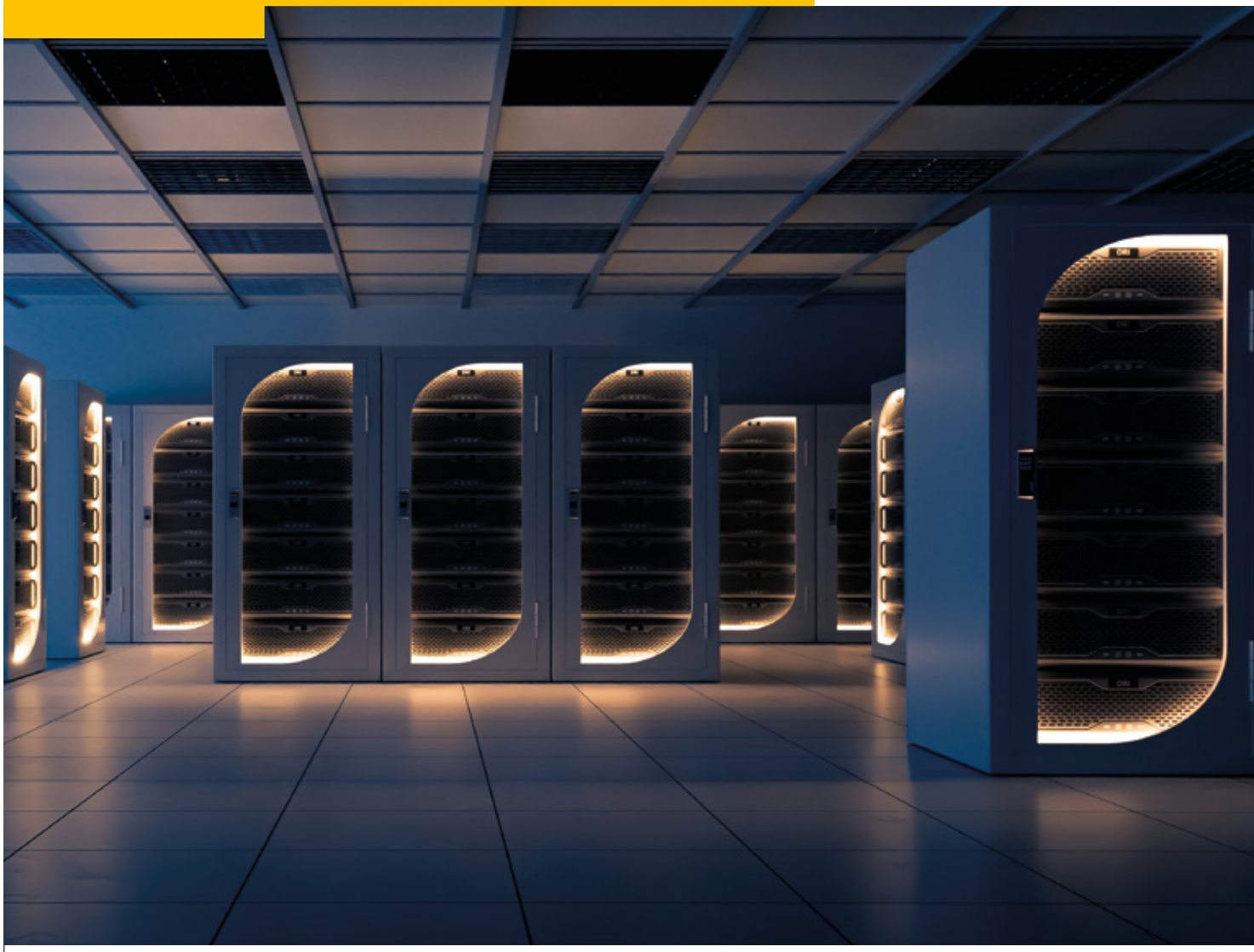
Data centres

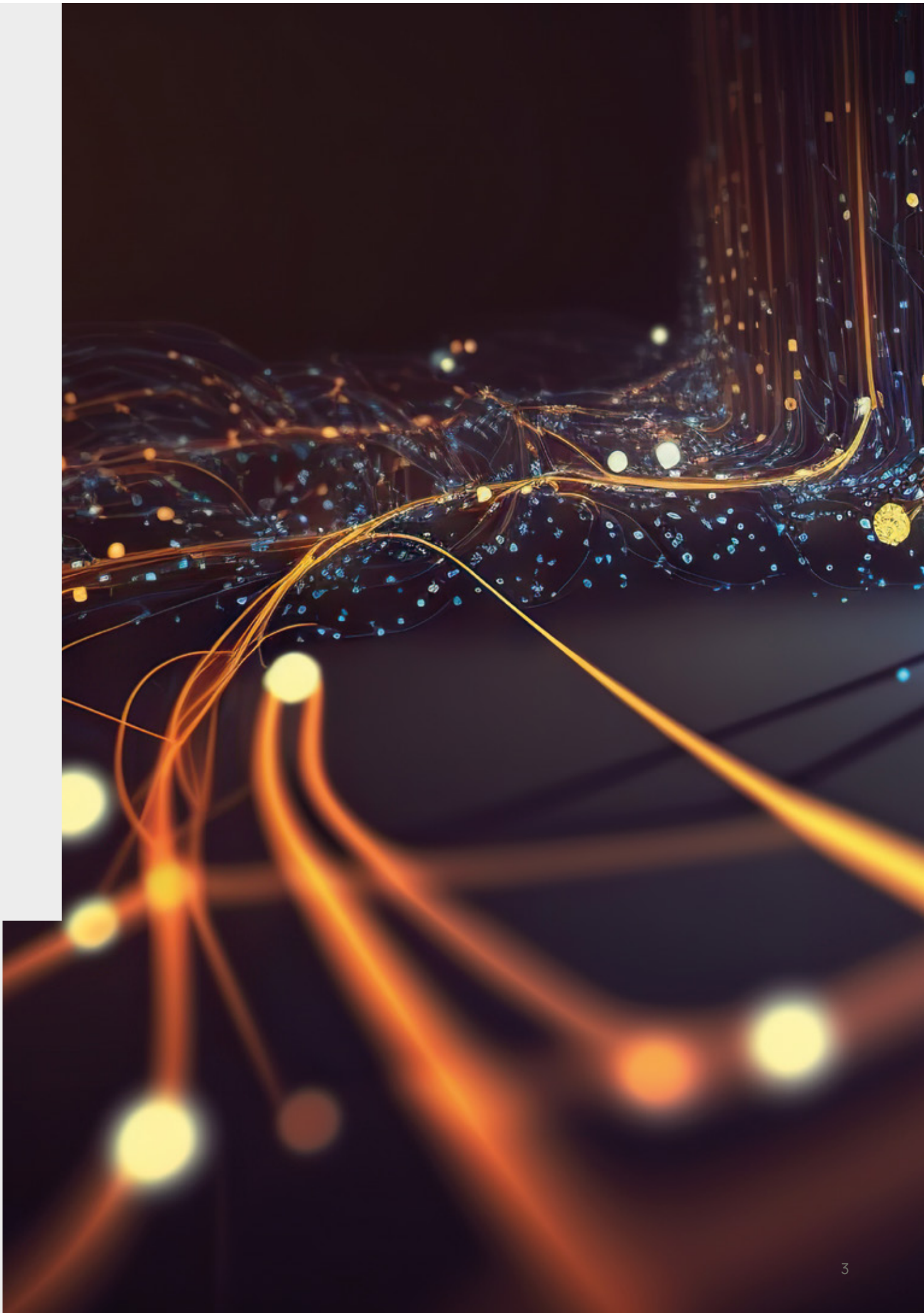
Safety, maximum availability, and profitability



Design the future of energy

BENDER

Table of content

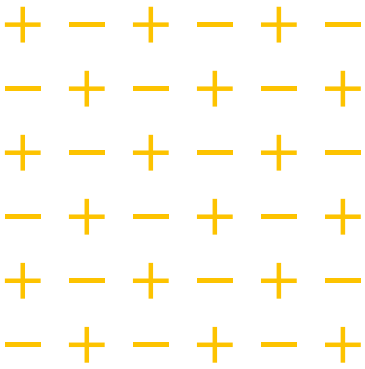


Safety, maximum availability, and profitability

Protecting data
Data protection is one of the most important requirements for data centres. Therefore huge efforts are made so that servers will not be compromised. Where the protection of data is concerned, it is however not sufficient to focus on the IT-infrastructure alone. Many additional aspects also need to be considered, starting with the power supply. As a safeguard against power outages, data centres are equipped with an alternative electricity supply (e. g. diesel generators) whose purpose is to guarantee uninterrupted operation of servers and other essential components. However if one of these components fails due to a technical fault, USP (uninterruptible power supply) alone will not suffice. A number of measures must be taken to prevent outages and ensure high availability 24/7/365.

Preventing outages
Data centres are highly complex installations. They consist of IT components such as servers and memories and other electrically operated parts of the installation which ensure trouble-free operation of the IT-components. These include among others the cooling system but also the power supply with all the components needed to provide electricity, such as bus bars, cables, and other parts. The failure of only one of these components could result in the failure of further parts of the installation. In an extreme case, a chain reaction effect could result in the entire data centre shutting down, which would mean considerable costs and possibly even data loss. It is imperative that such a scenario be prevented.

Ensuring reliable operation
Expert staff for data centres is scarce. There is fewer and fewer personnel available to monitor and keep up the highly complex operation of data-centres. To ensure smooth operation of the data centre, however, the staff needs to be able to easily oversee and assess the condition of the overall installation at any time. In the event of an error, the staff must be able to quickly recognise, to localise and to eliminate it. Otherwise there is the risk of further failures that will result in costs and, in the worst case, in data loss.



Electrical safety, availability, and DIN EN 50600

The European standard DIN EN 50600 or ISO/IEC TS 22237 (often dubbed data centre standard) defines how a data centre shall be designed in order to ensure reliable operation. It stipulates requirements for the structural design of buildings, power supply, air-conditioning, wiring as well as for the safety systems, and it describes requirements for the operation of these centres. DIN EN 50600 distinguishes four availability class ratings for data centres. Depending on the availability class, different measures shall be taken to maintain operation.

Availability class (Av. Cl.)	Av. Cl. 1	Av. Cl. 2	Av. Cl. 3	Av. Cl. 4	Av. Cl. 4 advanced
Availability	Low	Medium	High	Very high	
DIN EN 50600-2-2 Power distribution	No redundancy	Component redundancy	Concurrently maintainable	Fault-tolerant (Transfer switching equipment)	
Distribution paths	One **N**	One **N+1**	Several **2N**	Several **2N**	
DIN EN 50600-2-3 Environmental control	—	No fail-safe operation	Component redundancy	Concurrently maintainable	
Distribution paths	—	One **N**	One **N+1**	One **N+1**	Several **2N**

Availability class 1:
Stipulates only **low requirements** for the availability of a data centre. Operation can be interrupted at any time by unplanned maintenance work or technical faults.

Availability class 2:
Data centre availability is increased by **redundant components**. Interruptions of the operation due to maintenance work can be planned. Technical faults can still cause unpredictable downtimes.

Availability class 3:
Data centre maintenance is possible without interrupting operation. Most technical faults do not lead to a shutdown. This is achieved by employing **redundant systems and additional preventive measures**.

Availability class 4:
Operation can be maintained at any time even in the case of faults or technical failures. Interruptions of operation are practically excluded. This degree of availability is achieved by **extensive preventive measures**.

Bottom line:
Data centres which are operated in accordance with availability classes 3 or 4 require additional preventive measures apart from the redundant systems. This applies also to the power supply system which must not fail suddenly or randomly. **Faults in the power-supply or wiring therefore must be recognised early on and reliably** in order to prevent downtimes and to maintain operation of the data centre.

IEC 60364-6

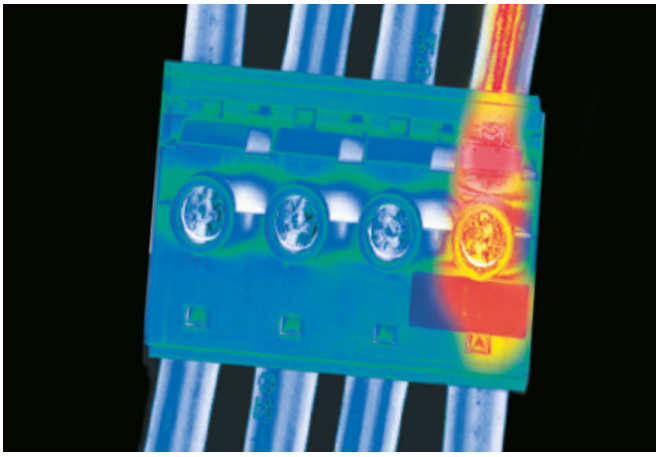
In the long run no electrical installation will run without faults. Faulty electrical devices or installations constitute a danger to human beings. To prevent accidents due to electric shock, electrical installations shall be checked regularly, and detected defects shall be corrected immediately. If there is an imminent danger that cannot be eliminated, operators shall ensure that the respective electrical installation or equipment will not be used in its defective condition. The timelines for the **periodic verification** of the electrical installations shall be defined in such a manner that any defects that may occur can be detected in good time.

For the verification to be carried out and defects to be eliminated, electrical installations and equipment must be switched off and separated from the power supply system. This requires work and takes time. In a data centre that must be available 24/7, interruptions of this type are unwanted. However, operators can avoid a shutdown for the verification of installations and equipment by employing technical and organisational measures as well as measures to protect people.

The installation of a measuring device that substitutes the work-intensive verification of installations and equipment may constitute such a safety measure.

Protection against fire

In Germany one in three fires can be attributed to a faulty electrical device or a fault in an electrical installation. Preventing such fires is in the interest of every data centre operator, since interruptions of operation, damage to property or injury to people due to fire incidents may undermine the very existence of their business. Even the tiniest electrical faults can cause a fire, insulation faults and the consequent leakage currents being the main cause of fires in electrical devices or installations. These root causes may be due to insufficient insulation, mechanical damage to the connection lines of devices, crumbly insulations of devices or lights due to continuous exposure to heat, humidity, and dirt. If a fire is caused by such a fault, cost-intensive failures or installation downtimes are the result, possibly even injury to people, damage to property and the environment, and, last but not least, expensive maintenance operations.



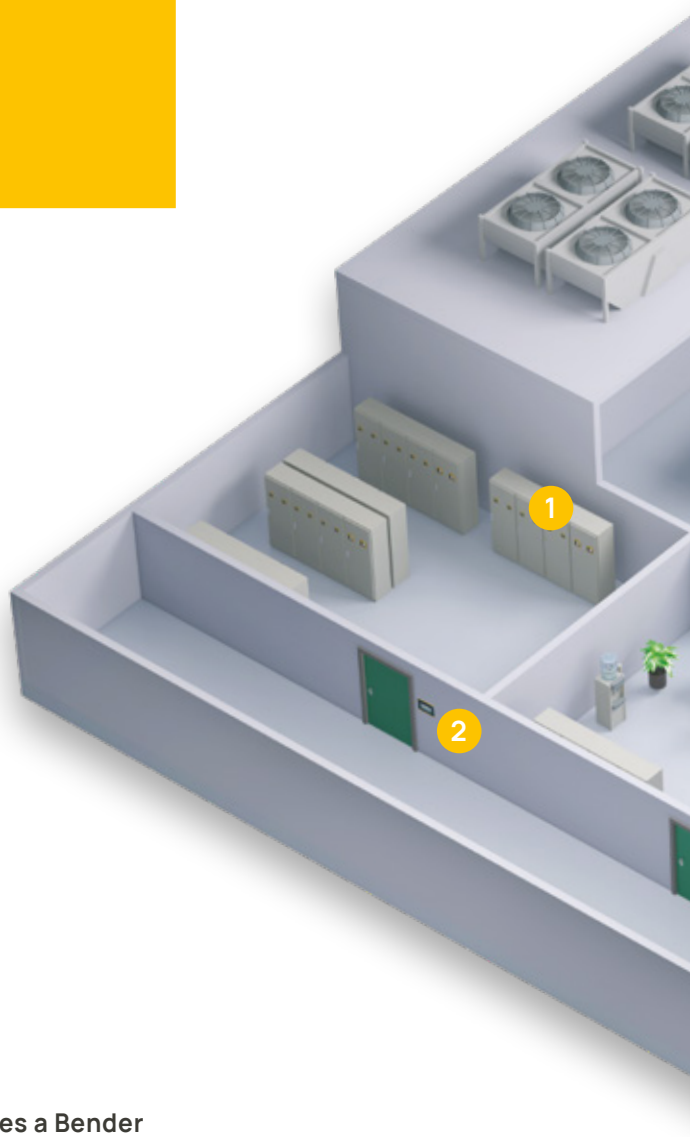
Overload of the neutral conductor

Detecting insulation faults and the concomitant leakage currents in good time is crucial in preventing fires in data centres.

More safety for data centres

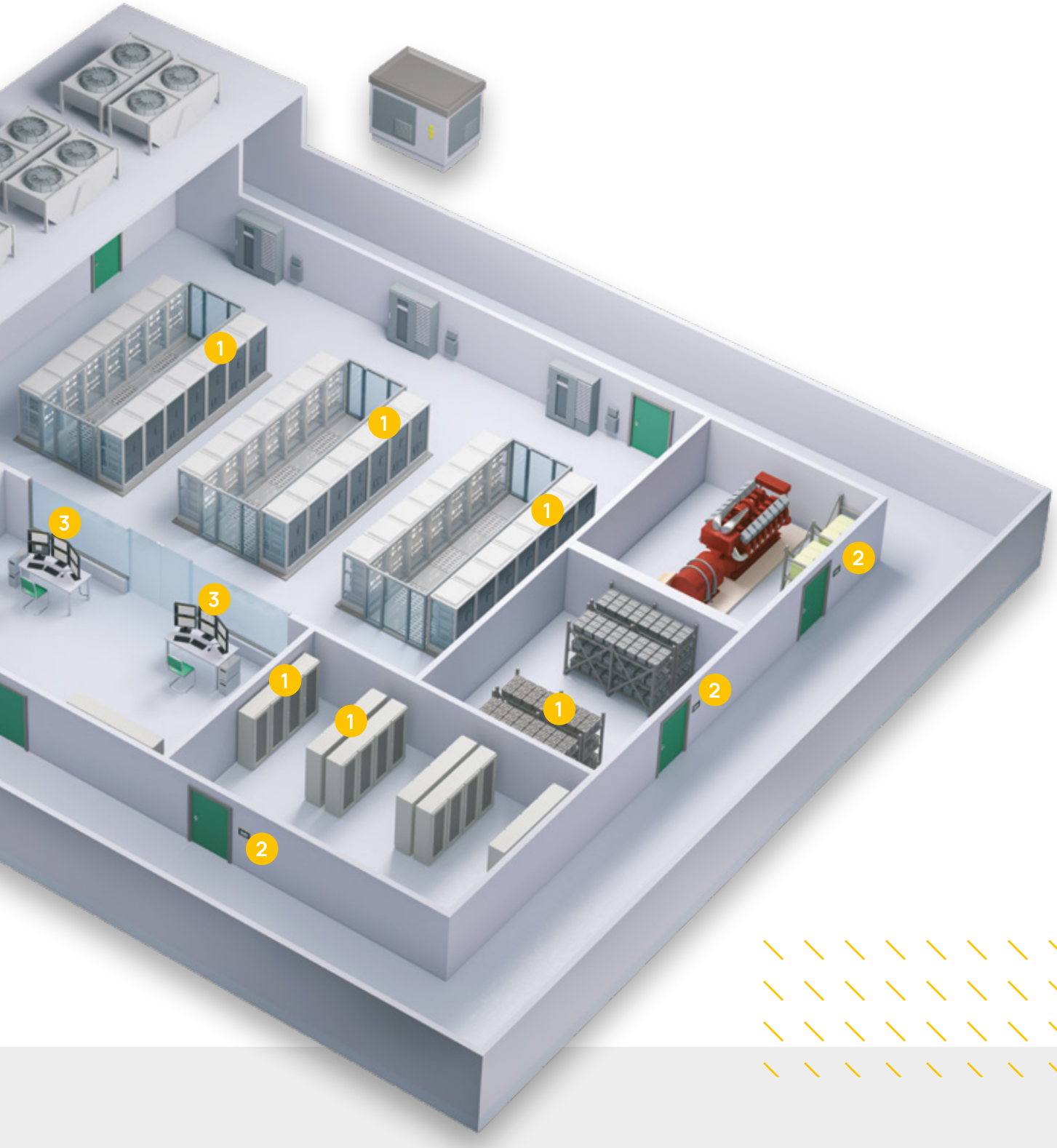
Preventing faults and downtimes through continuous monitoring (condition monitoring)

How can the operation of data centres be economically efficient and how can high availability be ensured without having to renounce on safety of the installation and personal protection? **To satisfy the requirements for safe operation, continuous monitoring (condition monitoring) of the entire electrical installation (servers, air conditioning, infrastructure) including power supply and wiring is indispensable. If data centres are to be operated in accordance with availability classes 3 or 4, measures need to be implemented that preclude interruptions of operation due to maintenance work or failures**. For such cases it is useful to **employ a condition-monitoring-system with residual-current monitoring**. This system continuously checks the status of the entire electrical installation and detects faults reliably and quickly before an unscheduled interruption of operation would be the result. Moreover, a residual-current monitoring system can locate faults with ease. This provides operators with the opportunity to react quickly and in a targeted manner to correct faults and avoid critical operating conditions.



How does a Bender condition-monitoring-system work?

Condition monitoring systems consist of sensors such as measuring-current transformers, evaluation units, and the condition monitor itself (see figure). The sensors (e. g. of the Linetraxx® series) continuously measure the residual current between lead and return lines. When a fault occurs, they measure a residual current, which is then recorded and analysed by the evaluation device (e.g of the RCMS series) and passed on via the existing interfaces (e. g. Profibus) to the condition monitor (e. g. COM465 or CP9…-I). Faults in the electrical installation are either displayed on a monitor via an internet browser (COM465) or on a condition monitor with display (CP9…-I). Integration via the Bender cloud solution POWERSCOUT® is possible, too. The condition monitoring system operates continuously 24/7. Additional analysis functions serve to assess the condition of an installation over a longer period of time. This provides staff with the best possible overview over the electrical installation's condition at any time.



Sensors and evaluation units

Condition monitor

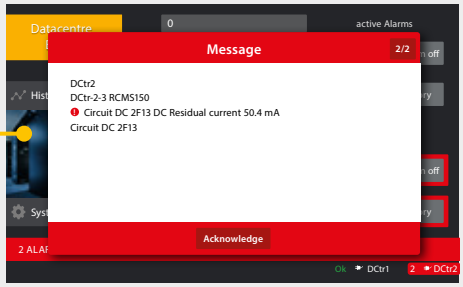
Powerscout

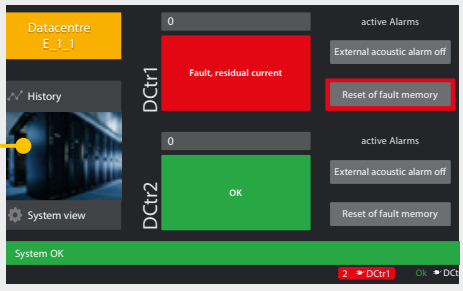
Advantages offered by Bender condition monitors

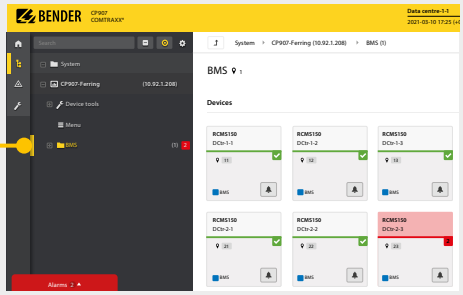
The principle benefit is prevention. **As the measurements are carried out continuously, occurring faults and critical operating conditions can be detected early on, a long time before a downtime is imminent**. At the same time, the danger of electrical fires is reduced and protection of people improved, since an alarm message is given when fault currents that pose a hazard to people occur. The continuous fault-current monitoring is also a recognised safety measure that permits forgoing an R_{iso} measurement during the periodic verification. With this approach, individual devices, parts of the installation, servers or server racks need not be switched off. Also the work involved in the manual R_{iso} measurement (including the administrative part) is reduced.

Not only can continuous residual current monitoring make the data centre more profitable but it can also lead to safer operation.

Examples for status displays shown by a Bender condition-monitoring-system.







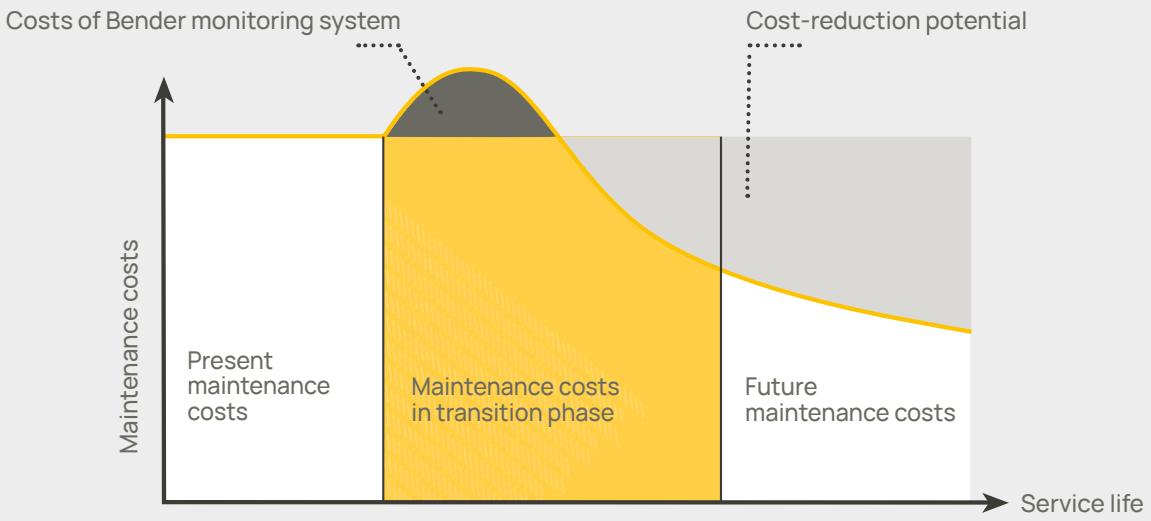
Advantages at a glance:

- Continuous monitoring of an installation
- Easy overview
- Error detection early on
- Localising of errors
- Effort and cost for periodic verification decreases
- Danger of electrical fires is reduced

For you, the operator of a data centre this means:

- Lower risk of sudden and unplanned downtimes
- Improved availability and profitability
- Increased protection of people and installations
- Fewer man-hours needed, reduced costs

Investment in a Bender condition-monitoring-system will mean huge advantages for data centre operators and will pay off after a relatively short time.



Intelligent planning for small and big data centres

The bigger a data centre, the bigger and more complex is also the entire electrical installation. The greater the number of monitored installation parts, the greater the overview, the better the localisation of occurring errors, and the quicker their correction. **Already when a data centre is planned, attention must be paid to the question how finely detailed a condition-monitoring system should be designed so that it will meet both the operational needs and the requirements under the applicable standards, especially DIN EN 50600 or ISO/IEC TS 22237 and the stipulated availability classes (see page 6).**

Automatic error search for higher availability
Electrical devices are subject to normal wear and tear and can become susceptible to failure as their service life increases. Rapid error detection prevents long down-times and reduces hazards to installations and people. **Combining a condition-monitoring-system with an automatic error-localisation system makes sense.** This can be taken into account already during the planning stage.

Profitable and reliable

Bender has decades of experience in the area of electrical safety. We offer practical solutions that pay off and lead to increased safety. Please do not hesitate to contact us if you have any questions. You can find the responsible contact persons here:
www.bender.de/kontakt/vertrieb-deutschland

Competent service for maximum safety and high availability of your data centre

Further information on our data-centre solutions is available here:
www.bender.de/loesungen/rechenzentren

bender.de

Bender GmbH & Co. KG

Londorfer Straße 65
35305 Grünberg
Germany

Tel.: +49 6401 807-0
info@bender.de
www.bender.de

2202en / 06.2023 / © Bender GmbH & Co. KG, Germany – Subject to change! The specified standards take into account the version valid at the time of printing.

BENDER