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

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

Thursday, April 26, 2012
Sydney New South Wales

TECHNICAL ARTICLE

FOR IMMEDIATE RELEASE

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

MISTAKES IN DATA CENTRES: THE MOST DECISIVE MISTAKES WHEN PLANNING, BUILDING AND OPERATING A DATA CENTRE – AND HOW TO AVOID THEM

There are many pitfalls to be avoided when planning, building and operating a data centre, and many mistakes which could in the end endanger security and availability in the worst case. Excessive operating costs are the consequence above all where energy efficiency is neglected.

Data centres are nowadays increasingly decisive for business activities of all kinds, both for the economy as a whole and for individual companies. IT services have become practically indispensable for smooth business process management, and are in many cases an absolute prerequisite.

CAREFULLY ADVANCE PLANNING

The foundation for an optimum data centre is laid at the planning stage. It is particularly fatal if the planning fails to consider later performance and availability requirements. The definition of the desired performance parameters for a data centre should cover not only the processing capacity of the computers, data storage and other systems, but also aspects such as climate control, security and complex IT processes. The expectations of the future user are a decisive factor in respect of performance and availability. The data centre architecture appropriate to the targeted availability class can be detailed on the basis of classifications developed by the Uptime Institute. The latter classifies data centres on a four-tier availability scale, ranging from Tier I for minimal availability demands to Tier IV for high availability. Unambiguous requirements are specified for each tier, for example with regard to the redundancy of power supplies, and should be observed in the planning.

It is thus recommended to draw up detailed advance planning well ahead of the actual construction phase, and here to take into account all future wishes pertaining to the performance, efficiency and security of the data centre. This includes also careful deliberations regarding the required accessibility of the infrastructure, as well as the necessary protective measures and a corresponding authorisation structure. All the affected departments, including the final user, should be involved in the planning process. The outcome is then a technical specification which serves as a basis for all later processes.

Electricity is a basic resource for every data centre and must be available round the clock without interruption. The elaboration and implementation of a power supply concept should thus be handled with the greatest possible attention to detail. Many a data centre project have been delayed in the past

because an adequately dimensioned power supply could not be realised in time. The ready availability of sufficient electricity is consequently an important location factor, and will probably become even more significant than ever with the transition to renewable energy sources.

GENERAL CONTRACTOR RESPONSIBLE FOR NEW BUILDINGS

Many different trades are involved in the actual construction of a data centre. This calls for very complex coordination. At the same time, the boundaries of individual responsibility are often less than clear. The result, planning errors and oversights which may later express themselves in increased material, labour or operating costs. If the intended grid spacing of the floor is not observed, for example, future maintenance may be hindered because the floor cannot be opened at the point at which it is actually necessary.

There is rarely a single person within the company with the necessary experience to spot all the potential problems which lie in the interactions of so many different trades. After all, expert knowledge in the fields of fire safety, climate control and electrical installation work is not usually one of the immediate core competencies of a data centre manager. Only a few of their number are likely to achieve an optimum result when attempting to build a new data centre alongside their usual duties. It is thus generally better to consult an experienced planner at an early stage, and then to commission a general contractor to take responsibility for implementation of the plans and completion of the project.

CERTIFIED COMPONENTS ONLY

Certification is another point which is often overlooked. If the matter remains unheeded until after building construction, a longer certification process is almost inevitable and modifications may prove necessary in the worst case. If certified solutions are demanded for the individual components of the installation, on the other hand, certification of the overall data centre will be correspondingly simpler.

When it comes to security, in particular, it is advisable to rely exclusively on certified solutions, so as not to prolong later certification processes for the data centre. At the same time, such solutions improve the ratings of insurance companies and financing banks. Where already codified, the latest IT standards should be observed. That serves not least to raise the confidence of internal and external clients.

FUTURE-PROOF DIMENSIONING OF ENCLOSURES AND RACKS

It is not only the data centre building which must be planned with a view to the future and the expected demands of the clients. The same applies to the basic infrastructure of network enclosures and server racks. If the load-bearing capacity of the chosen server rack is inadequate, for example, it will very quickly reach its limits with the highly compact blade systems of future virtualised data centres. The only solution then would be a complete and correspondingly expensive rebuild.

The whole enclosure system should be designed for flexibility and protection against unauthorised access, and should permit suite expansion in as many directions as possible. Modular, scalable solutions which offer a diversity of dimensions within a single product family, and at the same time also cover all typical standards, are here the ideal choice. Otherwise, future expansions would result in an increasingly heterogeneous environment, with all the associated disadvantages. Careful selection of an enclosure system guarantees that later reorganisation can be realised quickly and at favourable cost.

MODULAR SECURITY

From the user perspective, security is the most important quality criterion for a data centre alongside availability. If valuable information is stolen or deleted, the costs of adequate security measures are often shown to be negligible compared to the ensuing damage. On the other hand, over-dimensioning must be avoided at this point, so as not to increase costs unreasonably.

It is not necessary, for example, to implement the same security level for all areas of a data centre. Basic protection is sufficient for many rooms. The servers, however, should be operated at the highest security level demanded by the users. Modular concepts and high-security server cells permit expedient graduation of the security level. That reduces costs, without compromising the security offered.

MONITORING PROCESSES AND PARAMETERS

Another aspect of security is constant monitoring of the actual data centre processes. Otherwise, faults or emerging problems may remain unnoticed until it is too late, with the risk of damage, failures and corresponding costs. In this context, sensors in the various racks and systems, in combination with monitoring software, help the administrator to maintain the necessary overview. On the other hand, this overview can soon be lost if the system issues a flood of unsorted messages in which the genuinely relevant alarms are drowned. Preference should thus be given to systems with which the messages can be bundled intelligently, as the basis for defined action decisions. Furthermore, an emergency manual should be created for conceivable risk situations, so that everyone immediately knows what is to be done should a crisis or problem arise. That, too, helps to minimise the potential damage and achieve fast remedy.

It is false thrift, moreover, to forego service or maintenance contracts for the installed products. In the same way that regular vehicle inspections serve to prevent breakdowns on the road, the regular maintenance of data centre components can ensure that – in the ideal case – costly operational disturbances are averted. If a problem arises nevertheless, data centre managers with a service contract in their desk are in a comfortable position. They can rely on fast repair or replacement of the defective component. Attempts to save a few cents are here thus rather misplaced.

PROPER UPS DIMENSIONING AND SELECTION

On the internal side, uninterruptible power supplies (UPS) ensure that the connected systems continue to run until a standby generator takes over or, in the worst case, for the duration of a controlled shutdown, if the external power supply is lost. Data centres often require substantial stored energy times, in order to be able to guarantee the agreed service level under all circumstances. After all, core business processes of the data centre clients are usually dependent on the availability of central IT services.

With this in mind, it is imperative to exercise exceptional care when defining the required capacity and stored energy time for a UPS. If only the power consumption of the servers is calculated, for example, but that of the storage media, cooling and switches is ignored, then dangerous bottlenecks are almost inevitable in case of an emergency. One especially important point is precise description of the required

load range. If a server farm is based on blade systems, it is decisive that the UPS can also handle capacitive loads efficiently.

Investment savings rarely pay off in connection with a UPS system. Lower efficiency, non-scalable monolithic solutions, shorter battery lifetimes, no safe-swap functionality to permit module replacement during operation, no battery monitoring or unfavourable maintenance agreements may reduce the primary purchasing outlay, but then drive up operating costs and component replacement needs. In the worst case, they may even lead to unforeseeable downtimes.

CARE FOR UPS AND INTERNAL POWER DISTRIBUTION

Incorrect handling may damage UPS systems or else impair their proper functioning. If the system batteries are exposed to temperatures above 25°C, for example, then their service lifetime will be shortened accordingly. The guidelines of the American Society of Heating, Refrigerating and Air-Conditioning Engineers (ASHRAE) currently allow temperatures up to 27°C in the server room of a data centre. If this possible range is exploited to the full, however, the UPS batteries should be accommodated in a different area at a lower temperature. Regular battery maintenance is also important to avoid premature capacity loss. This is another task which is best left to a specialist.

Further attention should be paid to the internal power distribution beyond the UPS: If the distribution networks are not inspected regularly, there is a risk of downtimes due to defective power packs and switches, and those are situations in which even the best UPS is powerless.

COOLING WITH OPTIMUM PUE

A cooling concept tailored to the later layout of the data centre rooms should already be elaborated at the planning stage. That not only saves significant financial outlay, but also improves the PUE rating (Power Usage Effectiveness). A low PUE value is today taken increasingly as proof of system efficiency. PUE is the ratio of the total power consumption of a data centre facility to the power drawn by the actual IT equipment (servers/storage media/networking). The IT consumption is here the denominator and the total consumption the numerator. The ideal data centre thus possesses a PUE of 1, but that is naturally unattainable in practice. A realistic target for newly designed centres is a PUE from 1.2. This rating means that the power demand for cooling and the remaining infrastructure amounts to 20 per cent of the consumption for IT equipment. Even better results have been reported in isolated cases. In many older, unmodernised or poorly utilised data centres, on the other hand, it is common to encounter PUE ratings between 2 and 3, or even higher.

When defining a cooling concept, it is the detail which counts: If a fan-based cooling unit is installed at the greatest distance from the racks with the highest power density, overheating computers can hardly be a surprise – the chilled air will most likely fail to reach the rack concerned with an adequate volume, if at all. Given the high power densities of a data centre, it is probably expedient to abandon the concept of circulating air and to consider rack- or suite-based climate control solutions. A server failure, after all, is often far more expensive than an investment in an improved cooling system.

The dimensioning of split cooling units requires particular caution: If the output demands are not identified correctly, the lifetime of the system will be shortened by the permanent on/off-switching either

side of the target temperature. Exact planning and analysis before purchasing, and then constant monitoring of the current output demands, avoid the problem.

EVENLY POPULATED RACKS

Fully packed racks, and similarly racks with large gaps, perhaps then also without blanking plates, hinder optimum cooling. Over-full enclosures still get hot, while empty racks are much colder than really necessary. The various racks should thus be populated as evenly as possible. Cables must not be allowed to block the air paths, and empty rack modules should be closed to avoid short-cuts in the circulation. Blanking plates, purposefully minimised cabling and tidy cable routing are the simple measures which provide remedy.

Imprecise estimation of the cooling demand may also arise through repeated modification of the equipment configuration over time, with the result that either the cooling becomes overstretched, or else cooling energy is wasted. During normal operation, too, the cooling demand is subject to fluctuation, for example where fewer systems are active over the weekend. In such cases, automatic inventory control and sensor-assisted rack monitoring can prevent damage and wastage, and thereby reduce costs significantly.

INCORPORATE COLD AND WARM AISLES

In the meantime, many users provide for separate cold and warm aisles. Otherwise, the chilled and warm air can mix uncontrollably, and the energy consumption for cooling is raised accordingly. Where the circulating air is able to take short-cuts, there is a greater risk of hot spots. The best solution is to enclose the cold aisle with an additional ceiling, doors and partition walls. The cold air is then unable to escape and the overall system can be operated at higher temperatures. As already mentioned above, the guidelines of the relevant branch associations already offer greater leeway.

If separate aisles are incorporated, the fire extinguishing system must subsequently be adapted to the new situation. Otherwise, in case of fire, the extinguishing powder will simply land on the roof of the cold aisle instead of smothering the actual source of the fire. In fact, this is a good example of how important it is to keep an eye on the impact for other areas of the data centre when planning modifications, in order to avoid unexpected failures.

CONSIDER FREE COOLING

In cities such a Melbourne and Canberra, it is generally recommended to consider free cooling by way of the ambient air. This is always a suitable option up to an outdoor temperature of 21°C, though some data centres also operate with appreciably higher temperatures. In many cases, this form of cooling is sufficient for the most part of the year, rendering the installation of a chiller superfluous. The cooling water should never be colder than actually necessary. If the cooling is overdone, valuable energy is wasted and the costs are increased.

If humidity control is neglected, however, the air humidity may prove to be too high or too low for the sensitive equipment. It must be said, on the other hand, that the permissible ranges have already been extended in this respect. In case of doubt, a specialist can assess the local weather conditions and the

details of the planned data centre to decide whether or not it is possible to continue without cooling and climate control units.

CONCLUSION: PLENTY OF SCOPE FOR SAVINGS

If the most important rules are observed when planning, building and operating a data centre, the costs can be reduced significantly compared to less systematic approaches. No compromises are necessary with regard to security, performance and availability. On the contrary, they benefit from a consistent and carefully devised installation and operating concept.

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.

###