RITTAL Pty Ltd · 130-140 Parraweena Road · Miranda NSW 2228 · ABN 79 000 439 976

Thursday, April 26, 2012
Sydney New South Wales

TECHNICAL ARTICLE

FOR IMMEDIATE RELEASE

RITTAL Pty Ltd
HEAD OFFICE
130-140 Parraweena Road
MIRANDA NSW 2228
☎ 1800 350 665
1800 046 102
customerservice@rittal.com.au
www.rittal.com.au

CONTACTS
Troy Gersback
Marketing Coordinator - Australia & New Zealand
P: +61 2 9526 4904 | M: +61 400 873 917 | F: +61 2 9525 2888
tgersback@rittal.com.au

FLEXIBLE SECURITY IN DATA CENTRES: IT SECURITY MADE TO MEASURE

In almost every sector, be it financial management, logistics or mechanical engineering, critical business and production processes – taking in everything from enterprise resource planning to the telephone system – are IT-based. Failure can result in serious economic losses. Therefore, a risk prevention concept for IT structures is an essential part of the IT planning process. This is where data centres come to the fore. If IT is the central nervous system of modern companies, the data centre is their spinal cord. If this is damaged, it can paralyse all of a company's processes. However, managers also have to keep an eye on the price/performance ratio when it comes to risk prevention.

Data centres are faced with numerous risks, including fire, smoke generation, water damage, power failure and overheating. Other disruptive factors include cyber crimes and unauthorised third-party access to data centre rooms. Given the wide variety of threats, a comprehensive security concept plays a key role in all data centre planning and modernisation projects.

COSTS VS. BENEFITS

The cost of risk prevention must always be commensurate with the potential economic loss or damage mitigation. Potential risks, such as production downtimes, must always be weighed against the business process target. This is the full set of requirements that the business operations place on IT. The ratio of business process target to tolerable downtimes and potential damage indicates which operational losses are acceptable and which are not. This qualification and quantification of risks within the data centre infrastructure is not designed to protect solely against business losses. A holistic view of the entire data centre is also indispensable for planning. This is the only way to ensure that protection against fire, unauthorised access and overheating is implemented in a way that is demand-based and therefore cost-effective. Consequently, the first step is to define the availability requirements for IT. During subsequent implementation, data centre planners can use the Tier classifications of the Uptime Institute for guidance. The demands for power and cooling in particular are specified in four classes – Tier I to Tier IV – depending on the availability requirements. Tier IV specifications for particularly business-critical core processes achieve maximum availability of 99.995 percent.

SECURITY ROOMS OF ALL SIZES

Modular security rooms are the protective shell of data centres. They accommodate both IT devices, such as servers, switches and data memories, and the infrastructure. Regardless of whether a company has a high-security data centre or racks located in an office environment, various protection concepts comprising different resistance classes are available tailored to the exact requirements of the business processes. The concepts range from basic protection through to high-availability security rooms with minimal downtime tolerances. To be able to respond adequately to company needs, cost-effective concepts are modular and can be tailored flexibly to the structural conditions and availability requirements, e.g. by opting for a room-in-room concept. State-of-the-art data centre concepts provide for separate accommodation of server enclosures on the one hand and the infrastructure, e.g. low-voltage distribution, UPS systems, etc. on the other. The individual "rooms" (data centre area / technology area) are designed and built as protection cells to meet precise requirements. For example, the server cell is designed to achieve high-availability protection, while the remaining technology is equipped with less expensive basic protection. These modular security cells are quick and cost-effective to dismantle and reassemble at a new location and thus offer a high level of investment security. The data centre can also be expanded at a later date as the enterprise's requirements grow.

IT safes are an alternative to server rooms and they offer comprehensive protection for critical servers. These small "suits of armour" present an interesting and cost-effective solution for small and medium-sized enterprises. They provide protection against physical threats and are available as modular Basic Safes. In addition to the physical shell, various configuration components for cooling, power supply, emergency power and monitoring transform the safe into a complete compact data centre.

The micro data centre developed by Rittal in cooperation with IT service provider Bechtle for SMEs goes one step further. In this joint concept, Rittal supplies the entire infrastructure and physical security technology – Basic Safe as the enclosure, climate control, fire alarm and extinguisher system and energy distribution. Bechtle is responsible for the actual IT devices and software integration. The micro data centre is supplied as a complete package. It is essentially a plug-and-play system that is available in three variants with different levels of system redundancy. With a footprint of just 1 m^2, micro data centres offer sufficient computing power to supply several thousand SAP users at the same time.

PROTECTION AGAINST FIRE, WATER, SMOKE

Fire, water and smoke pose a fundamental risk for data centres. A multifunctional safety concept is needed when a data centre is taken into operation. A fire protection concept alone is insufficient.

Water is also a source of risk to IT that should not be underestimated. Most damage is usually caused by the water used to extinguish a fire. Therefore, data centres should remain watertight for long periods and should also offer protection against standing water. Watertightness in line with EN 60529 (IP standard) is a minimum requirement.

The prevention of smoke build-up must also be factored into any safety concept. The substances in flue gases mean they are often corrosive and can quickly attack and damage IT systems, thus significantly reducing the time till system failure. What's more, for smoke damage to occur, the fire does not even have to be close to the data centre. Certified flue gas-tightness to DIN 18095 or EN 1634-3 is essential.

For the prevention of fires in data centres, the residual risk must be reduced through additional measures. Early fire detection systems are designed to prevent fire damage from occurring in the first

place. They continuously extract air from the server enclosures at risk and the surrounding area and can detect even the smallest smoke particles. Due to the high air speeds in climate-controlled server rooms, the systems must be sufficiently sensitive. In this way, fires are detected and reported very early on (pyrolysis phase). At higher concentrations, the data centre is extinguished using non-toxic extinguisher gases. Unlike foam or powder, gases such as Novec 1230 do not soil or damage the sensitive IT equipment. The extinguisher gas exhibits a five-day atmospheric lifetime and is not harmful to people.

TRUST IS GOOD, CONTROL IS BETTER

It is the stuff of nightmares for data centre administrators – a leak in the liquid cooling system in an area of poor visibility, a smouldering fire that is detected much too late, or impermissibly high temperatures in the server enclosure. With rack-based cooling equipment, even a rack door left open unintentionally can cause considerable damage if the cooling output is affected or if unauthorised persons gain access to the valuable and sensitive hardware. In cases like these, appropriate countermeasures must be taken quickly to prevent or at least minimise damage. Early detection of the problem in question is a basic requirement in minimising response times. This is where a monitoring system with far-reaching alarm workflow concepts comes in to ensure the seamless operation of the IT infrastructure. Sensor-based solutions, such as CMC III from Rittal, are ideal for monitoring situations like these. The sensors constantly control ambient parameters, such as temperature, pressure and humidity, and immediately report any deviations. The RiZone management software, which is based on the CMC, goes one step further still. It uses intelligent interfaces to incorporate building control systems and server management, thus providing a holistic view of the data centre. The relevant officers are informed automatically as soon as a measurement in the data centre deviates from the defined parameters. If required, countermeasures can also be triggered automatically. This solution improves both safety and efficiency. For instance, the climate control can be configured so that the cooling output is based on the actual cooling requirements at specific locations.

SAFEGUARDING AGAINST POWER FAILURE

Suddenly the lights go out – even in Australia, power failures are surprisingly frequent. As even minor fluctuations or voltage peaks can have serious consequences for sensitive hardware, uninterrupted power supply (UPS) systems are an essential part of state-of-the-art data centres. They make it possible to bridge shorter downtimes and act as a kind of "filter" to absorb fluctuations and deliver only the exact amount of power required by servers.

UPS systems are classified to EN 50091-3 and EN 62040-3. Systems in quality class 1 VFI-SS-111, example models PMC 40 or PMC 120 from Rittal, deliver ultimate protection against power failure. Redundancies are recommended for UPS systems to safeguard availability. The above-mentioned Tier classes of the Uptime Institute provide planners with suitable guidelines. Modular UPS systems based on n+1 redundancies have proved their worth in practical applications. Purchasing and operating costs are lower. The use of two separate UPS systems is recommended for extremely high availability requirements.

Due to rising energy prices, efficiency is also an important factor. As the characteristic efficiency indicator for UPS, the level of efficiency expresses the ratio of power supplied to power output. A value of 95 percent is excellent. While UPS provides immediate assistance in case of power failure, data

centres must also be safeguarded against longer-term downtimes through autonomous emergency power generators. These mains backup systems – usually diesel generators or fuel cells – bridge longer power failures before the USP's batteries run out.

WHEN THINGS HOT UP – DATA CENTRE CLIMATE CONTROL AS PART OF FAILURE PROTECTION

Heat is not only caused by external fire – it also results from the heat dissipated from powerful data centre servers. With a low thermal load of up to 800 watts per square metre, for example, one climate control system per air circulation system is sufficient. However, this is not enough for powerful servers such as blades, which can generate over 20 kW of waste heat per rack. This is where liquid-cooled, rack-based climate control units, such as the Liquid Cooling Package (LCP) technology from Rittal, can prevent heat from destroying computers. These special cooling systems can also be used without a raised floor. This way, cooling output of up to 60 kW can be achieved per rack. Cold air is blown from the bayable air/water heat exchanger through slotted side panels directly in front of the servers into the enclosure. This type of cooling output is only required in exceptional circumstances and in case of high computing power in individual racks. These rack-based cooling units often also provide a "row-based" solution in which cool air is blown in a contained aisle. Climate control via a conventional raised floor is another possible solution. Here, too, the cooling requirements, including appropriate redundancy, must be factored into the planning. A modular approach based on the waste heat and spatial requirements prevents hot spots and server failures on the one hand and costly overdimensioning of the climate control system on the other.

Another very efficient option is to use geothermal energy. By pumping water into the ground it can return to the surface at a maximum temperature of 14 degrees Celsius. This achieves an excellent power usage effectiveness value of 1.06. Overall, climate control in data centres can be realised with clever and cost-effective solutions without jeopardising reliability.

CONCLUSION

Although you can never achieve 100 percent protection, careful planning enables effective risk prevention. It is therefore important to ensure that the corresponding certifications are in place in key safety areas. A holistic view of the IT landscape with a detailed analysis of the physical risks is essential. These are important elements in comprehensive risk management and make an important contribution to ensuring the availability of business-critical processes. The efficiency and scalability of solutions must also be taken into account. In view of dwindling budgets coupled with growing requirements, it must be possible to flexibly extend and reorganise the data centre infrastructure while keeping operating costs low. When investing in data centre security, it therefore always pays dividends to look ahead to the future and opt for expandable concepts. If operators take a structured and considered approach to data centre reorganisation, investments in data centre security will pay off the first time an incident is prevented at the very latest.

COMPANY BACKGROUND

World leader in enclosure and IT infrastructure technology, Rittal continues to expand its product offering with the highest quality, German engineering. Since its inception in Germany in 1961, Rittal has grown from a leading supplier of industrial enclosure and climate control technology to be a provider of

complete data centre infrastructure. From racks, power, cooling, remote monitoring and physical security, Rittal is paving the way in data centre technology to create the most energy efficient, secure, future proof data centres on the market.

Rittal Australia & New Zealand has over 100 employees with service and delivery centres in all major main land capital cities (excluding Darwin). Our modification capabilities ensure the perfect fit solution no matter what your application. Rittal Australia & New Zealand is backed by a worldwide team of 10,000 committed staff, 10 production facilities and 63 international subsidiaries.

Rittal is your local global provider of market leading technology.

IMAGES

- Available on request.

###