centre	■	n+1	2	2(n+1)
Rack supply	■	2	2	2
Air conditioning				
Recooler (chillers/cooling)	■	n+1	2n	2(n+1)
Climate control units in computer room	■	n+1	2n	2(n+1)
Pump system	■	2	2n	2(n+1)
Conduits	■	■	Ring	Ring
Building services management				
Display/reporting of operational thresholds	–	■	■	■
Alarm messages via e-mail, SMS, annunciator panels	–	■	■	■
Data recording	–	–	–	■
Evaluation option (ISO 50 001)	optional	optional	optional	optional
Maintenance				
Redundancy	–	■	■	■
Redundant power supplies	–	–	■	■
Maintenance during operation	–	–	■	■
Maintenance window	■	■	–	–

Source: TÜV Rheinland: www.tuv.com

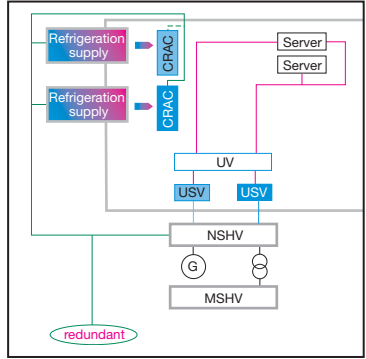
The block diagrams provide an overview of the CAT I to CAT IV categories. These diagrams indicate how a data centre has to be designed according to the availability requirements profile

in terms of infeed, power supply, climate control, building systems and redundancy in order to satisfy the safety requirements and achieve TÜV certification.

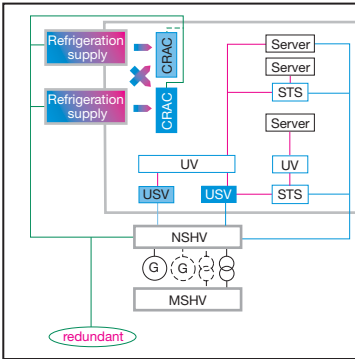
CAT I



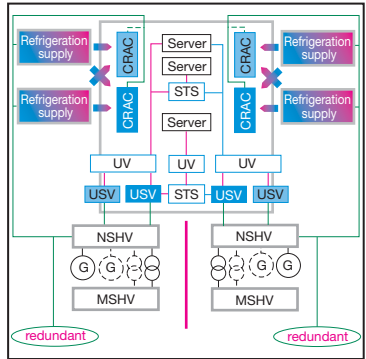
CAT II



CAT III



CAT IV



Legend

- CRAC = Air recirculation unit in the data centre
- UV = Sub-distribution
- UPS = Uninterruptible power supply
- NSHV = Low-voltage distribution centre
- MSHV = Medium-voltage distribution centre
- MS = Infeed/medium voltage
- CAT = Measuring category

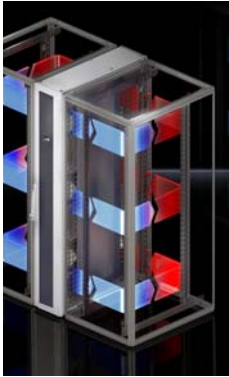
Factors affecting availability

A national and international standard relating to the security of a data centre does not yet exist. In German-speaking countries, TÜV or TSI test

protocols are used to assess the requirements placed on the physical IT infrastructure.

Redundant computer power and IT infrastructure for:

Optimum operating temperature



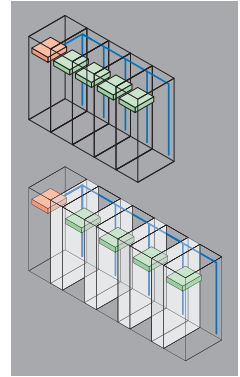
- ASHRAE standard (temperature/humidity)
- Thermal safety: Ensuring adequate heat dissipation (climate control)

Energy back-up



- Safety of the power supply
- Guaranteed even in the event of a power failure by provision of UPS or emergency power supply

Physical security



- For server racks and network enclosures
- Fire detection with very early fire detection, fire extinguishing system
- Intrusion and access control system

Availability through thermal safety

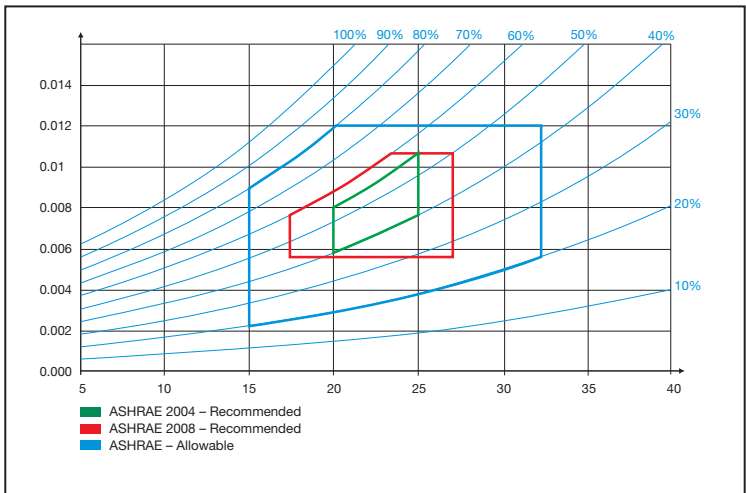
Almost the entire power consumption of a server rack or data centre is ultimately converted into heat. This heat must be dissipated from the server rack or data centre, as only then can the permanent availability of the IT systems be guaranteed. Thermal safety is achieved using the following concepts:

- implementing a climate control concept tailored to the characteristics of the IT rack or data centre
- providing a fully functional ventilation concept in the IT rack

- functionality and operational reliability with regard to heat dissipation (precision climate control)
- using a precision climate control system to provide constant levels of temperature and humidity
- modularity for extensions in the case of individual servers and data centres

Climatic recommendation (based on ASHRAE) in the IT rack:

- Permissible operating temperature short-term + 5°C to + 40°C, recommended 18°C to 27°C, permissible 18°C to 32°C
- Recommended air humidity 20% to 80% relative humidity

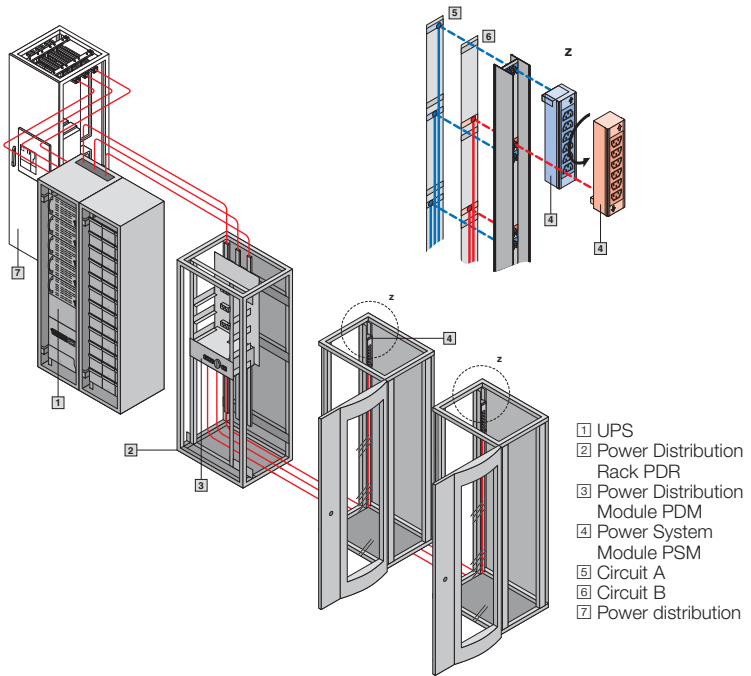


This ASHRAE hx-diagram shows the extent to which the limit values for the climate control requirements placed on servers have changed from 2004 to 2012.

Source: www.ashrae.org

Comprehensive power supply and power back-up

A reliable power supply is crucial to the availability of a data centre. This starts with the infeed and distribution of the power. If the building is connected to a ring main, then the power supply is provided via two medium-voltage lines and is hence redundant. Advantage: Even in the event of the failure of one line, power will still be provided via the second medium-voltage line. Transformers reduce a medium voltage in the range 3 to 30 kV to a low voltage of 400 V.



The power supply is an integral part of the infrastructure components in a data centre.

Features of the voltage in public electricity supply networks according to EN 50 160

Feature	Requirements	Measuring interval	Period under consideration
Mains frequency	Interconnected grid: 50 Hz + 4%/- 6% constant; 50 Hz \pm 1% for \geq 99.5% of the year Stand-alone operation: 50 Hz \pm 15% constant; 50 Hz \pm 2% for \geq 95% of the week	10-sec mean	1 year
Slow voltage changes	$U_{nom} + 10\%/- 15\%$ constant $U_{nom} \pm 10\%$ for $\geq 95\%$ of the week	10-min mean	1 week
Flicker/rapid voltage changes	Long-term flicker strength $P_{it} < 1$ for $\geq 95\%$ of the week and $AU_{10ms} < 2\% U_{nom}$	2 hrs (flicker meter as specified in EN 61 000-4-15)	1 week
Voltage unbalance	U (negative-sequence system)/ U (positive-sequence system) $< 2\%$ for $\geq 95\%$ of the week	10-min mean	1 week
Harmonics U_{n2} to U_{n25}	$<$ limit acc. to DIN EN 50 160 and THD $< 8\%$ for $\geq 95\%$ of the week	10-min mean of every harmonic	1 week
Sub-harmonic	under consideration		1 week
Signal voltages	$<$ standard characteristic – f(f) for $\geq 99\%$ of the day	3-sec mean	1 day
Voltage drops	Number < 10 to 1000/year; 50% with $t < 1$ sec and $AU_{10ms} < 60\% U_{nom}$	10-ms rms value $U_{10ms} - 1$ to 90% U_{nom}	1 year
Short-term power failures	Number < 10 to 1000/year; $> 70\%$ lasting < 1 sec	10-ms rms value $U_{10ms} \geq 1\% U_{nom}$	1 year
Long-term power failures	Number < 10 to 50/year lasting > 3 minutes		1 year
Intermittent overvoltage (L-N)	Number < 10 to 1000/year; $> 70\%$ lasting < 1 sec	10-ms rms value $U_{10ms} \geq 110\% U_{nom}$	1 year
Transient overvoltage	< 6 kV; μ s to ms		Not specified

Low-voltage switchgear in a data centre

In considering the economic aspects of the low-voltage switchgear for a data centre, the local site conditions, the switching duty and the availability requirements must be taken into account. Most important of all is to prevent injury to persons and damage to the plant. When selecting the appropriate switchgear installation, care should be taken to ensure that a type-approved switchgear installation (type approval by testing in accordance with IEC 61 439-1/-2, VDE 0660-600-1/-2) with extended testing of the response in the event of an arc fault (cf. IEC/TR 61 641, VDE 0660-500, supplement 2) is used. The switchgear and protective gear must always be selected by giving precedence to the standards to be adhered to in terms of the requirements placed on the entire network (full selectivity, partial selectivity). The recommendation is as follows: The low-voltage switchgear with busbar isolation is connected to the infeed via busbar systems with standard connection components. This minimises the number of faults. The low-voltage switchgear must be installed at the minimum distances from obstacles as specified by the switchgear manufacturer. The minimum dimensions of operating and maintenance aisles as set out in IEC 60 364-7-729 (VDE 0100-729) are to be observed.

Overall, power distribution requires the highest levels of supply reliability and consistently high transparency, e.g. via a power management system. In addition, a low fire load and low level of interference from electromagnetic fields are also necessary for reliable IT operation.

The following areas are relevant for power supply and back-up:

- One or more independent infeeds, depending on the availability requirements
- Transparent sub-distribution with clear power structure between main and sub-distribution
- Power back-up provided by UPS (uninterruptible power supply) systems
- DC circuit back-up using batteries and alternative power sources, such as photovoltaics or wind power
- Ability to switch the IT load on and off using intelligent socket systems

Reliable power distribution

The requirements placed on the power supply vary in every data centre according to the equipment present. However, the basic power supply is the same in each case. This means that many data centres take a power supply from an electricity supply company, one or more UPS systems, and a generator.

The example of the Rittal and Siemens solution demonstrates how to configure a safe and reliable power distribution system, see page 75.

This includes:

- Low-voltage distribution centre
- Data centre backbone
- Sub-distribution
- Socket systems

The UPS is also powered via the normal sub-distribution system.



Uninterruptible power supply (UPS)

A UPS, known internationally as an Uninterruptible Power Supply, is part of the basic configuration of a data centre. They were originally introduced on oil rigs, where they have been in use since the mid 1960s. The UPS is a critical factor in determining the availability of an IT infrastructure. In Europe, UPS systems are governed by the EN 50 091 standard and satisfy the following requirements:

- to ensure a constant output voltage, even in the event of millisecond peaks (voltage peaks, plus, spikes) or drops (voltage dips, sag) in the mains voltage
- to provide a clean, high-quality sinusoidal output voltage
- to filter dangerously high overvoltages (e.g. lightning strikes)
- to provide adequate reserve capacity in the event of a mains failure in order to ensure an orderly shut-down of the protected systems, or to maintain operations until the permanent reserve systems, such as emergency generators, are activated

The UPS systems generally have two functional units:

- smoothing of voltage peaks, e.g. as a result of lightning strikes and voltage dips
- switching over within milliseconds to battery operation

Battery operation normally lasts 10 to 15 minutes. The battery operation period might have to be extended depending on the destination country. Additional emergency power units or batteries can be connected as part of a hot-swap process. The UPS system and battery capacity is defined according to the specified stored energy time, the types of consumer and the level of consumption. Within this time, any affected systems in the load circuit should be shut down or turned off.



Overview of the IEC 62 040-3 classification code

Classification code							
V	F	I	S	S	1	2	3
Depending on the output		Output voltage curve			Dynamic response of the output		
During normal operation only		1 st letter: Normal or bypass 2 nd letter: Battery mode			1 st number: when operating mode changes 2 nd number: for linear load step (worst case) in normal or battery mode 3 rd number: non-linear load step (worst case) in normal or battery mode		











Meaning of the codes

<p>VFI: UPS output independent of changes in mains voltage and frequency. The power supply is within the limits set out in IEC 61 000-2-2. This is because the power supply is unregulated and, according to the note under this table, IEC 61 000-2-2 only specifies normal harmonic and distortion levels for the voltage, not any changes in frequency.</p> <p>VFD: UPS output depending on changes in mains voltage and frequency</p> <p>VI: UPS output frequency depending on the mains frequency, voltage stabilises (electronic/passive) within the limits for normal operation</p>	<p>S: Output voltage curve sinusoidal. Distortion form D < 0.08 harmonics, etc. < IEC 61 000-2-2 with linear and non-linear ref. load</p> <p>X: Output voltage curve sinusoidal with same quality as "S" with linear load. With linear and non-linear ref. load the distortion factor D is > 0.08 if the load exceeds the limits specified by the manufacturer.</p> <p>Y: Voltage curve not sinusoidal. If the limits set out in IEC 61 000-2-2 are exceeded (see manufacturer's specification for curve type).</p>	<p>1: ≤ Figure 1 in 5.3.1 (no interruption)</p> <p>2: ≤ Figure 2 in 5.3.1 (voltage interruption less than 1 ms)</p> <p>3: ≤ Figure 3 in 5.3.1 (voltage interruption less than 10 ms)</p> <p>4: Contact the manufacturer for details</p>
--	--	---

Note: IEC 61 000-2-2 specifies normal harmonic and distortion levels for the voltage that can be expected on the consumer connection in public grids before the consumer system is connected.

Allocation of power system faults to UPS systems

According to EN 62 040-3, the UPS product standard, the UPS can intercept ten different power system faults:

	Line faults	Time	E.g.	EN 62 040-3	UPS solution	Arrester solution
1.	Power failures	> 10 ms		VFD Voltage + Frequency Dependent	Classifica- tion 3 Passive standby mode (offline)	–
2.	Voltage fluctuations	< 16 ms				–
3.	Voltage peaks	4 to 16 ms				–
4.	Undervoltages	Continuous		VI Voltage Independent	Classifica- tion 2 Line Interactive mode	–
5.	Overvoltages	Continuous				–
6.	Surge	< 4 ms		VFI Voltage + Frequency Independent	Classifica- tion 1 Conversion mode (online)	–
7.	Lightning strikes	Sporadic				Lightning and overvoltage protection (IEC 60 364- 5-53)
8.	Burst	Periodic				–
9.	Voltage harmonics	Continuous				–
10.	Frequency fluctuations	Sporadic		–		

Types of line fault and the appropriate UPS solutions according to IEC 62 040-3 (VDE 0558-530) [12]

UPS operating modes

■ Normal operation

The rectifier is supplied with energy from the network and the battery is charged from the DC link.

■ Battery mode

In the event of a power failure on the public grid. The inverter is supplied with power from the battery until that battery is discharged.

■ Bypass mode

If the Inverter is overloaded or defective. Bypass mode is also activated if the rectifier or the battery develops a fault. The UPS is by-passed.

Conclusion

A UPS not only has the task of supplying the system in the event of a power failure, it must also constantly strive to improve the quality of the power supply.

EN 62 040-3 was drawn up with the goal of classifying UPS systems. It introduced a three-stage classification code, which can be seen in the standard.



Redundancy of UPS systems

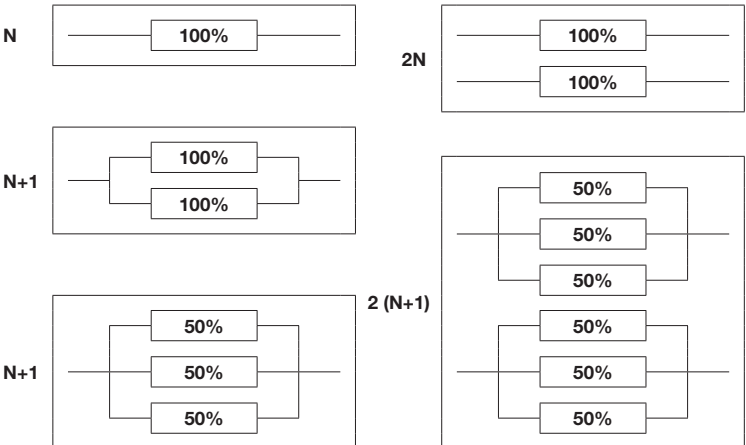
To ensure the security of the power supply, it makes good sense to install redundant UPS systems.

The data centre classification and permissible downtime indicate when redundant UPS systems are necessary.

Date Centre category	UPS			Permissible data centre downtime
	Server enclosure	Server enclosure	Data centre/ server room	
	up to 7 kW	from 7 kW to 40 kW	500 up to 2500 Watt/m2	
A	Standard, min. 10 minutes stored energy time (including ventilation), minimum duration depends on how long it takes to perform a controlled shutdown of the servers		Standard, min. 10 minutes stored energy time, minimum duration depends on how long it takes to perform a controlled shutdown of the servers	12 hrs
B	Redundant (N+1), at least 10 minutes stored energy time			1 hr
C	Redundant (2N), at least 10 minutes stored energy time			10 mins
D	Redundant 2 (N+1), at least 10 minutes stored energy time			< 1 min

Source: BITKOM matrix "Planning aids for a reliable data centre"

The following redundancies can be employed when using UPS systems:¹⁾



¹⁾ BITKOM, Reliable Data Centre

Availability through physical protection

(Excerpts from information published by the BSI (Federal Office for IT Security))

IT baseline protection catalogue

The modules of the IT baseline protection catalogue each contain a brief description of the components, procedures and IT systems under consideration, together with an overview of the security concerns and the recommended measures. The modules are grouped according to the IT baseline protection layer model into the following catalogues:

- B1: Overarching aspects of information security
- B2: Security of the infrastructure
- B3: Security of the IT systems
- B4: Security on the network
- B5: Security in applications

Risk catalogues

This section contains detailed descriptions of the risks that have been cited as security concerns in the individual modules. The risks are grouped into five catalogues:

- G0: Elementary risks
- G1: Force majeure
- G2: Organisational problems
- G3: Human error
- G4: Technical faults
- G5: Deliberate acts

In addition, a risk catalogue G0 Elementary Risks has been introduced; this contains generalised and highly condensed information about the basic risks. This catalogue can, for example, be used as the basis for a risk analysis.

Measures catalogues

This section provides detailed descriptions of the security measures cited in the modules of the IT baseline protection catalogue. The measures are grouped into six catalogues:

- M1: Infrastructure
- M2: Organisation
- M3: Personnel
- M4: Hardware and software
- M5: Communication
- M6: Emergency power supply



Access/authorisation to buildings, room, rack

Availability planning criteria

	Defining the purpose
Planning and design	<ul style="list-style-type: none"> ■ Identifying the application scenarios ■ Weighing up the risk potential ■ Documenting the application decision ■ Generating the safety concept ■ Defining usage guidelines
Procurement (where required)	<ul style="list-style-type: none"> ■ Identifying the requirements of the products to be procured (where possible on the basis of the application scenarios during the planning phase) ■ Selecting suitable products
Implementation	<ul style="list-style-type: none"> ■ Designing and performing test runs ■ Installing and configuring in accordance with the safety guidelines ■ Training and familiarisation of everyone involved
Operation	<ul style="list-style-type: none"> ■ Security measures for the operational system (e.g. logging) ■ Continuous maintenance and enhancement ■ Change management ■ Organising and carrying out maintenance work ■ Audits
Sorting (if required)	<ul style="list-style-type: none"> ■ Rescinding authorisations ■ Removing databases and references to this data ■ Reliable disposal of data media
Emergency power supply	<ul style="list-style-type: none"> ■ Design and organisation of data protection ■ Use of redundancy to increase availability ■ Dealing with security incidents ■ Creating an emergency plan

Source: www.bund.bsi.de

The IT rack as a basis for physical protection

The IT rack provides a basis for the secure accommodation of the servers and IT systems in a data centre.

Requirements for a secure server enclosure

- Scalability to accommodate the 482.6 mm (19") components
- Extendable through a smart range of accessories
- Ease of assembly coupled with reduced complexity of accessories

- Stability, i.e. load-bearing capacity of up to 1,500 kg for high server density and the use of blade servers
- Protection against unauthorised access and access by means of secure lock systems
- Installation of fire detection and fire extinguishing systems
- Facilities for extensions (additional IT racks)

In high-performance data centres, the racks are installed both individually and as bayed systems. A modular server enclosure can be dismantled or modified as required – including the climate control solutions.



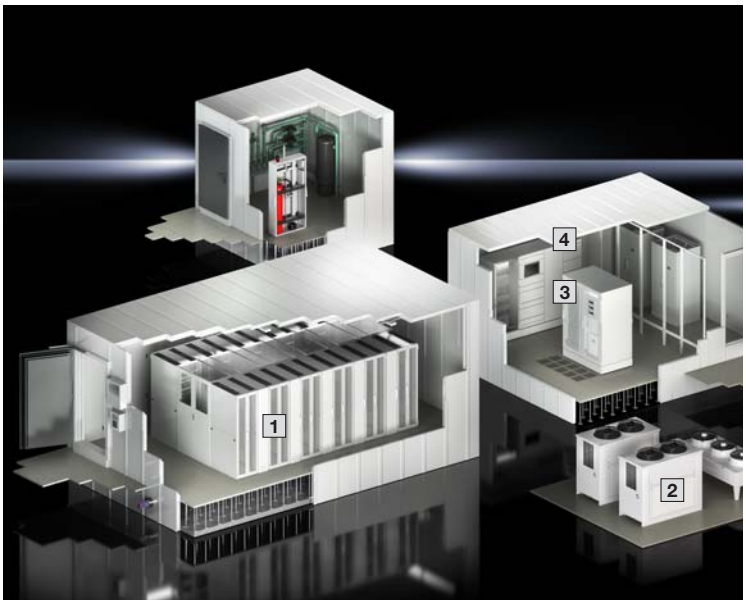
Safe, fire-resistant data centre as a system solution: the Rittal Micro Data Center

■ Efficiency

Factors for efficient IT

The energy demands of a data centre remain as high as ever – even after various efficiency measures have been introduced. In the running of a data centre, energy is often by far the most important cost factor. Electronic parts and processors in the data centre produce heat losses – the Thermal Design Power (TDP).

It is on this basis that the cooling for IT systems is designed, yet this also causes a conflict of interests between computing power, costs and climate control systems. In addition to availability and security, energy efficiency is one of the core demands placed on modern data centres.



1 IT server

2 Cooling

3 Power distribution

4 Lighting

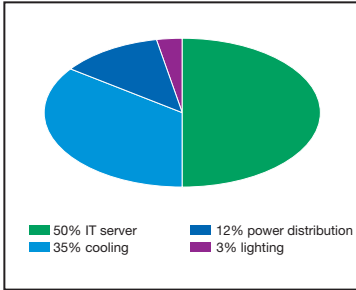
ENCLOSURES

POWER DISTRIBUTION

CLIMATE CONTROL

According to the latest measurements, the overall energy demand is divided as follows: 50% IT server, 35% cooling, 12% power distribution and 3% lighting.

Depending on the location, energy costs can influence the overall operating costs.



Variables affecting the efficient infrastructure of a data centre

- Efficient provision of the required energy
- Efficient heat dissipation from the servers
- Selection of architecture and location
- Scaling options

The higher the waste air temperature, the more energy efficient the cooling systems are. As a result: the higher the temperature difference (waste air/ supply air), the lower the air volume needed to transport the thermal load out of the data centre.

The principle is identical to using water as a cooling medium. The following also applies with liquid-based cooling: the closer to the hotspot (server) that the cooling effect is delivered, the more efficient the process.

The higher the water return temperature, the longer a free cooling system can be used – without a cooling machine.



Low-energy free cooling has a number of uses.

The following should also be considered in terms of efficiency criteria: the modularisation as well as the monitoring and targeted control of the consumers.

As part of an objective ROI assessment, it is important not only to consider the investment costs, but also to analyse the expected operating costs. In addition to personnel costs, priority must also be given to checking and evaluating the energy costs.

The sum of the efficiency criteria of the components, systems and therefore the entire IT infrastructure is critical for the overall level of efficiency of a data centre.

Efficiency in the energy used in data centres

A quantitative evaluation can be obtained in a number of ways.

The favoured approach of the Green Grid organisation uses two values:

- Data Centre Infrastructure Efficiency (DCIE)
- Power Usage Effectiveness (PUE)

Calculation formula for data centre energy efficiency

Data Centre Infrastructure Efficiency (DCIE)

$$\text{DCIE} = \frac{\text{Energy consumption of IT system}}{\text{Total energy consumption of data centre}} \times 100\%$$

Power Usage Effectiveness (PUE)

$$\text{PUE} = \frac{\text{Total energy consumption of data centre}}{\text{Energy consumption of IT system}}$$

Calculation of thermal energy

(heat loss or required cooling power)

$$Q = c \times m \times (T_a - T_z)$$

Q > Thermal energy
(heat/cooling power)

c > Specific thermal coefficient
(air/water)

m > Mass of medium
(air or water)

T_a = Waste air temperature

T_z = Air inlet temperature

The **DCIE** rates the energy efficiency level in the data centre as a percentage.

The often quoted **PUE value** determines the ratio between the power supplied to the data centre and the power consumed by the computers.

A PUE value of 3 is highly inefficient: two-thirds of the power supplied is needed for cooling, with just one third of the power being consumed by the computers. The closer this value is to 1, the more efficient the data centre. For example, PUE values of 1.3 are already outstanding and mean that 30% of the energy is not consumed by the servers or storage systems. The ideal PUE is 1.

PUE = total power consumption of the data centre/power consumed by the IT equipment

- The rule is: the more inefficient the individual components, the worse the energy efficiency of the entire data centre.
- The efficiency of a data centre is significantly affected by the active cooling output of the servers and the heat dissipation from the data centre.
- Among other factors, the temperature difference between the air inlet temperature and the waste air temperature from the server or data centre is relevant for running an efficient IT climate control system.



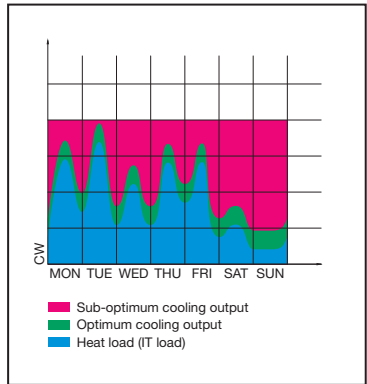
In an economically run data centre, all consumers are optimised for efficiency.

How to increase the efficiency of a data centre

- Replace old servers with new blade servers, virtualisation and server load management
- Optimisation of climate control system through temperature and air volume management
- Use of free cooling systems (using the ambient air for cooling)
- Aisle containment and thereby separating the warm and cold sides in the IT infrastructure
- Need-based management of cooling and distribution
- Cooling using groundwater or geothermal systems
- Alternative generation of electricity, e.g. via a photovoltaic system for private internal data centre consumption
- Holistic view of process using DCIM software (Data Centre Infrastructure Management)
- Choice of location with a higher average annual temperature
- Data centre network: load distribution according to efficiency criteria, including climate, energy costs, capacity

Efficiency example

Like the power consumption of the data centre, the cooling output must be designed for maximum performance in unfavourable ambient temperatures. The week-view graphic shows that without comprehensive management, this generally results in an overdimensioned cooling system.



Regardless of whether free cooling, aisle containment or climate control system optimisation is used, efficiency can be considerably increased in the IT infrastructure.

Monitoring

The information generated by centralised monitoring provides three important steps towards ascertaining the actual energy demand:

- Analysis
- Optimisation
- Control

Measuring the total energy requirement of a data centre in itself often points to potential ways of reducing energy consumption and costs. If the energy demand is adequately considered during the data centre design phase, investment decisions often need to be reconsidered.

For example, a slightly higher investment in energy efficient cooling may pay for itself within a few months.¹⁾

Monitoring, control and documentation using complex software

Monitoring of every system in the data centre is necessary to ensure security and availability. For this reason, a “reliable data centre” must have a Data Centre Management System (DCIM). Guidelines have been published in the IT Infrastructure Library (ITIL) and these apply to all IT organisations.



¹⁾ BITKOM, Energy efficiency in the data centre

Data Centre Infrastructure Management System (DCIM)

To ensure the comprehensive security of a data centre, system-wide monitoring of the entire infrastructure is required, in other words from the server to the climate control, power supply, cabling, fire protection and protection against unauthorised access. Intelligent monitoring systems are needed for this purpose. Sensors in the server racks and the data

centre gather information, such as the temperature, humidity, air velocity and performance of the computer, and pass this data onto the IT administrator via the Data Centre Infrastructure Management System (DCIM). Operation is automatically optimised, partly based on these readings, to increase efficiency.



The administrator can monitor the data centre directly from the monitoring drawer (in image: Rittal 1 U monitor/keyboard unit)



Access authorisation is an element of physical security.

- Power supply and back-up
- Cooling and distribution to the server racks and heat exchangers
- Temperature/humidity in the room and the servers
- Data centre and server rack monitoring
- Security including access authorisation
- Efficiency, energy consumption, energy balance and efficiency of cooling

Linking the data to the central building services management system and monitoring of this data is necessary to ensure optimum and energy-efficient operation of the data centre.

It is important that automatic reports are generated for the IT administrator at predefined intervals. This allows the degree of utilisation, operating costs and efficiency of the data centre to be monitored. Current, monthly and annual energy consumption trends can be derived from this data; operations can be extended to boost productivity and efficiency optimised.

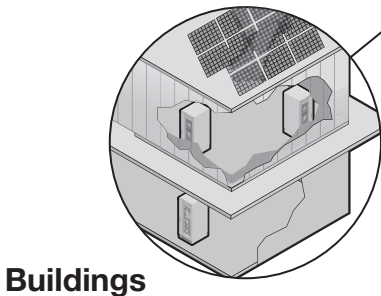
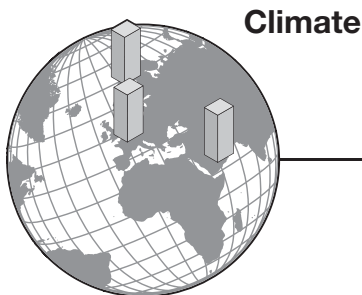
■ Location

Location factors

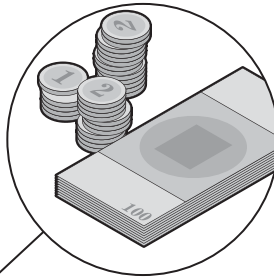
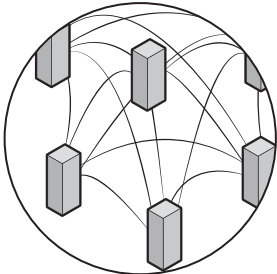
Location evaluation according to infrastructure

Location analysis from the perspectives of security, availability and energy-efficiency plays a crucial role in the planning and design of a new data centre.

- What are the climate conditions at the location, e.g. ambient temperature (comparison of Dubai/Germany/Norway)?
- What is available in terms of infrastructure, i.e. buildings, containers, power supply or alternative sources of energy (photovoltaics)?
- How high are the energy costs at the location and what alternatives are there to cooling?
- How accessible is the location (costs for required infrastructure, getting there, etc.)?
- To what level are skilled workers educated?

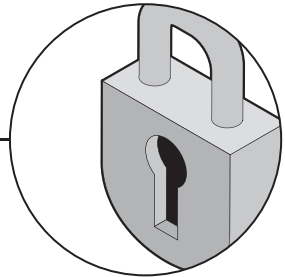


Network connection

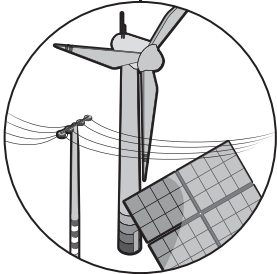


Taxation

**IT
decision
“Location”**



Security



Energy costs



**Skilled workers,
transport links**

IT INFRASTRUCTURE

SOFTWARE & SERVICES



Location factors

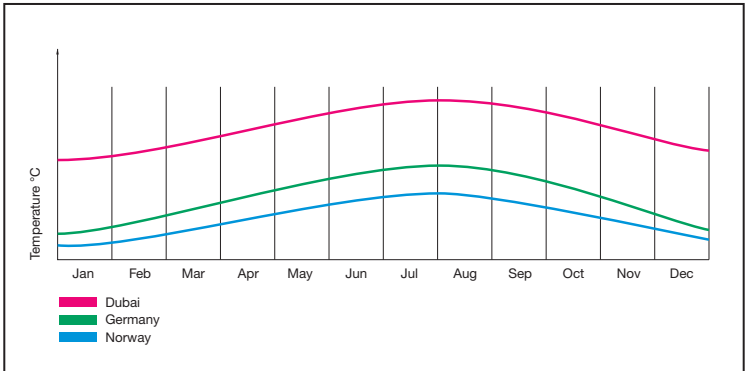
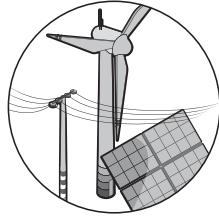
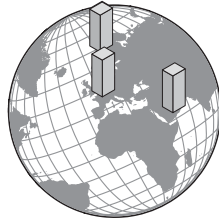
Climate and energy costs

Energy costs for the power supply to the systems and for climate control are decisive factors when choosing the location for a new data centre.

The average ambient temperature over the year (Germany 9.2°C or Norway 5.8°C) can be a key criterion in deciding on the location. With a low average annual temperature, the required air conditioning system can be operated for longer periods of time using free cooling, i.e. without a cooling plant.

Example:

- Norway – average annual temperature + 5.8°C
- Germany – average annual temperature + 9.2°C
- Dubai – average annual temperature + 27.4°C

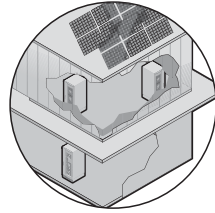


Comparison of average annual temperatures in Germany, Norway and Dubai

Location factors

Buildings, accessibility, skilled workers

- Position of the data centre in the building
 - Sunlight
 - Security
 - Power supply connection
- Costs of accessibility for infrastructure and server adjustments, maintenance, system failure, etc.
- Availability of qualified staff
- Expandability and therefore long-term future security



Increasingly complex IT systems and applications cannot be safely operated without qualified staff.

Location factors

Network connection, taxation and security

A risk assessment of the location must also be carried out. Potential risks are:

Network connection

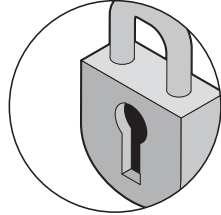
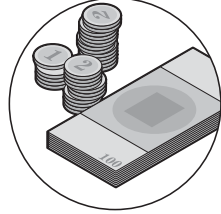
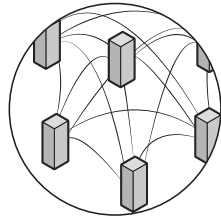
- Connection of Internet nodes

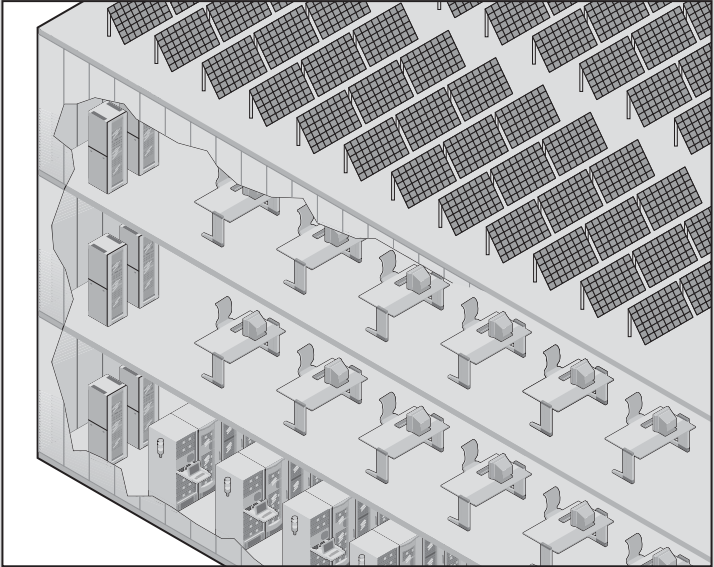
Taxation

- Regional taxes (e.g. trade tax) and charges

Security

- Natural disasters, e.g. risk of flooding or earthquakes
- Situation on the roads, e.g. routes for transporting dangerous goods
- Distance from airports (flight approach paths)
- Political stability and legal position
- Proximity to plants or equipment that pose a fire risk, e.g. power stations, chemical plants, pipelines
- Electromagnetically active sources, e.g. transformers, transformer stations, transmitting equipment and railway lines
- Secure access and protection against vandalism



Example of location factors in context

The example application considers a service company with 200 employees and a data centre capacity of 200 kW. The company's employees use software-based processes and tools. Digital data is therefore permanently stored and backed up. Some customers request data to be archived for up to 10 years, so the current volume of data amounts to 40 terabytes. The working hours of the employees are Monday to Friday from 6 a.m. to 8 p.m., which favours the use of renewable energy.

Climate and energy costs

Server in cool cellar, air conditioning system on the north side, energy input for air conditioning and computers correlates to output of the photovoltaic plant in the course of the day, purchased energy has been reduced by 90%

Buildings and accessibility

Central location, secure access to basement. Good transport links.

Network connection, taxation and security

High network costs for the dedicated line, low trade tax. Secure rural surroundings.

■ The future

Options for future IT infrastructures

New usage models, technology concepts and a different understanding of how data centre services must be made available to operators all influence the future developments and infrastructure of a data centre. A poor investment decision made today can be costly in the future.



Secure and protected data centres will also become more common in the future.

Operational reliability and energy efficiency are at the top of the priority list and are complex subjects. They range from optimised operating models, to energy saving cooling options and the use of efficient components in server power supplies. Improvements take place at all levels, from the microarchitecture of the server to the choice of location for the data centre.

DC power supply

Current developments demonstrate a marked trend towards using servers powered by a DC power supply with the aim of reducing energy consumption. Server manufacturer Hewlett-Packard estimates that the centralised distribution of direct current is up to 10% more efficient than alternating current. If the server is supplied directly with DC voltage, acquisition costs could be reduced by up to 15% and the physical space for the server by up to 25%.

New electronic components

A further development for servers other than the 19" format can also be expected. One way of achieving this is to encapsulate motherboards completely and allow them to be surrounded by a non-conductive coolant. Newer processors, for example those that have three-dimensional transistors, exhibit a constantly lower TDP (Thermal Design Power) in terms of power consumption.

Power density

Efficient solutions are required for process-intensive applications, such as cloud-based applications, the use of "Big Data" and the trend towards high resolution images and films (High Definition, Ultra High Definition). The IT infrastructure can offer an intelligent solution to the conflicting demands of performance, availability and efficiency.

Approaches include IT clusters in special environments; for example, disused tunnels in Scandinavia using sea water for cooling and the use of renewable energy.

Modular design

As a result of standardisation, even more data centres will in the future be constructed on a modular basis. This principle enables a data centre to be continuously expanded in line with the required computing power demands – scalable from 20 kW to 450 kW – using prefabricated modules for server and network enclosures, the air conditioning system and the power supply. This modular approach actively contributes to a reduction in investment and maintenance costs.

Climate conditions

There has also been a change in relation to the climatic conditions within a data centre. The ASHRAE association has relaxed the permissible benchmark data for operating data centres. Today, ambient temperatures of up to 40°C in the data centre are allowed. This temperature and humidity range enables outside air to be used for cooling, i.e. free cooling either indirectly using cooling water or directly using filtered outside air.

Data centres in Northern Europe can therefore be cooled with outside air, except for a few days a year. When deciding on a location, it is worthwhile analysing what conditions the outside temperatures offer for free cooling and thus for energy-efficient operation.



Specifically defined IT infrastructures enable future-proof data centres with a computing power demand of up to 450 kW to be built.

Rittal – The System.

Faster – better – everywhere.



ENCLOSURES

POWER DISTRIBUTION

CLIMATE CONTROL

System components for IT infrastructures

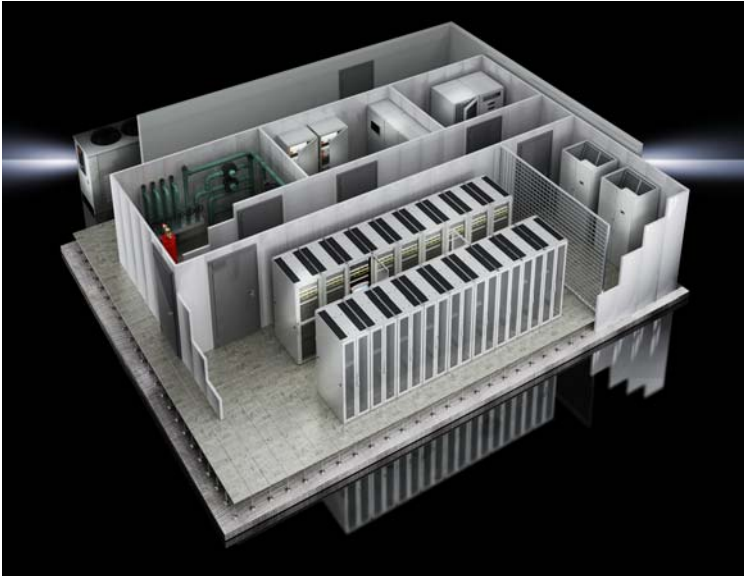
	Page
IT racks	66
Configuration and frame	68
Use in industrial environments	69
Ventilation and heat management	70
Access protection	71
Cable management	71
Panels	72
Operational reliability	72
General accessories	73
IT power	74
Power distribution components	74
UPS system components	77
Power management system components	79
IT cooling	80
Decision-making criteria and cooling variants	81
Overview of the systems	82
IT climate control solutions	83
Cooling	86
IT monitoring	88
Monitoring system components	88
IT security	90
Security components for the rack and room	90
Fire protection	92

■ IT racks

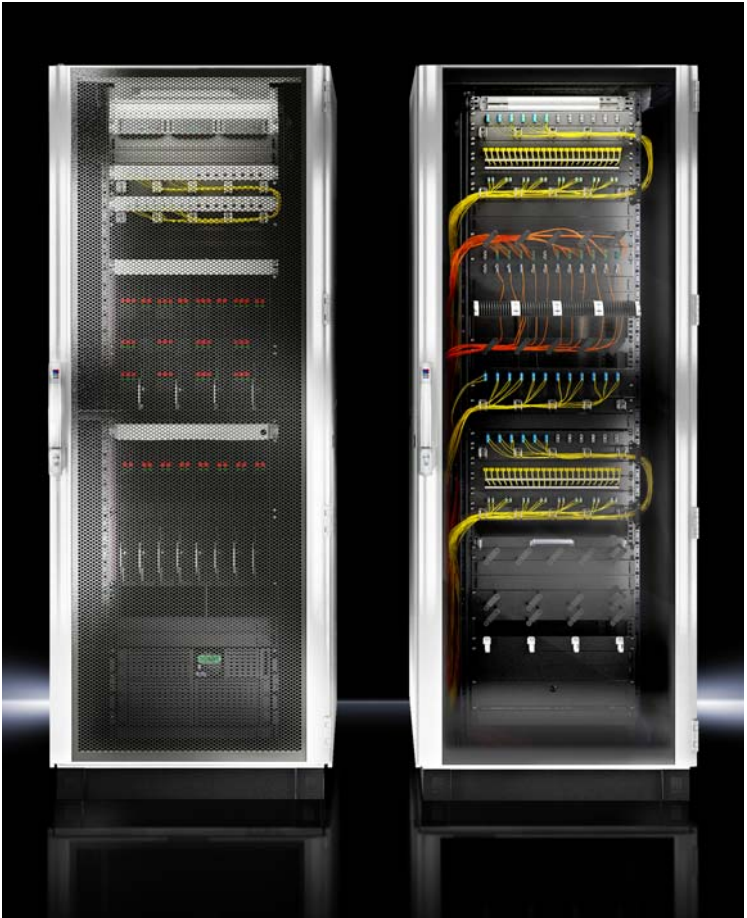
The performance of any IT infrastructure is reliant upon interaction between individual components. Today, IT rack systems play a key role with respect to the availability, reliability and Total Cost of Ownership (TCO) of the IT infrastructure. Suitable server racks have a system platform in which the climate control, power and security solutions are perfectly coordinated with one another, and the space available is optimised. The key criteria are:

- Maximum packing density
- Efficient space utilisation
- Adaptability

Modern IT racks can be flexibly arranged, have a positive influence on TCO, and help to cut the ongoing operating costs of each rack.



Schematic layout of the data centre model



At the heart of the rack-optimised design is the tried and tested TS 8 server and network platform, which has been improved further in the latest TS IT rack from Rittal.

Configuration and frame

Modern generations of servers and network equipment are designed in such a way that the density within a rack unit is continuously increasing. The typical power density today ranges between 3 – 5 kW, but in high-performance applications it can be 12 – 40 kW per rack. A secure server rack is scalable and can accommodate 19" components. To guarantee optimum space utilisation, racks with excess heights, such as 47 rack units (2,200 mm), are supplied. Depth-variable 19" profiles permit the individual configuration of heterogeneous server architectures. In addition to height, the depth is also greater. Rack depths of 1,000 to 1,200 mm are necessary today to house large servers.

Due to installed components with side ventilation, such as Core Switches, widths of 800 mm and over are also common. This ensures manufacturer specifications of free space for air flow and cabling are fulfilled.

A high load capacity of up to 1,500 kg is required to allow for the large number of servers, cables, power distribution units and points of contact for housings, or the use of heavy blade servers. Server racks and network enclosures are used both as stand-alone and bayed solutions. For this reason, the racks should be scalable, flexible and able to be bayed.



Interior design

A symmetrical frame design ensures maximum useful rack volume and permits scalable baying options for optimised space utilisation at all levels. An intelligent modular system, comprising of a range of racks and

accessories, provides an easy design to assemble, reduces the complexity associated with accessories and results in cost savings. It is important that an IT rack can be easily modified to meet the future requirements of the IT equipment.

Use in industrial environments

Typically, the degree of protection (International Protection Marking or IP code) in the data centre does not form part of the decision-making criteria. Through the convergence of industry and IT, more and more IT applications are being directly integrated into the industrial environment. For example, to ensure optimum surface protection

and enhanced corrosion protection, electrophoretic dipcoat priming and nano technology – which were developed for automotive engineering – are used. At the same time, there are IT racks with an industrial-quality degree of protection IP 55.



Ventilation and heat management



Another basic function of a server rack is to provide a flexible heat dissipation solution and precision climate control system. Reliable operation is put at risk without sufficient active or passive heat management. As packing density increases, so does energy efficiency. At the same time, demands on power distribution and heat management rise. More supply and data cables make heat removal and access to equipment difficult.

To allow air to circulate freely, the doors should have a high degree of perforation. Normally, perforation of 60 to 80% is provided. If hot and cold aisles are completely separated, trim panels and air baffles are also required.

Access protection



In addition to mechanical and heat technology properties, protection against unauthorised access to the IT rack must be ensured using intelligent locking and security systems. For example, the highest level of access protection is offered by 4 point locking systems, which can also be fitted with electronic access controls.

Cable management



Intelligent cable management – internal or external – helps with various cabling requirements; from sandwich cable routing, optical fibre cable routing, including safeguarding bending radii, and storing excess cable lengths in the rack. Inside the rack, cables should be arranged and laid in a logical way in order that equipment and cables can be easily and quickly accessed. Suitable cable routing systems reduce crosstalk during transmission of signals and protect the cable from damage. Cables are increasingly fed in from above via an opening in the roof plate or sometimes still via the base/plinth or raised floor.

Panels



A high level of flexibility for individual requirements provides you with a choice, such as glazed doors, roof plates with cable entry and divided side panels. For example, the side panels may not be screwed together, but can be assembled without using a tool with snap-on fixings. Lockable rack doors and side panels protect the server and data from unauthorised access. Depending on the level of security, different locking systems are available, e.g. with a key or combination lock, or an electronic or biometric locking mechanism.

Operational reliability



International standards, patents and certifications for server racks ensure their use worldwide. The most up-to-date earthing and equipotential bonding concepts, as well as optional EMC versions, secure high levels of operational reliability. In modern racks, automatic equipotential bonding is achieved directly by the locking device of the 19" level (see TS IT from Rittal image).

General accessories

The individual design is also simplified by unique accessories.

Here are some examples:

- **Base/plinth, underfloor frame, base mounting, castors and stabiliser**

Various components are available for flexible base mounting, cable entry and raised floor mounting. This enables individual system prerequisites to be implemented quickly and easily. An intelligent stabiliser increases security and heavy-duty transport castors also mean fully configured racks remain mobile and flexible.

- **19" component shelves**

Whether depth-variable, static or heavy-duty shelves for loads up to 150 kg – the comprehensive product range makes hardware integration easier. Slotted shelves ensure optimum vertical air flow.

- **Drawers**

Integrated multifunctional drawers that can be locked provide space to keep keyboards, documents or cables clean.

- **Server integration**

Stay flexible even with varying server architecture within a rack. With depth-variable slide and heavy-duty rails suitable for loads up to 150 kg and flexible universal mounting rails for the installation of heterogeneous server architectures using manufacturer-specific mounting kits.

In summary, the criteria for a secure server rack or network enclosure are:

- Stability and load capacity
- Ease of mounting and wide range of accessories
- Flexible design and ability to enlarge
- Integration of heat dissipation
- Cabling options in the rack
- Space for power supply
- Security, e.g. protection against unauthorised access
- Fire prevention
- Certifications and availability



■ IT power

Power distribution components

Power distribution requires maximum security of supply and consistently high levels of transparency. In addition, a low fire load and low level of interference from electromagnetic fields are important for reliable IT operation. The following areas are relevant for power supply and back-up:

- Depending on the demand for availability, one or more independent infeeds
- Transparent sub-distribution with clear power structure between main and sub-distribution
- Power back-up provided by UPS (uninterruptible power supply) systems
- DC circuit back-up using batteries and alternative power sources, such as photovoltaics or wind power
- Ability to switch the IT load on and off using intelligent socket systems



Power distribution from the power source to all IT equipment and back-up provided by UPS concepts

¹⁾ Rittal Energy Management, pages 22/23

Example of a solution from Rittal and Siemens:

- LD busbar trunking system as power backbone, can also be used in redundant configurations
- BD2 busbar trunking system as a stub line in the under floor base or above the racks for a direct supply
- Networked connection via panel boxes and parallel-routed standard bus system

Low-voltage distribution centre



- Structured system solution for the fast and safe configuration of low-voltage switchgear systems
- Type-approved connection of the Sivacon 8PS busbar trunking systems (LD system) to Ri4Power
- Scalable data centre applications, expandable on a modular basis, e.g. with the LD system

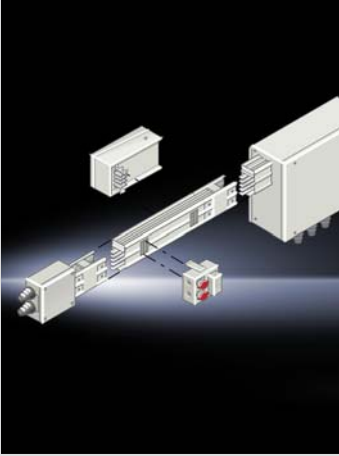
Data centre backbone



- Quick and safe planning and installation
- Clear power structure between main and sub-distribution in data centre
- Compact design for many data centre application areas, frame sizes of 1,000 A, 1,600 A and 2,000 A
- High level of availability thanks to simple sub-distribution connection (BD2 system)

Example of a solution from Rittal and Siemens:

Sub-distribution



- For example, using the BD2 system
- Complete transparency of power distribution in the rack suites
- High security of supply and automatic consumption monitoring
- High level of scalability
- High level of protection against unauthorised access through sealable outlet points
- Flexible adaptation to all data centre structures through 3D change in direction (250 A, 400 A, 630 A)

Socket systems

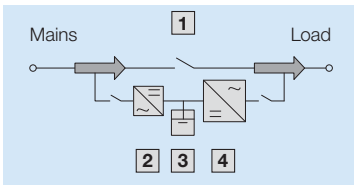


- For example, using PDU systems (Power Distribution Unit)
- Easy to connect the PDU to the tap-off units of the BD2 system (CE connector)
- Passive PDU without monitoring or management function
- Metered PDU with current and power measurement by phase (power supply)
- Switched PDU with additional switching of the connection
- Managed PDU with current measurement for each individual connection

UPS system components

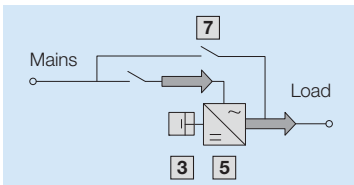
- Rectifier – converts current from the supply network (alternating or three-phase current) into direct current
- DC link – used to charge the battery of the UPS. In the event of a power failure, the DC link is supplied with power from the battery.
- Energy storage device – e.g. battery or fuel cell
- Inverter – converts the power provided by the DC link into AC voltage
- Static bypass – activated if the inverter is not working, e.g. in the event of overloading or an inverter, rectifier or battery fault

Due to the varying requirements of the individual devices, three UPS classes have become established. These are defined in the International Engineering Consortium's (IEC) product standard IEC 62040-3 and the European Union's standard EN 50 091-3 – arranged in terms of increasing security:



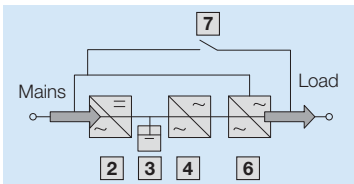
Offline UPS system

Normal operation without interference



Line-interactive UPS system

Normal operation via a four quadrant inverter [5]



Online UPS system

Normal operation via a rectifier [2] and inverter [4]

- | | |
|----------------------|----------------------------|
| [1] Switch | [5] Four quadrant inverter |
| [2] Rectifier/loader | [6] Static bypass switch |
| [3] Battery | [7] Manual bypass switch |
| [4] Inverter | |

Offline UPS

- UPS class 3 according to IEC 62 040-3.2.20
- The IT equipment to be supplied is connected directly to the available power supply
- An overvoltage or undervoltage is detected by the offline UPS and a switchover to battery operation takes place
- Time taken to switch from mains operation to battery operation from 4 to 10 ms
- Undervoltages and overvoltages are not compensated for
- Efficiency of approx. 95%

Network-interactive UPS or line-interactive UPS

- UPS class 2 according to IEC 62 040-3.2.18
- The UPS system is switched between network connection and the IT equipment to be supplied
- Electronic filters compensate for voltage fluctuations
- Battery unit is directly connected
- Time taken to switch from mains operation to battery operation from 2 to 4 ms, switched instantaneously in the reverse direction
- Efficiency of between 95 and 98%

Online or continuous converter UPS

- UPS class 1 according to IEC 62 040-3.2.16
- Generation of its own line voltage
- Connected consumers are continuously supplied with line voltage
- At the same time, the battery is charged irrespective of any voltage fluctuations
- High-quality sinusoidal voltage on the output
- With galvanic isolation or isolation transformers, interference is filtered by the neutral conductor
- Efficiency of approx. 90%, as voltage is converted by the static bypass, and power loss and heat loss occur

Security can be enhanced if UPS systems are equipped with additional redundancy and are duplicated. The parallel use of several UPS systems is worthwhile if large systems are being operated on the load side. Load management then connects or disconnects individual UPS systems.

Power management system components

A Power Management System ensures transparency of energy consumption and quality in the data centre and the availability of power distribution. Power management can be a part of the Data Centre Management System (DCIM, see also page 54). At the same time, it is the basis for optimising energy costs and consumption.

The functions

- Visualisation and analysis of energy data/flows
- Presentation of interdependencies
- Determination of savings potential – interpreted minimum and maximum values
- Energy measurements for calculation purposes
- Internal (rack line/part of building) or external (rooms/systems) comparison
- Preparation of decisions, e.g. for expansions of the power supply
- Verifiable efficiency improvements
- Targeted fault rectification through quick and detailed event and interference information
- Logging of fault and event information
- Fulfilling supply contracts through targeted control of consumers
- Automatic notification of service staff



■ IT cooling

The operational reliability and availability of IT depends substantially on the heat dissipation from the server rack or data centre. Heat problems in data centres can only be avoided through the implementation of modular climate control concepts. Due consideration must be given to parameters such as temperature, humidity, the velocity and pressure of air flows, as well as the heat losses of the installed components. An energy efficient and advanced climate control and cooling concept for data centres takes into account the needs and peripheral conditions.

A distinction is made between:

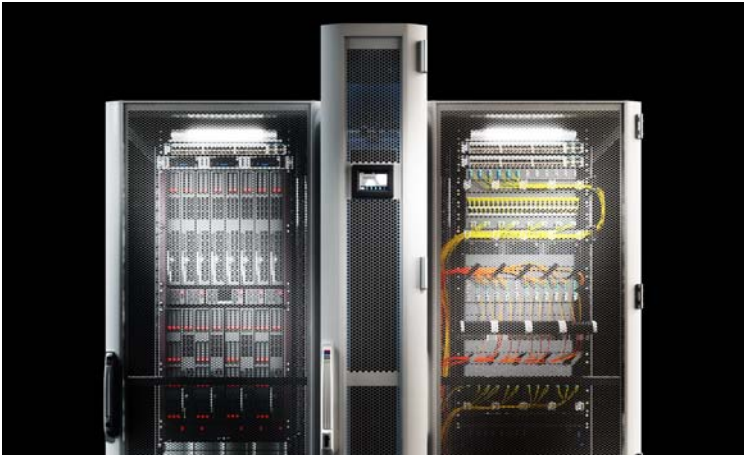
- ventilation systems (climate suitable for humans)
- air-conditioning systems for heat dissipation (IT cooling)

The heat load inside a data centre is caused by:

- Office lights, sunlight and other heat sources. This heat load is dissipated to the atmosphere by the air-conditioning system.
- IT equipment, e.g. servers. This heat load is dissipated by the IT cooling system.

When cooling active IT components, a distinction is made between:

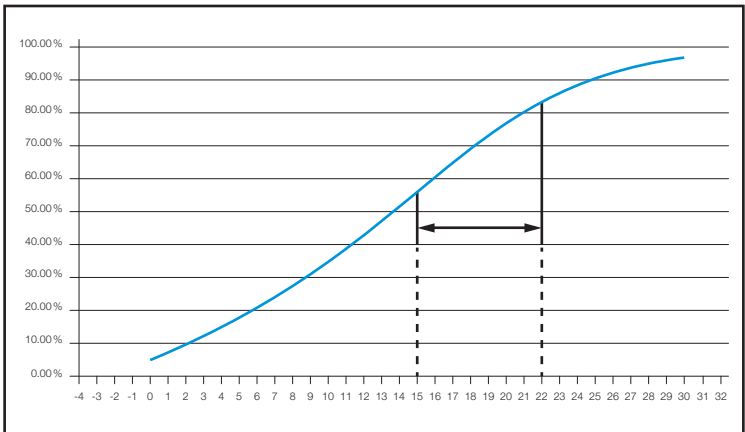
- Passive cooling (use of the ambient air)
- Active, rack-specific cooling
- High-performance cooling for the temperature-neutral expansion of the data centre



Decision-making criteria and cooling variants

The design of a climate control concept according to specific needs and application requirements, while giving due regard to all ambient conditions, means that several fundamental questions have to be answered. Software tools assist during the planning phase:

- What type of cooling system should be installed, e.g. hybrid solution, passive cooling, integrated hot aisle?
- How is the installation to be configured in terms of hot and cold aisles?
- What average temperatures should be maintained in the racks?
- How great is the temperature differential, return/flow temperature, ΔT ?
- What type of volumetric flow is required?
- What are the ambient conditions?
- Which flow direction has been selected and does the installation situation have any special features?
- What load fluctuations exist and what impact do these have on the cooling response times?
- How is the system to be dimensioned, taking future requirements into account?



According to the “2008 ASHRAE Environmental Guidelines for Datacom Equipment”, the air intake temperature for such equipment should be between 18°C and 27°C. Thanks to correct dimension of the heat exchanger, the free cooling limit temperature can come to within approx. 1.5 K of the permitted ASHRAE conditions.

Overview of the systems

■ Room cooling

Supply of cold intake air and dissipation of warm waste air.

■ Closed-circuit air-conditioning

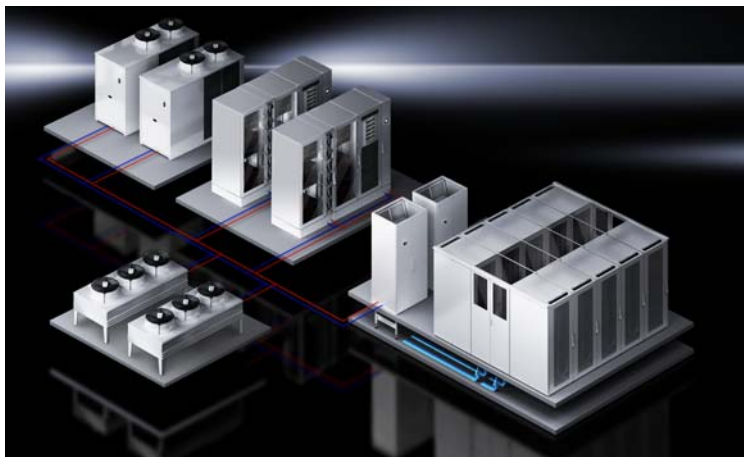
Intake air in the data centre is cooled in a heat exchanger. The heat exchanger is cooled using a refrigerant or water.

■ Server-rack cooling

For high loads > 20 kW heat loss, the heat exchangers in the rack are cooled directly using cooling water or a refrigerant.

The energy-efficient IT climate control system takes account of:

- Dimensioning of the cooling systems according to the actual power requirements
- Separation of cooling for server racks and room air-conditioning by partitioning of aisles
- Use of energy-efficient components, e.g. electronically commutated fans including power regulation of the cooling compressors
- Use of free cooling or adsorption cooling systems in conjunction with solar power
- Keeping the cooling water and room temperatures as high as possible
- Controlling all subsystems and continuous adaptation to the actual cooling power requirements



IT climate control solutions

Depending on the thermal output in the data centre, we differentiate between the following climate control solutions.

Raised-floor climate control

A traditional raised-floor climate control system is frequently used if the heat loss inside the rack is less than approx. 8 kW. The cold supply air is fed into the data centre via a perforated raised-floor in front of the server racks. Warm waste air is usually extracted via waste air ducts attached to the ceiling and cooled through a

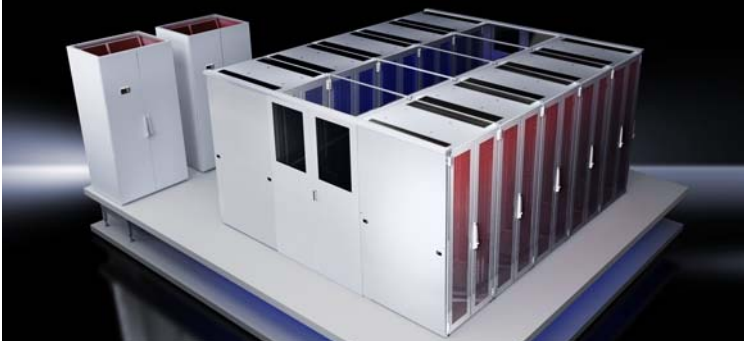
heat exchanger in the air recirculation unit with water or refrigerant. During this process, an air exchange containing approximately 10% external air is constantly being fed in to improve the quality of the recirculating air. The disadvantage of raised-floor climate control is that the supply air and waste air are mixed, which reduces the effectiveness of the cooling.



Raised-floor climate control with aisle containment

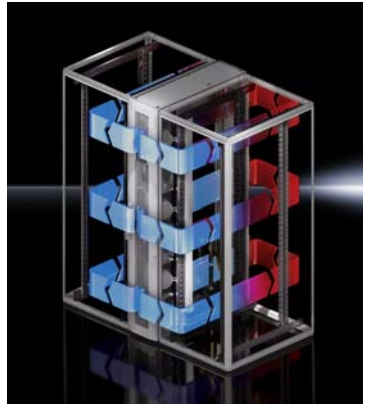
To improve the efficiency of the raised-floor climate control system, the cold or warm aisles can be enclosed.

Adopting this approach eliminates the mixing of the supply air and waste air. The server racks can be supplied with cold supply air in a more targeted manner and overall energy efficiency levels are increased.



Suite cooling

If the required cooling output exceeds approx. 10 kW, a raised-floor climate control system will in most cases not be adequate. In such cases climate control solutions are integrated directly into the racks and provide cool air flows via the raised floor. This reduces the loading on a raised-floor climate control system with aisle containment. In situations where there is a very high demand for cooling power, they handle all the heat dissipation from the racks. With this solution, the heat in an air/water or air/refrigerant heat exchanger is transferred to a fluid medium (water or refrigerant) and dissipated.

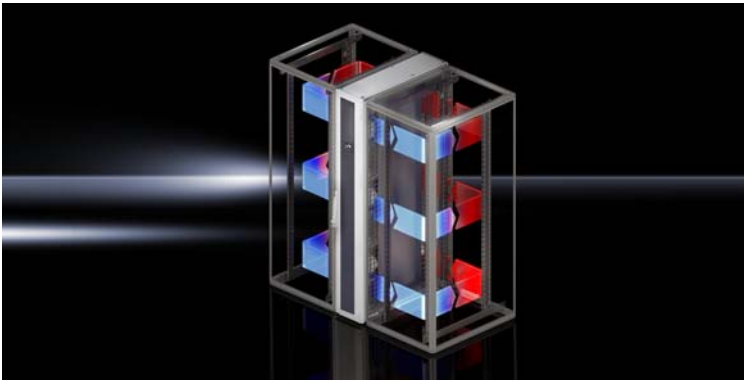


Rack-based cooling

In the case of heat loads, e.g. for high performance computing, of > 20 kW per rack, rack-based cooling is the most cost-effective and technically appropriate solution. A distinction is made between active and passive rack-based cooling. The main point is to ensure that the cooling system is as close as possible to the location where the heat is generated. High-performance cooling systems can dissipate up to 60 kW of heat load per rack. The complete system is partitioned. The hot air does not enter the normal air circulation circuit, but is extracted directly from the rear of the servers by water-cooled heat exchangers, which cool it before blowing it in again at the front.

Active rack-based cooling requires a cold water infrastructure in the vicinity of the enclosures. The water for the heat exchangers in rack-based cooling systems is usually treated and cooled centrally.

Energy-efficient, high-performance climate control can also be implemented without any fans. Air routing in the server systems with integrated high-performance fans is nowadays extremely efficient. Up to approx. 20 kW (e.g. LCP Hybrid from Rittal), passive rear doors in the racks are sufficient, as the powerful blade server fans are able to force adequate volumes of air into the heat exchangers. For maximum performance requirements, however, there is no real alternative to rack-based systems. Should the application demand even more output or increased redundancy, rack-based cooling systems can also provide mutual support. If the modules are positioned alternately between the server enclosures, they blow cold air at the front out in both directions, and thus supply the server enclosures from two sides. If redundancy is a major consideration, the cooling modules should be connected alternately to two different water circuits.



Cooling

Whether air, water or a refrigerant is used – all these heat transfer media have to be cooled. The heat transfer medium is directly or indirectly cooled in the recooling systems or the chillers. Free cooling is being used more and more frequently for treating the cold water. In modern systems, the free cooling limit temperature can actually extend up to within 1.5 K of

the desired water flow temperature. In other situations, more expensive chiller systems are used. The admissible server supply air temperatures have been raised by ASHRAE to 27°C, which means that water flow temperatures of 20°C are possible.

There are three different free cooling methods:

Indirect free cooling

The heat load of the data centre is transferred via an air flow over an air/water heat exchanger in an air recirculation unit to a water/glycol medium. This medium is then cooled outside the building in a recooler using external air.

Direct free cooling

The direct free cooling method feeds the heat load from the data centre directly out to the atmosphere. The supply air is mixed proportionally with waste air according to the external temperature and warmed until it reaches the required temperature. Only when external temperatures are high will cooling to the desired room temperature in recirculation mode with the help of refrigerant cycles be necessary.



Other free cooling concepts

One method is adiabatic cooling. Here, the air flow in an indoor air unit is moistened and hence cooled. Cooling without free cooling, e.g. by opening the window, is still used today but is inefficient. This is because all the outside air coming into the building has to be cooled in the summer and heated in the winter, which increases energy costs dramatically.

Conclusion

The energy-efficient climate control of a data centre is solved in a technically optimum manner with due regard for the specific conditions within the building, economic factors and availability requirements. The most suitable climate control solution is tailored to the permissible downtime per year. The BITKOM matrix for reliable data centre operation offers the following recommendations.

Data centre category	Climate control ¹⁾			Permissible data centre downtime
	Server enclosure	Server enclosure	Data centre/server room	
	Up to 7 kW	From 7 kW to 40 kW	500 up to 2500 Watt/m ²	
A	Climate control required, redundancy optional	Climate control required, redundancy required, UPS support	Precision cooling, redundancy, separation of cold/warm aisles, UPS support if necessary	12 hrs
B	Climate control required, redundancy required	Climate control required, redundancy required, UPS support	Precision cooling, redundancy, separation of cold/warm aisles, UPS support	1 hr
C	Climate control required, redundancy required, UPS support	Climate control required, redundancy required, UPS support	Precision cooling, equipment and conduits redundant, separation of cold/warm aisles, UPS support	10 mins
D	Climate control required, complete redundancy required, UPS support	Climate control required, complete redundancy required, UPS support	Precision cooling, equipment and conduits redundant, separation of cold/warm aisles, UPS support, emergency cooling system using additional climate control system	< 1 min

From this it may be concluded that the higher the requirements placed on the availability of an IT climate control system, the higher the investment necessary to meet them.

¹⁾ BITKOM, Reliable Data Centre



■ IT monitoring

Monitoring system components

For most companies, the defined availability of their IT services is the most important prerequisite for reliable and controlled business processes. The security of the physical IT infrastructure begins with each individual rack. The monitoring concept provides preventive protection to guard against consequential costs and simultaneously serves as the central organisational unit for linking to facility management.

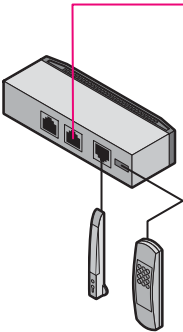
Error and alarm messages are sent to defined service or security management systems. Data exchange via bus systems and integration into LAN and facility management systems ensure the transparency of all security-relevant data.

The modular design principle of components can be tailored to the defined requirements and expanded through the use of a range of sensors and actuators. As monitoring incorporates various different aspects and can be integrated into central facility management systems, it becomes the central point of information in the data centre.

CMC III Processing Unit Compact

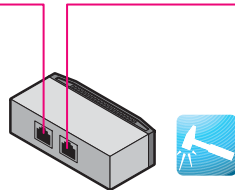
CMC III CAN bus access

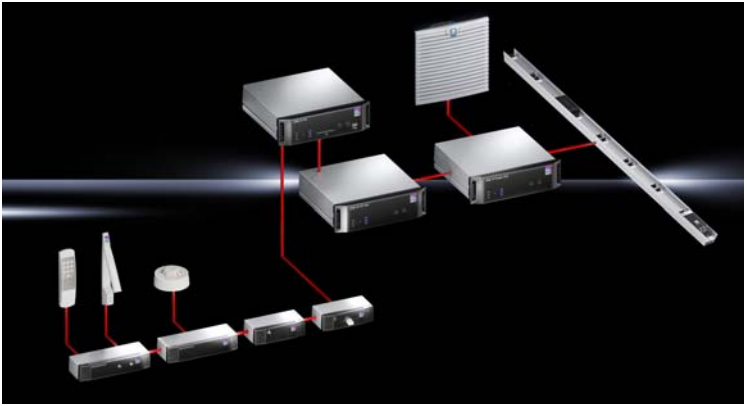
with integrated IR access sensor



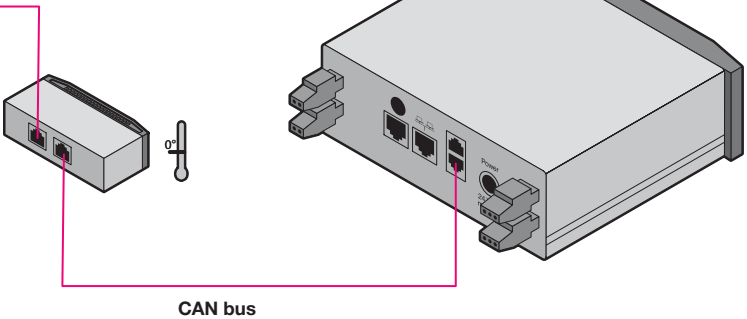
CMC III sensors

for direct connection





CMC III sensors
for direct connection



■ IT security

Security components for the rack and room

Optimal physical year-round monitoring is only possible with a large outlay on staff; not a cost-effective option for the normal operation of a server rack or data centre. At the same time, protection against unauthorised access is required. An optimal security concept implies a multidimensional approach that covers access to the server rack and the data centre.



ENCLOSURES

POWER DISTRIBUTION

CLIMATE CONTROL

Requirements of a security concept for a data centre

- Access control by
 - installing a digital locking system in the server rack and data centre
 - using an authorisation concept to access the data centre
 - installing an intruder alarm system in the data centre connected to a security service or the police
- IT infrastructure control by
 - installing monitoring sensors and video technology in the rack and data centre
 - using early fire detection and extinguishing technology
- Climate control by
 - using temperature sensors and sensor technology to measure ambient conditions
- Administration control by
 - segmenting racks and network topologies
 - installing KVM functions and switches (keyboard-video-mouse)
 - integrating a monitor unit (monitor-keyboard-drawer)

Together with security-relevant parameters, this enables all supply channels used for power back-up, cooling generation and distribution to be centrally monitored and visualised.



Fire protection

Structural fire protection measures

Reliable fire protection is another prerequisite for secure data centre operation. When designing or expanding a data centre, suitable extinguishing technology should be considered. In addition to providing protection, fire protection is designed to use various devices to detect fires within a server rack and data centre early and extinguish them. Fire, smoke and aggressive gases always pose a risk for IT, thus automatic fire extinguishing systems or oxygen reduction systems that use gaseous media are recognised solutions.

When considering fire protection measures, all the required regulations, guidelines and protection targets should be observed, in order that the data centre can then be certified in accordance with EN 1047-2.

Data centre category	Technical fire protection ¹⁾			Permissible data centre downtime
	Server enclosure		Data centre/server room	
	Up to 7 kW	From 7 kW to 40 kW	500 to 2500 W/m ²	
A	Monitoring unit with early fire detection and extinguishing technology (with a reserve of passive extinguishing medium)	Fire alarm system, monitoring unit with early fire detection and independent extinguishing technology (with a reserve of passive extinguishing medium) or oxygen reduction system (fire prevention system)	12 hrs	
B	Monitoring unit with early fire detection and extinguishing technology (with a reserve of passive extinguishing medium)	Fire alarm system, monitoring unit with early fire detection and independent extinguishing technology (with a reserve of passive extinguishing medium) or oxygen reduction system (fire prevention system)	1 hr	
C	Fire alarm system, monitoring unit with early fire detection and independent extinguishing technology (fire extinguishing system) or oxygen reduction system (fire prevention system) in a redundant design		10 mins	
D	Fire alarm system, monitoring unit with early fire detection and independent extinguishing technology (fire extinguishing system) or oxygen reduction system (fire prevention system) in a redundant design		< 1 min	

¹⁾ BITKOM, Reliable Data Centre

The European standard stipulates the structural requirements and the strictly defined flame impingement times in the event of a fire. Structural fire protection must be considered in addition to technical fire protection.

Organisational fire protection measures

Along with technical and structural fire protection, organisational fire protection must also be implemented. Current conditions and future developments are also relevant to these considerations.

Organisational fire protection includes the following: an emergency plan, an IT restart plan, fire regulations, a fire brigade plan, an emergency exit plan, signage, a smoking ban, a foodstuffs ban, company and staff induction, security officers, visitor regulations and staff instruction.

Data centre category	Structural fire protection ¹⁾			Permissible data centre downtime
	Server enclosure		Data centre/ server room	
	Up to 7 kW	From 7 kW to 40 kW	500 to 2500 W/m ²	
A	Walls, floor, ceiling: Fire-resistance class of at least F90, protection against flue gas and water spray, door fire-resistance class of at least T90, cable bushing with the same protection value	Walls, floor, ceiling: Fire-resistance class of at least F90, protection against flue gas and water for 30 mins, door fire-resistance class of at least T90, cable bushing with the same protection value		12 hrs
B	System performance test of the structural fire protection walls, floor, ceiling: in accordance with European standard EN 1047-2, cable bushing with the same protection value, protection against flue gas and water spray for 60 mins	System performance test of the structural fire protection walls, floor, ceiling: in accordance with European standard EN 1047-2, cable bushing with the same protection value, protection against flue gas and water spray for 60 mins		1 hr
C	System performance test of the structural fire protection walls, floor, ceiling: in accordance with European standard EN 1047-2, cable bushing with the same protection value, protection against flue gas and water spray for 60 mins	System performance test of the structural fire protection walls, floor, ceiling: in accordance with European standard EN 1047-2, cable bushing with the same protection value, protection against flue gas and water spray for 60 mins		10 mins
D	System performance test of the structural fire protection walls, floor, ceiling: in accordance with European standard EN 1047-2, cable bushing with the same protection value, protection against flue gas and water spray for 60 mins			< 1 min

¹⁾ BITKOM, Reliable Data Centre

Rittal – The System.

Faster – better – everywhere.



ENCLOSURES

POWER DISTRIBUTION

CLIMATE CONTROL

Solutions for IT infrastructures

	Page
RiMatrix S, RiMatrix	96
Engineering & consulting	98
Commissioning, service and support	99
RiMatrix S	100
The first “turnkey data centre”	100
Scalable up to 450 kW	101
System accessories	
Rack/cooling	102
Power	103
Cooling	104
Monitoring	105
Security with RiMatrix S	106
Flexibility with RiMatrix S	107
RiMatrix	108
The modular system for standardised components	108
System accessories	
Rack	108
Power	108
Cooling	109
Monitoring	109

Rittal – The System.

Faster – better – everywhere.

IT infrastructures

At first glance, the construction or modernisation of a data centre appears to be a mammoth project.

A secure, available and energy efficient IT infrastructure benefits the company as a whole. Even during the preparation and analysis phases, potential can be identified and complex challenges can be used intelligently. The result: a rapid return on investment (ROI) through individual, standards-based solutions.

Consultancy

In order to technically implement a data centre, IT consultants are guided by the expectations of the customer.

For this purpose, the entire process chain is considered:

- Consultancy
- Quote preparation, ROI calculation
- Order handling
- Logistics, delivery, commissioning
- Full documentation
- Acceptance, certification
- Administration
- Extensions, changes
- Maintenance, spare parts
- Service, hotline

For the end customer, a functioning and perfectly coordinated process chain is a key factor in the success of the solution.

The RiMatrix S standardised data centre

RiMatrix S (S = standardised) represents the **construction of a standardised data centre** in an existing building, in a security room and also as a container solution. Rittal offers **predefined modules for data centres** with a cooling output of 450 kW.



Benefits:

- Low investment costs
- Short delivery and commissioning times
- PUE (Power Usage Effectiveness) 1.5 to 1.15
- Full documentation including tested characteristic curves and data sheets
- Simplified final certification of the reliable data centre
- Easy to extend and ready to meet future challenges

The RiMatrix customised data centre

In 2005, Rittal launched RiMatrix – the complete solution for **constructing customised data centres**. RiMatrix comprises series-produced solutions from the rack, power, cooling, monitoring and remote management, and security fields.



Benefits:

- Individual data centre solutions on a standardised basis (customised data centre)
- Flexibility in the selection of components and technologies
- Ongoing development of products
- Energy efficient solutions even for IT infrastructures with a total output in excess of 450 kW
- Pay as you grow
- Easy to extend right down to the component level

■ RiMatrix S, RiMatrix

Engineering & consulting

Innovative strength plus IT expertise plus decades of experience, all from a single source.

Thanks to our intelligently compiled portfolio of solutions, we will continuously supply you with ideas, concepts, innovations and the precise IT solution that you need for your company, right from the start. With Rittal, you can commit to high-end solutions: Engineering & consulting, data centre construction, IT infrastructures, and the international Rittal service. Utilise the knowledge, experience and products of a successful global player, for yourself and your IT.

Rittal develops and optimises individual IT solutions on your behalf, from small IT units to complex data centres. Our specialists carefully analyse the current status and your future requirements, the structural and physical conditions, and the existing IT structures, and use this information to tap into proven optimisation potential.

This facilitates the planning and implementation of IT systems with maximum efficiency in terms of performance, cost, processes, energy input, compatibility, availability and security. Rittal's technical and detailed planning teams will conduct all the necessary analyses and calculations, prepare all the drawings and documents, and select the optimum solutions and components for your IT environment.



Commissioning, service and support

Rittal International Services

- Installations are carried out by internationally trained staff (Haiger training centre, Super-Visor system)
- Experienced staff with many years of expertise are constantly travelling all over the world
- Quality management (independent testing by outside experts, as well as internal quality testing covering laboratory and production inspections through to cross-facility system acceptance)
- Proven expertise in all areas (research and development, purchasing, sales, project planning, project management, servicing)

Pre-sales

- Requirement analysis
- + load test
- + thermography
- + simulation and calculation

Implementation

- Installation/integration
- + commissioning
- + instruction
- + certification

After-sales

- Maintenance/installation + repairs
- + spare parts management
- + training
- + service contracts



■ RiMatrix S

The first “turnkey data centre” – RiMatrix S

The alternative to customer-specific data centre configuration in three designs: RiMatrix S

- Turnkey solution from one supplier, resulting in fewer interfaces and less effort at the design stage.
- High level of planning confidence and PUE can be calculated up front
- Standardised, series-produced data centre modules
- Only one Model No. for fully functioning centre, including server and network racks, climate control, power distribution and back-up, monitoring and DCIM (Data Centre Infrastructure Management)
- Available for immediate delivery



ENCLOSURES

POWER DISTRIBUTION

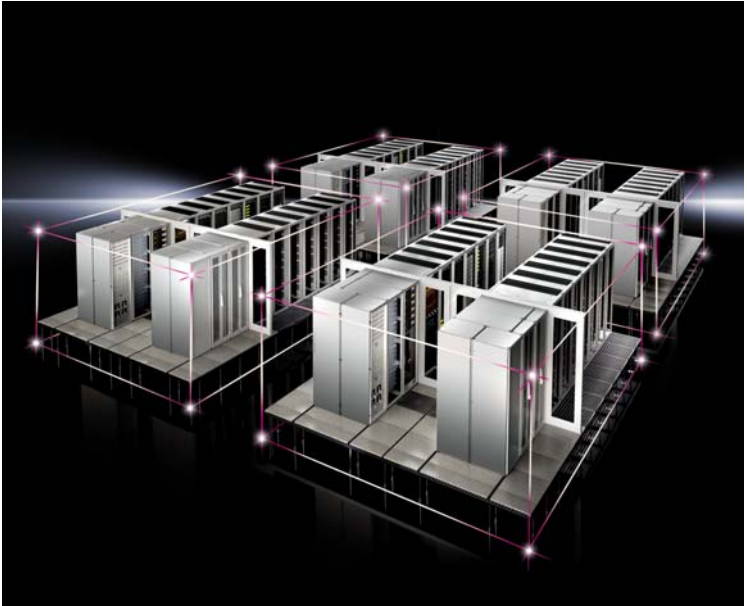
CLIMATE CONTROL

Scalable up to 450 kW

All RiMatrix S modules may be scaled for almost any power levels up to 450 kW. Various modules are available, which are used according to the spatial conditions.

Examples:

- Simple assembly of chessboard-like structures
- Parallel or serial arrangement
- Shared cold aisle and/or hot aisle
- Simple connection to supply infrastructures



System accessories – Rack/cooling

- Space-saving climate control in the raised floor
- n+1 redundancy in climate control
- Simple airflow with high energy efficiency
- TS IT racks with 19" frames, including compartmentalisation for logical separation of hot and cold zones
- TS IT accessories may be installed without the need for tools
- Rack depth 1,200 mm, installation height 42 U



System accessories – Power

A modular UPS system is used to provide power back-up for the rack. The complete n+1 redundancy with consistent parallel architecture ensures a high degree of availability. The battery supports the controlled shutdown of the servers or activation of a generator.

The maximum load is 60 kW for the Single 6 module and 90 kW for the Single 9 module. All components can be monitored via the CMC III monitoring system and incorporated into the RiZone DCIM solution.



System accessories – Cooling

Zero U-space cooling systems are provided for climate control, so that no installation space for servers is lost.

- The heat exchangers are located beneath the racks.
- The heat exchanger connection is easily accessible via the raised floor behind the racks.
- The n+1 redundancy offers a high level of availability, i.e. even if one zero U-space cooling system should fail, the required cooling capacity is still provided.
- EC fans ensure a low energy consumption, and the system is dimensioned to enable energy-saving part-load operation.
- The fans are arranged in the front of the server racks in the raised floor, in a maintenance-friendly configuration.
- Intelligent air flow via the raised floor guarantees optimum operation.



System accessories – Monitoring

- Monitoring of all relevant parameters, e.g. temperature, air humidity, leaks, etc., is performed by the CMC monitoring system
- Connection of security products, such as smoke extraction systems (SES)
- Continuous monitoring and evaluation of operating states using the RiZone DCIM software
- Display of efficiency and consumption values of the active systems
- Intelligent alarm management workflows for optimisation and protection
- Predefined projects, plug-and-play monitoring and management



Security with RiMatrix S

RiMatrix S provides peace of mind, thanks to:

- Reduced complexity
- Tested, quality-verified components
- Defined and monitored production processes
- Documented system test of the entire data centre module

For you as the user, this translates into:

- Low investment costs
- PUE (Power Usage Effectiveness) up to 1.15
- Tested characteristic curves and data sheets



ENCLOSURES

POWER DISTRIBUTION

CLIMATE CONTROL

Flexibility with RiMatrix S

The decoupling of the RiMatrix S modules from a physical cover and defined infrastructure interfaces make the modules extremely flexible.

For you as the user, this translates into:

- Simple integration into new or existing rooms with hot or cold aisle containment
- Installation in system-tested security rooms ...
- ... or as a flexible container solution
- Standardised modules for simplified worldwide delivery
- Commissioning by over 150 service partners with more than 1,000 service engineers



■ RiMatrix

The modular system of standardised components

Rack



Network/server enclosures

- Can be used individually for stand-alone installations and data centres
- Complete system solutions for small to large networks
- Maximum configuration diversity and protection for installed equipment
- Investment protection and flexibility thanks to simple conversions and use of our extensive modular system

Wall-mounted enclosures

- Choose from an extensive range of products – the right enclosure to suit all applications – up to protection category IP 66
- Wide choice of sizes available from 3 U to 21 U
- Wide choice of accessories with “Rittal – The System.”
- Fast assembly, modification and simple installation based on the modular principle

Power



Holistic, systematic energy management concepts

- Comprehensive and complete solutions for power distribution and back-up, consistently modular, and expandable as required
- Optimum energy and cost efficiency with maximum availability of the entire system
- Reduced installation, administration and manpower costs
- High level of investment security
- All from a single source

Cooling



- State-of-the-art climate control technology, from cooling of a single rack through to entire data centres
- Individual climate control concepts for rack, suite and room cooling
- Enhanced security plus superior energy and cost efficiency
- Optimisation with aisle containment and cross-system control concepts
- Energy-efficient cooling using IT chillers
- Minimisation of operating costs due to free cooling
- Environmentally friendly thanks to resource savings and reduced CO₂ emissions
- Planning, assembly, commissioning and service – all from a single source!

Monitoring



- A better overview of your IT infrastructure
- Enhanced security
- Automated processes
- Exceptional cost efficiency
- High energy savings
- Simple project management
- Fast installation
- Flexible, individual solutions using standard products from Rittal
- High standard of quality with coordinated standard products

Rittal – The System.

Faster – better – everywhere.



ENCLOSURES

POWER DISTRIBUTION

CLIMATE CONTROL

Expert knowledge

	Page
Standards and regulations	112
Electromagnetic compatibility	121
Copper cables	128
Optical fibres	131
Network cabling	134
Connectors	138
Important network technology devices	140
Network access methods	144
Terms relating to the Internet	150

■ Standards and regulations

Important standards for data and telecommunications

List of general standards	
DIN EN 61 000-6-3 (VDE 0839, Part 6-3)	Electromagnetic compatibility (EMC) Generic standards – Emission standard for residential, commercial and light-industrial environments
DIN EN 61 000-6-1 (VDE 0839, Part 6-1)	Electromagnetic compatibility (EMC) Generic standards – Immunity for residential, commercial and light-industrial environments
DIN EN 50 098-1	Customer premises cabling for information technology – Part 1: ISDN basic access
DIN EN 60 794 (VDE 0888)	Optical fibre cables
DIN EN 60 825-2 (VDE 0837, Part 2)	Safety of laser products – Part 2: Safety of fibre-optic communications systems
DIN EN 55 022 (VDE 0878, Part 22)	Information technology equipment. Radio disturbance characteristics. Limits and methods of measurement
DIN EN 50 288-5-1 (VDE 0819-5-1:2014-03)	Multi-element metallic cables used in analogue and digital communication and control Part 5-1: Sectional specification for shielded cables up to 250 MHz. Horizontal and building backbone cables
DIN EN 60 603-7-1 (VDE 0687-603-7-1:2012-01)	Connectors for electronic equipment Part 7-1: Detail specification for 8-way, shielded, free and fixed connectors

Installation of terminal equipment

List of standards for the installation of terminal equipment	
DIN EN 50 310 (VDE 0800-2-310:2011-5)	Application of equipotential bonding and earthing in buildings with information technology equipment
DIN EN 61 918 (VDE 0800-500:2009-01)	Industrial communication networks Installation of communication networks in industrial premises
DIN VDE 0845 VDE 0845 Supplement 1:2010-11	Overvoltage protection of information technology equipment (IT installations)

Types and use of communication cables	
DIN VDE 0891	Use of cables and insulated leads for telecommunications and information processing installations
DIN EN 60 794 (VDE 0888)	Fibre-optic cables
DIN EN 50 174-2 (VDE 0800, Part 174-2)	Information technology Cabling installation Installation planning and practices inside buildings



Network installation

Summary of DIN EN 50 173 standards: Information technology – Generic cabling systems

The concept of generic cabling systems is an essential part of the information technology infrastructure in buildings today, as it provides significant technical and economical benefits compared with the demand-oriented approach. The approach was originally developed for service-independent, universally applicable pre-cabling to support ICT network applications in office premises. The basic principles of generic cabling systems – uniform topology, classification of channels with defined characteristics, standard interface to connect terminal equipment – can also be transferred to other fields with certain modifications. Examples are industrial premises, residential buildings and data centres.

The series of EN 50 173 standards was developed by CENELEC/TC 215 in order to take account of the need of users for suitable standards for these application areas. During the development of this series, care was taken to ensure that the requirements and characteristics that apply to several or all types of buildings were only defined once – in Part 1.

Therefore, in order to implement a generic cabling system in a specific environment (building type, site), DIN EN 50 173-1 must always be applied together with the relevant part 2, 3, 4, 5, etc.

DIN EN 50 173-1 contains the primary and secondary cabling sub-systems and the transmission-relevant specifications of the channel classes and associated component categories for cables, connectors and connection cords of the terminal equipment.

In the current publication of **DIN EN 50173-1:2011-09, Information technology – Generic cabling systems – Part 1: General requirements**

an important modification introduced the requirements for the component categories 6A and 7A. Further changes to the previous version are the modification of the requirements for the insertion loss of coaxial channels, modification of the channel of class OF-100 for optical fibre cabling, the definition of a new optical fibre category OM4, and the supplementation and modification of requirements for the joining technique. Modifications also include the definition of both a new interface for two optical fibres as well as for 12 and 24 fibres, the revision of the test requirements for the mechanical and environment-relevant performance of the joining technique, the update of Annex F “Supported network tools”, and the introduction of a new normative Annex I “Test methods for determination of compliance with the standards of the EN 50 173 series”.

DIN EN 50 173, Part 2:**Office premises**

contains specifications for the tertiary (horizontal) cabling subsystem and requirements for the so-called information technological connection at the workplace which shall be used in office premises. These requirements apply equally for premises in buildings with mixed use (homes, doctors' surgeries, law offices, etc.), which are intended to be used as offices. In addition to the consideration of the new channel classes EA and FA and the associated component categories 6A and 7A, this standard contains requirements for type OM4 multimode optical fibres and type OS2 single mode optical fibres, and revised specifications for the joining technique.

DIN EN 50 173, Part 3:**Industrial premises**

contains the special requirements for generic cable systems which shall be applied for industrial premises. It supports the users of industrial automation systems who are increasingly interested in the use of a generic infrastructure instead of proprietary solutions, especially for continuous integration of these solutions into existing company networks in the office sector. These have, as a rule, been generic in design for many years and mostly use Ethernet-based protocols. The supported network tools for process monitoring and control are given in DIN EN 50 173-1. Allowance has been made for the topological features of industrial communication cabling systems by the introduction of additional horizontal floor wiring and intermediate cabling

subsystems; typical reference designs and the achievable maximum channel lengths are provided. In addition to channel lengths with symmetrical copper cables and optical cables with quartz glass fibres, the standard also contains the corresponding requirements for the use of synthetic fibres and plastic-coated quartz glass fibres. The specifications for the joining technique to be used take into account the harsh environmental conditions frequently found in industrial plants. In addition to the new channel classes EA and FA and the associated component categories 6A and 7A, this standard contains revised specifications for the joining of optical fibres.

DIN EN 50 173, Part 4:**Private residential units**

contains specifications for the generic cabling systems to be used in homes (single family and multi-family dwellings). These requirements apply equally to premises in buildings with mixed use (flats, doctors' surgeries, law offices, etc.), which are intended to be used as dwellings. The standard takes into account that in flats a variety of network applications from one or more of the following groups often have to be supported: Information and Communication Technologies (ICT), Broadcast and Communication Technologies (BCT) and Control/Command Communications in Buildings (CCCB). To support ICT and BCT network applications, the standard introduces the subsystem of residential cabling, which may be supplemented by a secondary subsystem where appropriate. Contrary to the star-shaped structure of ICT and BCT network

applications, the topology for CCCB applications can have various configurations (for example, bus, branch, closed loop).

Clause 5 of the standard therefore defines an individual cabling structure for these applications that may be realised in the coverage area subsystem. Corresponding CCCB network applications are specified, for example, in the standards of the DIN EN 50 090 series. In addition to taking into account the new channel classes EA and FA and the associated component categories 6A and 7A, this standard contains corrected levels of BCT channels with coaxial cables, updated formulas regarding the length of BCT channels and revised specifications for the joining technique.

DIN EN 50173, Part 5: Data centres

provides the operators and planners of data centres with a tool which allows for structured cabling for the first time and at the same time takes into account the special needs and characteristics of these facilities. Data centres are characterised by the extremely high volume of data cables needed for the provision of central server services (for example, web hosting) to a large number of users, both internally as well as to the outside world. The cabling topology defined in this standard provides a flexible structure which quickly and efficiently supports modifications and expansions to the cabling with minimum operational disruption while also taking into account the need for redundant network designs.

The high-performance channel classes provide a future-proof and economically attractive cabling infrastructure that will support the rapidly increasing transfer rates of the transmission facilities in data centres. This Part also considers the new channel classes EA and FA and the associated component categories 6A and 7A. In addition, this standard contains detailed specifications for optical fibre cabling and multimode optical fibre cables, revised specifications for the joining technique and the normative Annex B “Use of joining technique with high packing density in optical fibre cabling”.

Supported network applications (Appendix E)

Cat.	Network application	Source	Alternative name
A	PBX X.21 V.11	National requirement ITU-T recommendation X.21 ITU-T recommendation X.21	
B	S0 bus (extended) S0 point-to-point S1/S2 CSMA/CD 1Base5	ITU-T recommendation 1.430 ITU-T recommendation 1.430 ITU-T recommendation 1.431 ISO/IEC 8802-3	ISDN basic connection ISDN basic connection ISDN primary multiplex connection Star LAN
C	CSMA/CD 10Base-T CSMA/CD 100Base-T4 Token ring 4 Mbit/s	ISO/IEC 8802-3 ISO/IEC 8802-3 ISO/IEC 8802-5	Ethernet Fast Ethernet
D	TP-PMD CSMA/CD 100Base-TX Token ring 100 Mbit/s CSMA/CD 1000Base-T	ISO/IEC FCD 9314-10 ISO/IEC 8802-3 ISO/IEC 8802-5t ISO/IEC 8802-3	Media-dependent physical layer for twisted pairs Fast Ethernet High-speed token ring Gigabit Ethernet
E	ATM LAN 1.2 Gbit/s	ATM Forum af-phy-0162.000	ATM-1200/category 6
F	FC-100-TP	ISO/IEC 14 165-114	

Optical fibre cable runs

CSMA/CD 10Base-F Token ring	ISO/IEC 8802 AM ISO/IEC TR 11802-4	Connection of terminals to optical fibre cables
FDDI	EN ISO/IEC 9314-3	Distributed data interface with optical fibres
SM-FDDI LCF-FDDI	ISO/IEC 9314-4 ISO/IEC C 9314-9	Single-mode FDDI FDDI with low-cost optical fibres
FC-PH ATM	ISO/IEC CD 14165-1 ITU-T recommen. I.432	Fibre Channel B-ISDN

Important regulations for data and telecommunication enclosures and housings

“Rittal – The System.” means: efficient system solutions for the IT industry using modular and scalable infrastructures.

Constantly increasing demands for permanently available IT systems call for customised data centre solutions from a single source. With its years of experience as a system partner to the IT industry, Rittal draws on its expertise in the very specific issues and requirements of this sphere of activity.

Irrespective of whether server and network technology or data centre development are concerned, Rittal's innovative solutions for the IT sector are always synonymous with security, availability and optimum cost efficiency.

Its solutions comply with international standards and regulations, and set new benchmarks. The relevant standards, regulations and other useful hints are listed in this section.



ENCLOSURES

POWER DISTRIBUTION

CLIMATE CONTROL

DIN 41 488 Sheets 1 – 3	Dimensions for enclosures
DIN 41 494 Part 7	Construction of electronic equipment, dimensions for enclosures and rack rows (dimensions for 19" system)
DIN 43 668	Keys for cells or enclosure doors of electrical switchgear (double-bit) Size 3: Low-voltage installations
ETS 300 119-3	Equipment Engineering (EE); European telecommunication standard for equipment practice, part 3: Engineering requirements for miscellaneous racks and cabinets
IEC 60297-3-100	Dimensions of mechanical structures of the 482.6 mm (19 inch) series, part 3-100: Basic dimensions of front panels, subracks, chassis racks and cabinets Panels and racks, part 2: Cabinets and pitches of rack structures
DIN 43 656	Colours for indoor electrical switchgear

The German Energy Management Act states that: "Electrical power installations and power-consuming equipment shall be set up and maintained properly, i.e. in accordance with the recognised technical rules, such as the provisions of the German Association for Electrical, Electronic & Information Technologies (VDE)".

As systems below 1000 V are so widespread and diverse, special significance is attached to VDE 0100 "Provisions for the erection of power installations with rated voltages below 1000 V".

Other regulations which must be observed for power installations are the Technical Connection Conditions (TAB) of the electricity supply companies, and for telecommunications and aerial installations, VDE 0800 regulations for telecommunications systems and VDE 0855 provisions for antenna installations.

New installations should have provision for extension and should be economical. Important information on this can also be found in the connection conditions in the standard specifications lists (**DIN**) published by the German standards committee.

CE marking: legal position, standardisation

EU Directives

EU Directives lay down principles for the standardisation of (legal) regulations and standards applicable in Member States. They are used to simplify goods transactions within the EU.

Products that meet the requirements described in the Directives are identified with the CE mark.

Directives that are relevant to Rittal products:

- The EMC Directive 2004/108/EC
- The Low Voltage Directive 2006/95/EC

By using a CE mark, the manufacturer confirms on his own responsibility that his products conform with all the applicable EU Directives, i.e. the manufacturer must find out which EU Directives are relevant for his products. Enclosures that are intended and used for low-voltage switchgear enclosures in accordance with IEC 61 439 are subject to the provisions of the Low Voltage Directive, evaluated in accordance with DIN EN 62 208, and labelled with a CE mark.

Empty housings for general and IT applications and mechanical accessory components are not currently subject to any applicable EU Directive.

■ Electromagnetic compatibility

What is meant by EMC?

Electromagnetic compatibility (EMC) is the ability of an electrical appliance to operate satisfactorily in its electromagnetic environment without adversely affecting this environment, which may also contain other equipment.

High packing densities in electronic modules and ever-increasing signal processing speeds often cause faults in complex electronic equipment, measurement and control systems, data processing and transmission systems, and ICT systems. These faults can often be attributed to electromagnetic influences.

There are fundamental requirements for the

- prevention/reduction of interference emissions
- defined immunity to interference

The following definitions apply to immunity to interference:

An item of electrical equipment is said to be immune to interference if interference factors (up to a certain limit) do not lead to malfunctions:

■ Function impairment

A permissible impairment to proper functioning.

■ Malfunction

An impermissible impairment to proper functioning. The malfunction ends when the interference factor subsides.

■ Function failure

An impairment to proper functioning which is no longer permissible and which can, for example, only be eliminated by means of repair.



Basic EMC concepts

- Electromagnetic interference is the effect of electromagnetic factors on circuits, appliances, systems or living things.
- Interference source refers to the origin of the interference.
- Potentially susceptible equipment refers to electrical equipment whose function may be affected by interference factors.
- Coupling refers to an interaction between circuits through which energy can be transmitted from one circuit to another.
- Interference is an electromagnetic factor which may induce an undesirable influence in an electrical installation (interference voltage, current or field strength).

Interference sources and interference factors

Interference sources may be divided into:

- Internal sources of interference
 - artificial, i.e. technically induced
- External sources of interference
 - natural, e.g. lightning; electrostatic discharges
 - artificial, i.e. technically induced

Where technically induced interference sources are involved, a distinction must be made between the effects of electromagnetic factors created and used for business purposes (such as radio transmitters, radar, etc.), and electromagnetic factors occurring within the context of operations or in the event of a fault and which are not deliberately generated (e.g. spark discharges on switch contacts, the magnetic fields generated by high currents, etc.).

Interference may take the form of voltages, currents, or electrical, magnetic and electromagnetic fields, which may either occur continuously, periodically, or randomly in a pulse shape.

In low-voltage networks, the following applies:

- The most interference-intensive temporary events are caused in low-voltage networks by the switching of inductive loads, e.g. power tools, household electrical appliances, fluorescent lamps.
- The most dangerous overvoltages (according to level, duration and power content) are caused by fuses tripping in the event of a short circuit (duration in the millisecond range).

Electrostatic discharges

When solid materials rub against one another, electrostatic charges may be generated. These will discharge quickly on conductive surfaces but may persist for a long time on less conductive surfaces.

Upon contact with conductive parts, the electrostatic voltages associated with such charges in non-conductors may cause interference or even destruction in electronic components as discharge current.

Electrostatic discharges from humans onto control components and device housings are particularly significant. The voltages occurring in such cases may be as high as 15,000 V, with discharge currents of up to 5 A, and current rise rates of up to 5 kA/ μ s. The risk of malfunctions or damage is increased by poorly conductive floor coverings and low air humidity.

Examples of the sensitivity of semiconductor components

Components at risk	Voltage
ICs (Integrated Circuits) in P-FP (Plastic Flat Pack) and P-LCC (Plastic Leaded Chip Carrier)	from 20 V
Schottky diodes	from 30 V
Field-effect transistors and EPROMs	from 100 V
Operational amplifiers	from 180 V
Film resistors	from 350 V
Schottky TTL	from 1,000 V
ICs in CLCC (Ceramic Leaded Chip Carrier)	from 2,000 V

Measures to protect electrostatic-sensitive components

- Sensitive components should remain in their original packaging until they are required.
- Sensitive components must only be stored and transported in high-resistance conductive or antistatic containers.
- When removing a component from the packaging, first touch the packaging to discharge it. Only then may the component be removed.
- When populating a printed circuit board, first touch the printed circuit board to discharge it. Only then may the component be inserted.
- The components may only be handled at specially designed workplaces:
 - Soldering iron tips must be earthed.
 - Work tables and floors must be antistatic and conductive.
 - Work should be carried out on work mats, which are connected to the skin via an antistatic wrist strap.
 - Work clothes should be made of cotton and not of synthetic fibres that become charged.
 - Shoes should be covered by a conductive material.
- A minimum distance of 10 cm from VDUs should be maintained.

Interference mechanisms and countermeasures

A distinction can be made between the following types of coupling mechanism:

- Conducted interference
- Field-related interference
 - Field interference
 - Radiation interference

Conducted interference

Galvanic coupling

Interference arises over shared line sections (power supply cables, earthing, etc.) and can be avoided or limited by:

- short and low-resistance shared line sections
- a separate power supply
- electrical isolation using optocouplers, isolation transformers, relays, etc. for signal lines and to separate the power supply and data cables.

Capacitive coupling

Capacitive interference is caused by unintended capacitances in the circuitry between conductive structures belonging to different circuits. Countermeasures are:

- short, non-parallel cable runs between components
- use of shielded cables.

Inductive coupling

Interference voltages are usually induced between independent circuits as the result of rapidly changing high currents, or by electrostatic or lightning discharges. These might be interpreted as a signal or result in voltage flashovers.

To minimise or avoid these problems, the following measures are recommended:

- using twisted or shielded cables
- large distances between power and data cables
- smallest possible areas enclosed by circuits.

Wave interference

Electromagnetic waves on cables can cause interference voltages through a combination of capacitive and inductive coupling. This happens if the wavelength of the disturbance is more or less the same as the system dimensions or the rise times of the interference pulses correspond to the signal propagation times. A countermeasure is

- the use of shielded cables.
- Measures to minimise the effect are
- filters and/or
 - overvoltage protection devices.

Field interference (low frequency)

Very low-frequency currents cause a low-frequency magnetic field which may induce interference voltages or initiate interference via direct magnetic effects (magnetic data storage in computers, sensitive electromagnetic test equipment). Low-frequency electric fields of high intensity may be generated by low-frequency high voltages (high-voltage overhead lines), resulting in interference voltages (capacitive interference).

Of practical significance are magnetic fields, the effects of which can be reduced via

- shielded cables
- shielding housings (the determining material property is permeability, which is too low in the case of sheet steel; permalloy, for example, is much better).

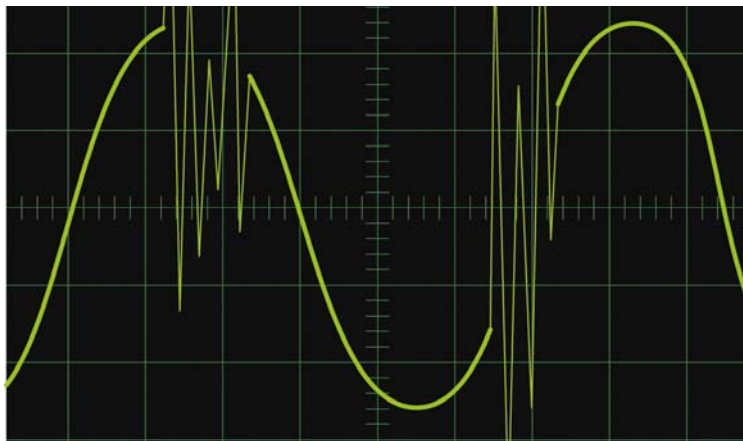
Radiation interference (high-frequency)

The electromagnetic waves which radiate from electrical circuits in an open space can produce interference voltages, whereby such interference must then be considered in relation to the distance to its source (near field or distant field).

In a near field, either the electrical component (E) or the magnetic component (H) of the electromagnetic field will predominate, depending on whether the source of the interference carries high voltages and low currents, or high currents and low voltages. In a distant field, generally speaking, E and H can no longer be considered separately.

Interference can be reduced via

- shielded cables
- shielding housing (Faraday cage).



Housing/RF shielding

The requirement profile can be determined using the following checklist.

Checklist to determine the requirement profile for EMC housings

- What types of interference occur in the given application (electric, magnetic or electromagnetic field)?
- What interference limits can occur in the application (field strengths, frequency range)?
- Can the requirements be met by a standard housing or an RF shielded housing (comparison using attenuation diagrams)?
- Are there any other EMC requirements (partitioning within the housing, special potential equalisation within the housing, etc.)?

Every sheet metal housing already offers good **basic shielding** within a broad frequency range, i.e. attenuation of electromagnetic fields.

For large enclosures, **medium shield attenuation** can be achieved via cost-effective measures to create multiple conductive connections between all housing parts.

High shielding attenuation levels in the frequency range above approx. 5 MHz can be achieved via special seals which connect the conductive inner surfaces of doors and removable panels, roof and gland plates to the conductive sealing edges of the housing body or frame, in a largely slot-free manner. The higher the frequencies occurring, the more critical the openings in the housing become.



Copper cables

Identification colours of bare and insulated conductors

Current system	Conductor designation	Code	Colour	Conductor designation	Code	Symbol	Colour
DC current	Positive	L+	¹⁾	Neutral conductor with protective function	PEN		yegn
	Negative	L-	¹⁾				
	Neutral conductor	M	lbl				
AC current	Outer conductor	L1; L2; L3	¹⁾	PE conductor	PE		yegn
	Neutral conductor	N	lbl				
¹⁾ Colour not defined			–	Earth	E		¹⁾

Design codes for types of lines and cables used in communication technology

Example:

J- Y (St) Y 20 x 2 x 0.6 Lg

= Wiring cable, PVC insulated wires, electrostatic shield, PVC cable sheath, 20 wire pairs, cable diameter 0.6 mm, layer-stranded

Designation position:

J-	Y	(St)	Y	20	x 2	x 0.6	Lg	11		
1	2	3	4	5	6	7	8	9	10	11

1 Type of cable

- A-: External cable
- FL-: Flat cable
- J-: Wiring cable and flat webbed cable
- Li-: Litz wire
- S-: Switch cable

2 Core insulation

- Y: Polyvinyl chloride (PVC)
- 2Y: Polyethylene (PE)
- 02Y: Cellular PE

3 Shield

- C: Copper braid
- (K): Shield made of Cu strip over PE sheath
- (L): Aluminium strip
- (mS): Magnetic shield made of steel strip
- (St): Static shield

4 Sheath

- E: Encapsulated plastic strip
- FE: Cable made of flame retardant material < 20 minutes
- G: Rubber casing
- H: Halogen-free material
- L: Smooth aluminium sheath
- (L)2Y: Al sheath welded with PE material
- M: Lead sheath

5 Protective sheathing

- Y(v): PVC sheath (reinforced)
- 2Y: PE sheath

11 Armour

- A: Layer Al wires for induction protection
- B: Steel strip for induction protection

10 Stranding arrangement

- Bd: Bundled
- Lg: Concentric
- rd: Round
- se: Sector-shaped

9 Type of stranding/design

- DM: Dieselhorst-Martin quad stranding
- Kx: Coaxial cable
- P: Paired
- PIMF: Pairs in Metal Foil
- St: Star quad w. spec. characteristics
- St I: Star quad without phantom utilisation
- St II: Star quad for short-haul cable
- St III: Star quad, at 800 Hz
- St IV: Star quad, at 120 kHz
- St V: Star quad, at 550 kHz
- St VI: Star quad, at 17 MHz




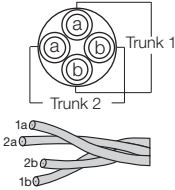
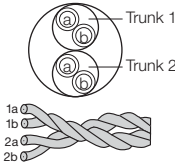

8 Cable diameter in mm

7 Stranded element

- x 1: Single wire
- x 2: Pair (two-core)
- x 3: Triple
- x 4: Quad

6 Number of stranded elements

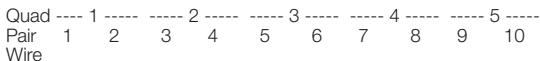
Structure of copper cables, stranded elements

<p>Wire</p> 	<p>A wire is a conductor with an insulated core.</p>
<p>Pair (two-core)</p> 	<p>A pair (two-core) consists of two stranded cores (twisted) that form a wiring circuit (loop). The pair is the simplest symmetrical stranded element.</p>
<p>Pair (two-core)</p>  <p>Sheath wire</p>	<p>A shielded pair is a Pair in MetalFoil (PiMF). It consists of two stranded cores that form a wiring circuit (loop) and that has a protective static shield applied around it. A galvanised iron wire (sheath wire) is connected to the static shield along its entire length.</p>
<p>Star quad</p>  <p>Trunk 1</p> <p>Trunk 2</p> <p>1a</p> <p>2a</p> <p>2b</p> <p>1b</p>	<p>A quad consists of four stranded cores, from which a wiring circuit is formed from each of the two opposing cores (loop, trunk and trunk circuit). The trunks are also referred to as two-cores.</p>
<p>Dieselhorst-Martin quad (DM quad)</p>  <p>Trunk 1</p> <p>Trunk 2</p> <p>1a</p> <p>1b</p> <p>2a</p> <p>2b</p>	<p>Dieselhorst-Martin quads have two cores twisted to form a pair and two pairs twisted into a quad. Both pairs have different twists to achieve better crosstalk attenuation. A DM quad has lower capacitance and a lower transmission loss compared to a star quad.</p>
<p>Bundle</p>  <p>Stranded element, e. g. pair</p>	<p>A bundle comprises five consolidated stranded elements.</p>

Identifying and counting communication cables

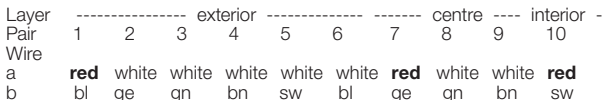
Communication cables are ALWAYS counted in pairs:

- Bundled (colour and ring coding)
 - Colours per quad: red (rt), green (gn), grey (gr), yellow (ge), white (ws);
 - Rings per wire: [Quantity/distance in mm];
 - from 11 pairs upwards: additional coding of bundles using colour coils

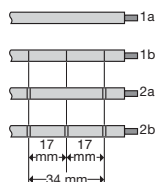


a	[0/0]	[2/34]	[0/0]	[2/34]	[0/0]	[2/34]	[0/0]	[2/34]	[0/0]	[2/34]
b	[1/17]	[2/17]	[1/17]	[2/17]	[1/17]	[2/17]	[1/17]	[2/17]	[1/17]	[2/17]

- Layer stranding (colour-coding)
 - Counted layer by layer from exterior to interior;
 - all a-wires white, every first a-wire per layer red (meter wire);
 - b-wires in ascending order
 - blue (bl), yellow (ge), green (gn), brown (bn), black (sw)

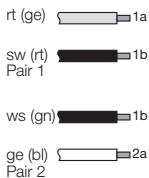


Coding with rings
(e.g. for J-2Y(St)Y
2x2x0.6 Bd)



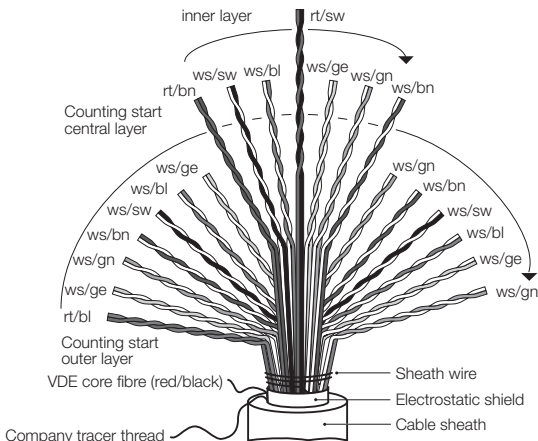
Primary colour red,
rings black

Colour-coding
(e.g. for J-Y(St)Y
2x2x0.6 Lg)
new (old)



Example:

J- Y (St) Y 20 x 2 x 0.6 Lg



Identifying optical fibre cables

Design codes

Example:

A- W S F (ZN)2Y Y 12 G 50/125 3.0 B 600 Lg

= External cable with filled loosely buffered fibres, metal elements in the filled cable core, PE sheath with non-metal strain relief elements and PVC sheath, 12 graded fibres with 50 mm core diameters and 125 mm sheath diameters, with an attenuation coefficient of ≤ 3 dB/km and a bandwidth of 600 MHz per km at a wavelength of 850 nm, layer stranding.

Designation position:

A-	W	S	F	(ZN)2Y	Y	12	G	50/	125	3.0	B	600	Lg
1	2	3	4	5	6	7	8	9	10	11	12	13	14

1 Type of cable

- A-: External cable
- AT-: External cable, splittable
- J: Internal cable

2 Structure

- F: Fibre
- V: Buffered fibre
- W: Loosely buffered fibre, filled
- B: Buffered fibre, filled

3 Cable core

- S: Metal element in the cable core

4 Filling

- F: Petrolatum filling

5 Sheath

- H: External sheath made of halogen-free material
- Y: PVC sheath
- 2Y: PE sheath
- (L)2Y: Layer material
- (ZN)2Y: PE sheath with non-metal strain relief elements

6 Armour

- B: Armour
- BY: Armour made of PVC protective sheathing
- B2Y: Armour made of PE protective sheathing
- H: Sheath made of halogen-free material
- Y: PVC sheath

14

- Lg: Layer stranding

13

- xxx: Bandwidth in MHz for L = 1 km

12 Wavelength window

- B: Wavelength 850 nm
- F: Wavelength 1300 nm
- H: Wavelength 1550 nm

11

- xxx: Attenuation coefficient in dB/km

10

- xxx: Sheath diameter in μm

9

- xxx: Core diameter in μm or mode field diameter in μm at Single-mode fibres (MNM)

8 Type of fibre

- E: Single-mode fibre (MNM)
- G: Graded fibre glass/glass
- K: Step-index synthetic

7

- xxx: No. of cores

Typical characteristics of optical fibre cables – example

Type of fibre	G 50/125	E 9/125
Core diameter in μm	50 ± 3	≈ 9
Mode field diameter in μm	–	9 ± 1
Sheath diameter in μm	125 ± 25	125 ± 25
Tensile strength	5 N	5 N
Average tensile strength	50 N	50 N
Bending radius	50 mm	50 mm
Bandwidth in MHz \times km at	850 nm: 200...600; 1,300 nm: 600...1200	
Loss in dB/km at	850 nm: 2.5...3.5; 1,300 nm: 0.7...1.5	
Dispersion in ps/nm \times km at	–	1,300 nm: < 5; 1,550 nm: < 20

■ Network cabling

Bandwidth

The bandwidth is the difference between the upper and lower frequency expressed in the physical unit Hertz (Hz). The greater the bandwidth, the more information theoretically transmitted per unit of time. For this reason it is a reference value for the analogue transmission capacity of a channel. In addition, bandwidth also

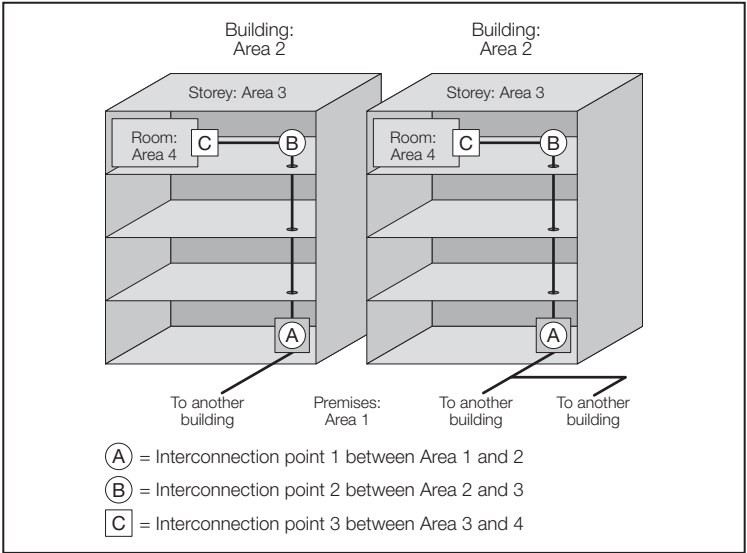
means the transmission capacity of a system measured in bit/s, Mbit/s or a multiple. Thus there is a direct correlation between bandwidth and transmission rate. Where data transmission is concerned, the maximum transmission speed depends on the bandwidth of the network.

Building wiring

Building wiring is a component of structured wiring and denotes universal, manufacturer-independent wiring in a building for information technology communication. Components of building wiring standards are:

- Wiring planning
- Topologies/network design
- Installation
- Electromagnetic compatibility
- Performance and application classes of cable types

Building wiring when referred to as secondary wiring covers the area between building distributors, BD, and storey distributors, SD.



Building wiring with backbone and horizontal wiring

Source: Lexikon der Datenkommunikation

Network application classes and cable categories

Class	Category	Frequency range	Possible applications
A	1	up to 100 kHz	Analogue telephone
B	2	up to 1 MHz	ISDN
C	3	up to 16 MHz	10BaseT, token ring
D	5	up to 100 MHz	100BaseTX
E	6	up to 250 MHz	Gigabit Ethernet, ATM
F	7	up to 600 MHz	Gigabit Ethernet, ATM

Characteristic values for frequently used telecommunication cables

Wire Ø d mm	Characteristic values				Attenuation factor α at 800 Hz dB/km	Characteristic impedance Z_w at 800 Hz Ω
	R Ω /km	L mH/km	G μ S/km	C nF/km		
0.4	270	0.7	0.1	34	1.31	1260
0.6	122	0.7	0.1	37	0.91	810
0.8	67	0.7	0.1	38	0.69	590
0.9	52	0.7	0.1	34	0.58	550
1.2	29	0.7	0.1	35	0.45	430

Coding of network cables

Example:

10 Base

Intended transmission rate in MBit/s
Base (baseband)
Broad (broadband)



Suffix F for optical fibres
Suffix T for twisted pair

(Coaxial) cable with a transmission rate of 10 MBit/s and a maximum cable length of 200 m

Characteristics

Designation	Twisted Pair 10BaseT	Ethernet optical fibre 10BaseF
Application	Ethernet, token ring, FDDI, ATM	Ethernet, token ring, FDDI, ATM
Max. subscribers	any number	any number
Impedance in W	–	–
Transmission rate in MBit/s	10	10
Max. length in m	100	500
Comment	For Ethernet and FDDI tree or star-shaped point-to-point connection. All 8 connections of the RJ45 connector should be allocated. With repeater no length restriction.	Point-to-point connections. Suitable for bridging long sections. Bridges are connected at the ends to transfer to twisted pairs and coaxial cables.

Cable architectures

Identification scheme in the form XX/YYZ introduced.

XX represents the overall shielding:

U = unshielded

F = foil shield

S = braided shield

SF = braided and foil shield

YY represents the core pair shielding:

U = unshielded

F = foil shield

S = braided shield

ZZ represents:

TP = Twisted Pair

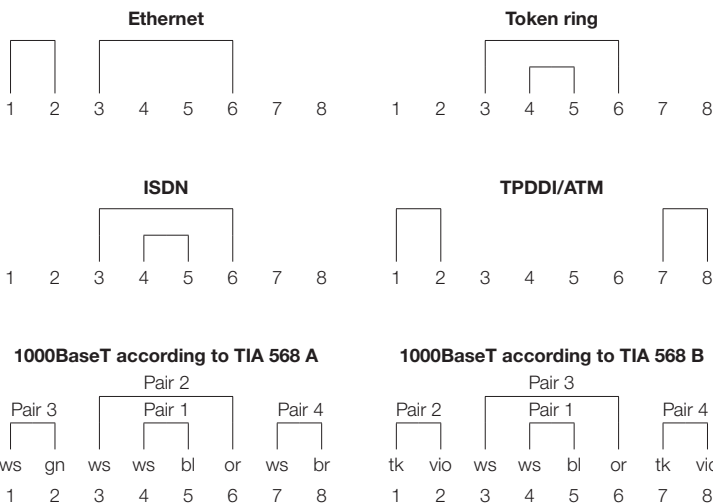
QP = Quad Pair

Connectors

Classification of connector/cable types

Jack/coupling	Cable types
Twinax; BNC E; BNC F	Coaxial cables
RJ 11 – 45 48 modular jacks; 32 modular jacks	Shielded/unshielded twisted pair cable (2 to 4 pair)
F-SMA E 2000; LC; MTRJ; ST; ST Duplex; Biconic; FC/PC	Optical fibres
D-Sub 9-pin; D-Sub 15-pin; D-Sub 25-pin; ADO 4/8; TAE 4/6	Shielded/unshielded cables

Pin configuration and pair allocation for twisted pair wiring with RJ 45 connectors



Optical fibre connector selection

Type	For	Typical insertion loss	Advantage	Disadvantage
F-SMA	Multi-mode fibres	0.7...1 dB (G50/125) 0.6...0.8 dB (G62.5/125)	Connector cannot be disconnected by hand without using tool (when using specified torque)	<ul style="list-style-type: none"> ■ Difficult to connect to tightly packed patch fields due to screw closure ■ No locking element, therefore fibre contact not possible, higher attenuation values
DIN	Single, multi-mode fibres	0.2...0.4 dB (9/125) 0.2...0.4 dB (50/125)	Precise centring of the fibre core in the connector	<ul style="list-style-type: none"> ■ Only standardised by DIN, no widespread dissemination (German telecommunications corporation) ■ Cannot be directly fitted, pigtails must be spliced
FC/PC	Single, multi-mode fibres	0.2...0.5 dB (9/125) 0.2...0.5 dB (50/125)	Similar to DIN connector	
ST	Single, multi-mode fibres	0.3...0.4 dB (G50/125) 0.2...0.3 dB (G62.5/125)	Locking device prevents rotation	
SC	Single, multi-mode fibres	0.3 dB	<ul style="list-style-type: none"> ■ Locking device ■ Engages when inserted 	
FDDI (MIC)	Single, multi-mode fibres	0.5 dB	<ul style="list-style-type: none"> ■ No confusion between sender and receiver path ■ Clear port allocation due to coding 	<ul style="list-style-type: none"> ■ Expensive construction, not field-formable ■ Large space requirement for connector and jack
E 2000	Single, multi-mode fibres	0.2...0.4 dB (9/125) 0.2...0.4 dB (50/125)	<ul style="list-style-type: none"> ■ Latch mechanism ■ Shield/protective flap protects operator from laser beam ■ Compact design for high packing density 	
LC	Single, multi-mode fibres	0.2 dB	<ul style="list-style-type: none"> ■ Latch fastening closure ■ Compact design for high packing density 	
MTRJ	Single, multi-mode fibres	0.3 – 0.5 dB	<ul style="list-style-type: none"> ■ Latch fastening closure ■ Compact design for high packing density 	



■ Important network technology devices

Building distributor, BD

The building distributor represents the interconnection point of the site wiring to the building wiring. The BD includes all points of contact of the building wiring with patchboards and patch fields, and the points of contact to the site wiring. The transmission medium may contain, for example, optical fibre cables to TP cables or other data cables.

Building distributor

Network card (Network Interface Card – NIC)

for Ethernet networks

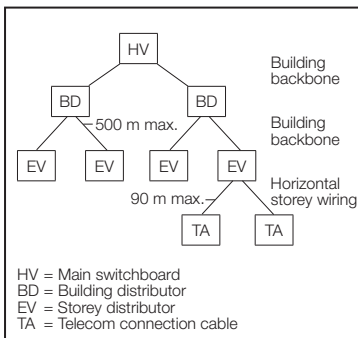
Consisting of:

- Network interface, for 10Base5, 10Base2, 10BaseT, 100BaseT, etc., to connect to the network cabling
- Process logic to convert parallel data into bit-serial data
- Bus interface to connect to the PC bus

The NIC works on OSI Layers 1 and 2; network cards that support 10 and 100 Mbit/s automatically adjust themselves to the correct speed.

Gateway

The generic term **gateway** encompasses a series of different types of technical equipment that is required to establish connections between networks. Depending on the complexity of the gateway, it can refer to a single repeater or complete computers.



Cabling areas in accordance with the cabling standard EIA/TIA 568

Gateways are required if a network

- is to be structured; i.e. divided into subnetworks
- is to be extended; i.e. the network is to be physically enlarged
- is to be intermeshed with other networks; i.e. several LAN will be connected to one another or a WAN connection is planned, so that a heterogeneous network is achieved.

Repeater

A repeater regenerates signals, increases the maximum segment length; works on OSI Layer 1; other types:

- **Multipoint repeater:** enables a network to be segmented to increase availability
- **Star coupler:** to connect numerous network segments, enables media conversion (e.g. from copper to optical fibre)

Source: Lexikon der Datenkommunikation

- **Hub or concentrator:** to build networks in star topology, with additional functionalities (bridge, router), often cascadable, universal and widely used device.

Bridge (Switch → Multiport Bridge)

To divide large networks into smaller subnetworks; incorrect data packets remain in the subnetwork, switch disconnection is possible, as data packets for an address are not transported to the internal subnetwork; works on OSI Layer 2; other types:

- **Local Bridge:** to connect similar and different networks (e.g. Ethernet – token ring)

- **Remote Bridge:** to connect networks via wide area networks
- **Multiport Bridge** (often identical to switch): to connect several subnetworks.

Router

To navigate in extended LAN and WAN networks of different types, protocols and topologies; works on OSI Layer 3.

Gateway

To connect completely different networks, e.g. connecting LAN to open WAN or host systems; works on OSI Layers 4, 5, 6 or 7.

ISO OSI Layer model:

(OSI: Open Systems Interconnection, ISO: International Standards Organization)

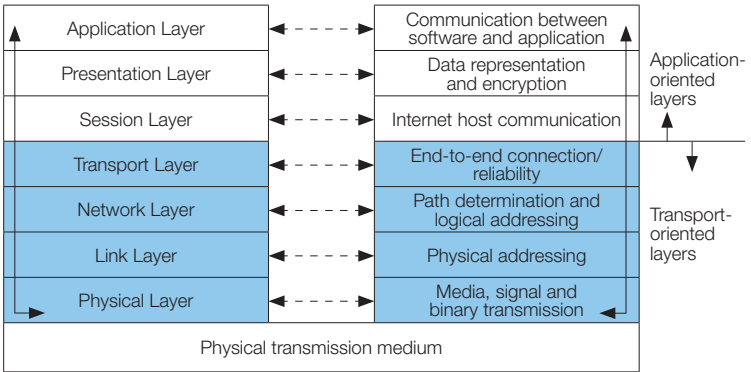
The OSI model describes all components required for computer communication. A total of seven layers that build on one another are defined. Applications based on the top level of the model should be able to function completely independently of the model and network. Their access to the transmission medium is achieved through all seven layers.

Information which is to be transmitted from one system to another must initially pass through all the layers below it before reaching the top layer.

The information is then transported via the physical medium (network cabling). At each layer, control information (protocol overhead) is added to the data.

Systems can only communicate with one another if their layer structures match.

Of the seven layers of the model, the three upper layers (5, 6 and 7) are application-oriented, the four lower layers (1 – 4) are transport-oriented.



Source: Lexikon der Datenkommunikation, page 374

- Actual transport
- - - - - Virtual protocols of the layers

The OSI reference model showing division into application and transport layers

Basic concepts of the OSI model:

Instances: An instance is a module in a layer, which can be implemented in hardware and software. Communication can take place vertically with instances in higher or lower layers and horizontally with spatially separated instances.

Services: Services that a layer offers to a higher layer.

Protocols: The communication between instances on the same layer is carried out through protocols.

Packets: Information is exchanged between layers via packets.

7. Application Layer

This is the part of software that is responsible for communication, and at the same time the starting point and destination of the transported user data.

For example, during file transfer the layer is responsible for adapting the file to the standard conventions on the target system (e.g. with respect to the file name).

E-mail is an example of a service offered by this layer.

6. Presentation Layer

This provides the application with an interface to the network and defines the program's access method to the network. It provides functions for data transport by converting data from above into a valid standard format for the network, i.e. its tasks are formatting, structuring, encrypting and compressing data.

5. Session Layer

This establishes the connection in the network for the higher network services. The session layer is responsible for managing communication between two applications.

4. Transport Layer

This is responsible for establishing a connection between two devices and the individual transport layer, which maintains an end-to-end connection between the physical end points. As the uppermost of the transport layers, it offers the application layers above it a general and independent transmission service. It is of no concern to the transport layer whether layers 1 to 3 are implemented as LAN or WAN.

3. Network Layer

The Network layer is an additional layer, which is actually not required if the end systems are connected to one another directly by a cable. In complex and heterogeneous networks, a direct connection is rare. The network layer contains the logic for sending data in complex and heterogeneous networks to the destination device via several network nodes (not required for end systems with a direct cable connection). In packet-oriented networks (e.g. all LAN), it controls connection establishment and clearing, undertakes routing and is responsible for addressing. The network layer establishes an end-to-end connection between devices. These devices do not have to be the end systems, they can also be network gateways. X.25 Packet Layer is an example of a service offered by layer 3.

2. Link Layer

This is responsible for ensuring the data transmission is accurate. The bitstream from above is broken down into frames, as the single transmission of data blocks is simpler, more manageable and easier to correct. At the receiving end, the layer undertakes recovery of the bitstream from the frames coming from below. For circuit-switched networks (e.g. telephony service-oriented networks, ISDN) it also controls connection establishment and clearing. The X.25 HDLC protocol is an example of a level 2 protocol.

1. Physical Layer

This is the only layer in direct contact with the physical transmission medium and is therefore responsible for the electrical and mechanical definitions (e.g. the pin assignment, voltage and interface signals). The physical layer defines the physical connection within the network. It has the task of controlling the medium and is the only layer to directly send and receive the unstructured bitstreams. An example is the X.21 interface, which is also used in the X.25 protocol.

■ Network access methods

CSMA/CD and Ethernet

The IEEE recommendation **802.3** describes the access method **CSMA/CD** (Carrier Sense Multiple Access/ Collision Detection) and physical transfer to a data bus. All terminals are connected to a bidirectional bus. Data can be transmitted at speeds from 1 to 10 Mbit/s.

Although the recommendation assumes a bus structure, today's networks are usually star-shaped. Every terminal maintains a connection to a central node (hub), which interconnects all connected lines internally. This means a star is physi-

cally created, although it still acts as a bus structure logically through the management of the hub.

It is often wrongly assumed that the CSMA/CD medium access method is identical to **Ethernet**, which is actually a special product used by CSMA/CD. It was developed by Xerox, DEC and Intel and has been used for the past 20 years or so.

Further developments include Fast Ethernet (100Base, etc.) and Gigabit Ethernet (1000Base, etc.) for transmission rates of up to 100 or 1000 Mbit/s.

Ethernet cabling variants

Name	Cable type	Segment length	Segments	Terminals in all segments	Min. distance between terminals	Transfer rate
10Base5 ThickWire	Coaxial cables	500/3000 m	5	100/492	2 m	10 Mbit/s
10Base2 ThinWire	Coaxial cables	185/925 m	5	30/142	0.5 m	10 Mbit/s
10BaseT Twisted Pair	Twisted copper cable	100 m	1	1	–	10 Mbit/s
10BaseFP	Optical fibre	500 m	1	1	–	10 Mbit/s
10BaseFB	Optical fibre	2 km	1	1	–	10 Mbit/s
100BaseT	Twisted copper cable	100 m	1	1	–	100 Mbit/s
100BaseVG	Twisted copper cable	100 m	1	1	–	100 Mbit/s
1000BaseCX	Twinax copper cable	25 m	1	1	–	1000 Mbit/s
1000BaseLX	Optical fibre Multimode Monomode	440/550 m 3000 m	1	1	2 m	1000 Mbit/s
1000BaseSX	Optical fibre Multimode	260/550 m	1	1	2 m	1000 Mbit/s

Token ring

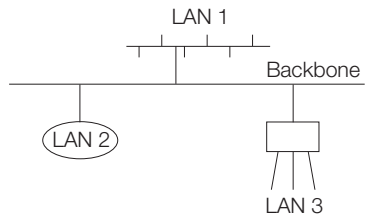
The token ring ranks in second place with regard to its distribution in LAN network structures. Originally developed by IBM, it was only later that it was standardised in the IEEE 802.5 recommendation. It is predominantly found in home environments dominated by IBM computers. LAN technology with a ring topology has been in use for around 10 years. The simple ring structure has been slightly modified to achieve higher fault tolerance. Each terminal is connected separately via a cabling centre (Ring Wiring Concentrator, RWC).

This creates a star-shaped ring, which is physically a star, but logically a ring. The ring can be run at 4 or 16 Mbit/s and is cabled with copper multi-strand twisted pairs.

Data traffic on the token ring takes place in a single direction. Each terminal receives data via the receiving end and sends it to the next terminal via the sending end after a short delay. The interim buffering and short delay are required so that the permission to send – the so-called free token – applies to the entire ring. The access method is known as token passing.

Backbone (BB)

The backbone network forms a separate infrastructure for information exchange between the networks and systems in hierarchically configured networks. As a rule, this is used to describe networks like a Wide Area Network (WAN) that connects several subnetworks, such as Local Area Networks (LAN), via bridges and routers. Its distinguishing features are low levels of downtime, high transmission capacity and a lack of local connections. A distinction is made between collapsed backbones and distributed backbones.

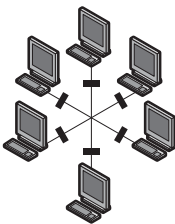


Source: Lexikon der Datenkommunikation

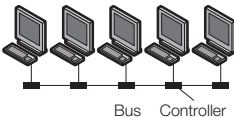
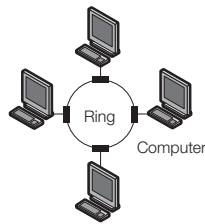
Network topologies

The topology describes the basic geometric structure of the cabling. Four standard topologies, the ring, bus, star and tree, have become established. In larger networks hybrids of these topologies can be found.

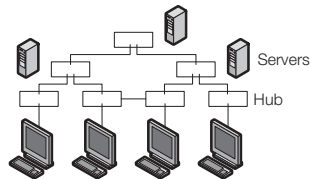
		Advantages and disadvantages
Ring	In a ring topology, the network terminals are each connected to the next terminal and the last one to the first to form a ring, e. g. token ring; FDDI	+ Fault tolerance + Guaranteed bandwidth – High costs – Complexity
Bus	All network terminals communicate via a common data cable: e.g. Ethernet	+ Complexity in small networks – Fault problems – Fault analysis – Bandwidth in large networks
Star	Point-to-point connections to the individual network nodes are established from a central network node (hub, switch)	+ Fault tolerance + Bandwidth – Fault in the central network node
Tree	The tree topology is characterised by a high level of flexibility in its structure. It can be formed by cascading hubs or switches: e.g. 100BaseAnyLan.	+ Flexibility – Complexity



Star



Bus Controller



Workstation Tree

Network protocols

Most network protocols are consolidated into protocol sets, which are grouped together to handle the various communication tasks in networks.

Examples of protocol sets

		Advantages and disadvantages
TCP/IP	(Transmission Control Protocol/Internet Protocol) The computers connected to the network are identified by IP addresses. A device with an IP address is known as a host. Originally, TCP was developed as a monolithic network protocol, but was then divided into the protocols IP and TCP. The core group of the protocol family is supplemented by the User Datagram Protocol (UDP) as an additional transport protocol. In addition, there are numerous auxiliary and application protocols, such as DHCP and ARP. Developed by the US Department of Defense at the end of the 1970s as part of the DoD protocol family. It is one of the most widely used protocol sets. Used in all important operating system platforms, such as Unix, VMS, Windows and DOS. Particularly suitable for heterogeneous environments.	+ Heterogeneous environment + Routable + Widely used
IP	Internet Protocol	

TCP/IP protocol set

Transport protocol TCP

TCP is a connection-oriented protocol that provides fault correction and flow control services. The provision of these services incurs additional expenditure, as connections must be established and completed. Correcting errors utilises additional capacities.

Terms relating to TCP/IP protocol set

ARP	(Address Resolution Protocol) Allocation of hardware addresses to IP addresses				
BGP	(Border Gateway Protocol) Contains accessibility and routing information				
BIND	(Berkeley Internet Name Domain) Implementation of DNS				
BOOTP	(Boot Protocol) A network node requests information from a network. The requests are answered by a BOOTP server.				
Datagram	Information unit in layers 3 or 4 of the TCP/IP model				
DNS	(Domain Name System) Builds a naming service system				
EGP	(Exterior Gateway Protocol) Provides routing information and does not look for the best route				
ftp	(file transfer protocol) Protocol for data transfer				
HELLO	The HELLO protocol obtains the route via the response time				
ICMP	(Internet Control Message Protocol) Provides information about the status and errors in the TCP/IP				
MAC	(Medium Access Control) Physical media access addresses				
SNMP	(Simple Network Management Protocol) Management protocol to adjust and manage network devices				
SOAP	Originally stands for Simple Object Access Protocol. This is a network protocol with which data is exchanged between systems and remote procedure calls are performed. SOAP is an industry standard of the World Wide Web Consortium (W3C). SOAP in the TCP/IP protocol stack:				
	Application	SOAP			
		HTTP	HTTPS	...	
	Transport	TCP			
	Internet	IP (IPv4, IPv6)			
Open access	Ethernet	Token bus	Token ring	FDDI	...

SMTP (Simple Mail Transfer Protocol)

Simple protocol for exchanging electronic mail.

Network protocol IP

The Internet Protocol is used as a network protocol directly via the actual network technology of layers 1 and 2. It provides the layers above it with an unreliable (uncontrolled) and connectionless datagram service.

Data is transferred in the form of data blocks (IP or Internet Packet) via connectionless communication. The protocol undertakes addressing and routing via gateways and routers, which connect the individual networks in an internetwork.

With IP, each network node can communicate directly with every other node. IP is not a hierarchical concept.

Formation of IP addresses

Address class	Class bit	Number of network bits	Valid address area	Notes
A	0	7	1 to 126	0 and 127 are reserved
B	10	14	128.1 to 191,254	255 is reserved for broadcast
C	100	21	192.0.1 to 223.255.254	
D	1110	–	224.0.0.0 to 239.255.255.254	is reserved for multicasting
E	1111	–	240.0.0.0 to 255.255.255.254	is reserved for multicasting

■ Terms relating to the Internet

Browser	A program that can be used to read and interpret HTML pages
CIX	(Commercial Internet Exchange) An agreement between network providers relating to the free exchange of data traffic
DNS	(Domain Name System) System that creates a computer hierarchy
FTP	(File Transfer Protocol) An Internet service for copying files
HTML	(Hypertext Markup Language) Metalanguage (or programming language) for creating information pages in text files, which can be viewed with browsers
HTTP	(Hypertext Transfer Protocol) This is a protocol for transferring data via a network. It is primarily used to load web pages from the Internet into a web browser
HTTPS	The HTTPS protocol is used to encrypt and authenticate communication between a web server and browser (client) on the Internet. The S stands for secure.
InterNIC, NIC	(Network Information Center) Allocation of globally unique computer addresses for the Internet. The international association is the InterNIC. Each country has their own NIC. The German NIC is located in Karlsruhe.
IP	(Internet Protocol) Basic protocol of the Internet
IRC chat	(Internet Relay Communication) A "live" discussion forum
MIME	(MultiMedia) An e-mail in MIME format can contain both ASCII text and binary data files. The sender creates a coherent mail file, which is unpacked by the receiver
PPP	(Point-to-Point-Protocol) Common TCP/IP protocol via a serial (telephone) line
SLIP	(Serial Line Internet Protocol) Alternative TCP/IP protocol via a serial (telephone) line
TELNET	Terminal connection to a remote computer in the network
URL	(Uniform Resource Locator) Language element of the HTML language. A graphics file, a program or a file on any computer on the Internet can be addressed via a URL.
WAIS	(Wide Area Information Service) Search for information on the Internet in indexed databases
WWW	(World Wide Web) A Hypertext-based information system on the Internet

Files in different formats can be copied and/or displayed in a browser with the help of URLs (URL: Uniform Resource Locator). The URL consists of the protocol, computer name, directory and file. The most common protocols are http, ftp, file and mailto.

Examples

http	http://www.rittal.de/index.html	An HTML file is loaded and displayed.
ftp	ftp://www.rittal.de/netz//EMV_IT.PPT	The EMV_IT.PPT file is copied to the hard disk.
file	file://C:/EMV_INFO.htm	The EMV_INFO.htm file is loaded from the local hard disk.
mailto	mailto: mustermann@www.rittal.de	An e-mail program is launched by the browser. The recipient's address is assigned.

Domain Name System (DNS)

DNS assigns logical names to all network computers that represent the numerical network addresses. The entire address space is divided into domains (areas) on the Internet, which are each managed by a computer used specially for this purpose, the Domain Name Server.

Name servers are computers or programs, which manage information about the structure of the hierarchical address space. Each name server is only responsible for the domain

allocated to it and maintains additional connections to neighbouring name servers. It can forward messages to other name servers via these external contacts when the recipient of a message is located in a different domain. Name servers resolve symbolic addresses into network addresses. In doing so, interpretation takes place from right to left. The broadest subdivision therefore appears first of all at the far right of the address. Usually double-digit country codes or user groups are distinguished.

■ Glossary

ASHRAE

- Wikipedia: The American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE) is a professional association for all employees in these sectors in the USA. The association's headquarters are in Atlanta. It was founded in 1894 originally as the American Society of Heating and Ventilating Engineers (ASHVE). In 1954 the name was changed to the American Society of Heating and Air-Conditioning Engineers (ASHAE). The organisation's current name comes from the 1959 merger with the American Society of Refrigerating Engineers (ASRE). The ASHRAE Handbook is a four-volume reference book on climate control technology. One of the volumes is updated each year. ASHRAE also publishes standards and guidelines relating to climate control technology, which are referenced in building codes.

Bypass

- Wikipedia: Bypass means: Bypass (digital systems), circumventing the pipeline in a CPU

CRAC

(Computer Room Air Condition)

- Air recirculation unit in the data centre

Customised Data Centre

- Tailored data centre solutions in a standardised format

DCIE

- Data Centre Infrastructure Efficiency.
The DCIE rates the energy efficiency level in the data centre as a percentage.

DCIM

- Wikipedia: The abbreviation stands for Data Centre Infrastructure Management, a discipline partly supported by software for green IT data centre planning.

Rectifier

- Wikipedia: Rectifiers are used in electrical engineering and electronics to convert alternating current to direct current. Along with inverters and converters, they form a power converter module. To dampen alternating components, a rectified voltage is usually smoothed.

Rack unit

- Wikipedia: A rack unit, abbreviated to U or RU, is a unit of measurement that describes the height of equipment designed to be mounted in a rack. Equipment with a rack unit height of one is described as "1 U", two rack units as "2 U" and so on. 1 U is 1.75 inches (44.45 mm) high. Equipment measured in rack units is designed to be mounted in 19" racks. The width of the 19" front panels is 482.6 mm.

IT Infrastructure Library (ITIL)

- Wikipedia: The IT Infrastructure Library (ITIL) is a set of best practices in the form of a series of publications relating to the implementation of IT service management (ITSM). It underpins the International Service Management Standard for IT business processes. The set of guidelines and definitions describes the required processes, organisational structure and tools for managing an IT infrastructure. The ITIL focuses on IT companies delivering added value to customers. For this purpose, the planning delivery, support and efficiency optimisation of IT services are considered in terms of customers' needs, as these are relevant factors in achieving a company's business objectives. In Germany, the contents are updated and improved by itSMF Deutschland e. V. (IT Service Management Forum Germany), which also provides a knowledge and information exchange platform to drive IT industrialisation forward.

IT Baseline Protection Catalogue

- Wikipedia: The IT Baseline Protection Catalogues (before 2005: IT Baseline Protection Manual) are a collection of documents from the German Federal Office for Security in Information Technology (BSI) that serve to detect and combat security-related weaknesses in the IT environment (IT cluster).

Monitoring

- In this context: monitoring, control and documentation using complex software.
Wikipedia: The word monitoring is an umbrella term for all types of immediate systematic detection (logging), observation or monitoring of an operation or process using technical aids (for example, long-term ECG) or other surveillance systems. Regularly repeating observations is a central element of the respective programme, as only in this way can conclusions be drawn based on the comparison of results (see also longitudinal study). One function of monitoring is intervening in an observed procedure or process if this does not take the desired course and/or specific thresholds are not met or are exceeded (see also control engineering). Monitoring is therefore a special type of logging.

MS

- Supply/medium voltage

MSHV

- Medium-voltage distribution centre

NSHV

- Low-voltage distribution centre

PDU

- Power Distribution Unit

Photovoltaics

- Wikipedia: The direct conversion of light energy, usually from the sun, into electrical energy using solar cells.

Power Management System

- A Power Management System ensures transparency of energy consumption and quality in the data centre and the availability of power distribution. It can be part of the Data Centre Management System. At the same time it is the basis for optimising energy costs and consumption.

Precision climate control

- Functionality and operational reliability in relation to heat dissipation

PUE

- Power Usage Effectiveness. Total power consumption of the data centre/power consumed by the IT equipment. The PUE value determines the ratio between the power supplied to the data centre and the power consumed by the computers.

Redundant

- Wikipedia: The term “redundancy”, adjective redundant, (Latin redundare “to overflow, to be abundant”) refers to:
 - a state of overlap or abundance in terms of excess, see surplus product.
 - redundancy (technology), the availability (mostly for safety reasons) of multiple technical resources with an identical or comparable function, which are not required during fault-free, normal operation.

RiMatrix

- System components that are standardised and fully compatible with each other for the assembly, expansion and modification of new, existing and constantly growing company data centres. Consists of prefabricated modules to install in system-tested security rooms, standard aisle compartments or containers.

RiMatrix S

- The first completely preconfigured, standardised data centre – pre-certified by TÜV Rheinland.

RiMatrix S Selector

- Configurator for designing a complete, customised RiMatrix S data centre. Can be found on the Rittal homepage at www.rittal.com. Also available as an App.

Rittal – The System.

- Products as a modular, coherent system platform, which considerably speeds up steps such as designing, configuring, modifying and commissioning thanks to maximum system compatibility, thus increasing efficiency and convenience.

TDP

- Thermal Device Power

Tier®

- Levels of availability (tier). The US Uptime Institute has defined a number of availability classes for data centres; these are referred to as the Industrial Standards Tier® Classification.

TS 8 server platform

- TS 8 is at the heart of the rack-optimised design at Rittal. The TS 8 server platform has been further optimised in the latest TS IT rack from Rittal.

UPS

- Uninterruptible power supply. In the standardised RiMatrix S data centre from Rittal, an integrated UPS system ensures a reliable power supply. The modular, uninterruptible power supply functions in accordance with the n+1 redundancy principle using consistent parallel architecture.

UV

- Sub-distribution

Availability

- The availability of an IT infrastructure is calculated as follows: $\text{Availability} = (1 - \text{downtime} / \text{productive time} + \text{downtime}) \times 100$. An IT system is deemed to be available when it is able to carry out the tasks for which it was designed. Availability is expressed in percent and is split into availability classes.

Inverter

- Wikipedia: An inverter is an electric device that converts DC voltage into AC voltage; in other words DC current into AC current. Along with rectifiers and converters, inverters form part of the power converter module.

ZUCS

- Zero U-space cooling system. This is used as a climate control system for standard Rittal RiMatrix S data centres. Every server rack has its own heat exchanger and fan in the raised floor. The concept is known as a zero U-space cooling system (ZUCS), as the cooling elements do not take up any space in the rack. If a ZUCS fails, climate control for the entire module continues to be provided thanks to n+1 redundancy.

■ Bibliography

BITKOM publications

Bundesverband Informationswirtschaft
Telekommunikation und
neue Medien e. V.

(Federal Association for Information
Technology, Telecommunications and
New Media)

Albrechtstraße 10A

10117 Berlin

www.bitkom.org/de/publikationen

- Reliable Data Centre
Guide, December 2013
- Series on Environment & Energy,
volume 2: Energy Efficiency in the
Data Center
A Guide to Planning, Modernization
and Operation of Data Centers

Bundesamt für Sicherheit in der Informationstechnik (Federal Office for IT Security – BSI)

Godesberger Allee 185 – 189

53175 Bonn

www.bsi.bund.de/EN/

- Information from the Internet
Department B 23, Public Relations
and Press

TÜV Rheinland

TÜV Rheinland AG

Am Grauen Stein

51105 Cologne

<http://www.tuv.com/en/uk/>

www.tuv.com/consulting

- Information from the Internet:
Criteria catalogue for auditing
server rooms and data centres

LEXIKON DER DATEN- KOMMUNIKATION (Data Communication Lexicon)

MITP Verlag GmbH

Königswinterer Str. 418,

D-53227 Bonn

- Klaus Lipinski (ed.)

LEXIKON DER KOMMUNIKA- TIONS- UND INFORMATION- TECHNIK

(Communication and Information Technology Lexicon)

Hüthig GmbH

Im Weiher 10

D-69121 Heidelberg

- Niels Klußmann

Microsoft TechNet Library

Microsoft Corporation

One Microsoft Way

Redmond, WA 98052-6399

USA

[http://http://technet.microsoft.com/
en-gb/en-uk/library/bb432646.aspx](http://http://technet.microsoft.com/en-gb/en-uk/library/bb432646.aspx)

- Determining cost of availability

Beuth Verlag GmbH

Am DIN-Platz Burggrafenstraße 6

10787 Berlin

- The standards mentioned:
IEC, VDE, DIN

Rittal GmbH & Co. KG

Postfach 1662, 35726 Herborn,
Germany

Technical presentations and specialist
publications (white papers)

- Modern data centre infra-
structures (SME interview by
Bernd Hanstein)
- Data centre of the future
(Bernd Hanstein)
- Data centre challenge
- Energy-efficient IT climate
control (Daniel Luther)
- Power distribution in the data
centre
- Power back-up in the data
centre using modular
UPS systems (Jörg Kreiling)
- Sensor network for rack and
room monitoring
- RiZone – The Rittal management
software for IT infrastructure
(Bernd Hanstein, Markus
Schmidt, Thorsten Weller)
- Fire extinguishing systems in the
data centre (Alexander Wickel)

Rittal – The System.

Faster – better – everywhere.



ENCLOSURES

POWER DISTRIBUTION

CLIMATE CONTROL

TS IT – added value included

1 Individual use

The ideal basis for virtually all network and server technology requirements

2 High load capacity and variable internal installation

A load capacity of up to 1,500 kg with no need for tools to adjust the 19" mounting levels

Alternative mounting dimensions easily achieved with lateral offset (21", 23", 24" possible)

3 Tool-free installation

System accessory mounting using new, time-saving snap-in technology (available for component shelves, cable conduits, etc.)

4 Intelligent cable management

Multi-functional roof for side cable entry, ensures maximum user-friendliness and free air flow for active components

5 Side panel fast assembly

Divided side panel with quick-release fasteners, integral lock and internal latch

6 Impressive door concept

Glazed door for high-performance server applications with LCP climate control or vented doors for climate control

7 Divided rear doors

Divided rear doors from a height of 1,800 mm for space-optimised positioning

8 Intelligent accessories

Simple and quick selection of system accessories using the new TS IT concept

9 Integrated added value with 19" system

Direct, space-saving, clip-on mounting of the new Rittal rear PDU busbar in the zero U-space

Toolless integration of cable management and Dynamic Rack Control at the front

10 Simple positioning

Labelling of the rack units and pitch pattern in the depth for simple adjustment of the distance between 19" levels

Previously published:

1

2013

Standard-compliant switchgear and controlgear production

Application of IEC 61 439

2

2013

Enclosure and process cooling

3

2014

Technical aspects of enclosures

4

2014

The world of IT infrastructures

Background information and decision-making criteria

Rittal – The System.

Faster – better – everywhere.

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

Normal fee 12,50 €

You can find the contact details of all Rittal companies throughout the world here.



www.rittal.com/contact



FRIEDHELM LOH GROUP