DCA review

by Simon Campbell-Whyte, DCA Executive Director

THE SCIENTIFIC PROCESS of research can be a little slow and frustrating for some, and I include myself as guilty of being impatient. However, only this methodical approach can produce reassurance of belief and certainty of vision. Having spent some 12 months collecting and validating data, the PEDCA project is now entering the phase of developing the solutions, ie the Joint Action Plan for the European data centre sector. This convergence of the project with the real world of constructing solutions to problems enables us to "see" the potential impact possible on the horizon.

For example the development of the DCA Certifications, although based on many voices and many shared views, satisfyingly addresses more than one requirement highlighted by the research.

I'm also glad the programme itself has been developed the "difficult" way ie with all the necessary procedures, processes and rules to ensure it can be more than just a "badge" and can stand the test scrutiny and time. It is also realised that this takes time and has recognised steps to follow. The next steps include "Peer" review by four Academic institutions, further industry feedback and the first review of the requirements. The latter is scheduled for September and anyone can participate by joining the steering group at **www.data-central.org**

In this issue you can read a report from the public launch of the DCA Certifications programme, if you missed this one, rest assured there will be others across Europe during the year. In closing I would like to thank all the contributors to the development and especially those who participated and presented at the event. With regards to PEDCA we will be running four "focus panels" to consult further with the industry across Europe. In addition, to ensure everyone has the opportunity to have their say in shaping the future of the industry, online participation is now launched at **www.data-central.org**

Certification launch

DCA launched its quality assurance programme for Data Centres, which is now ready to deploy, on the 10th June at University Of East London. The launch was chaired by DCA SVP Matt Pumfrey of Smart Carbon Control who introduced a keynote from DCA President Steve Norris of Virtus Data Centres. Steve, a firm advocate in raising the bar of professionalism even higher, gave an opening speech that laid down the challenge our industry faces in dealing with the global economy of the future by bringing forward solutions such as the DCA Certifications.

Steve's speech reiterated the need for our sector to champion its excellence and raise awareness of the importance of data centres to our daily lives and businesses, enlightening policy makers to see good data centres as assets and enablers that should be encouraged.

The theme of energy consumption is one of the critical areas addressed by the DCA Certification programme. This was discussed at the next keynote by Lord Rupert Redesdale, who as a former Energy Spokesman for the Liberal Democrats and now Chief Executive of the Energy Managers Association (EMA), fully understands the issues facing data centres in the UK and many other European countries. Rupert painted a sobering picture of what the future will look like in the midst of dwindling energy resources, rising demand and greater dependence on data centres. It was clear that the DCA and EMA, working together can engage the energy managers of the ICT industry to drive the wholesale energy efficiencies that are urgently needed.

Steve Norris

The DCA Certifications mark is underpinned by existing standards and recognised best practices. As Duncan Clubb CTO of CS Technology demonstrated in his presentation, the standards landscape of the data centre is extremely wide ranging and in some cases fragmented which leads to much subjective debate even amongst the data centre experts. Which can lead to at best, a lack of clarity, and at worst, mistrust amongst the very customers and policy makers data centre sector must to engage with. Duncan's talk threw out the question of whether data centres standards are currently working for, or against, the interests of the industry – with the consensus view clearly being the latter. One key stakeholder for the data centres is the Cloud industry, driving growth into data centres.

Alex Hilton Chief Executive of the sectors leading association, the Cloud Industry Forum, presented the already established CIF Certification for cloud based services based on a robust code of practice. Alex's presentation highlighted the urgency and importance of the data centre sector to complete the missing piece in the picture. Alex also demonstrated some of the remaining barriers to cloud adoption which the DCA Certifications will help address. CIF and the DCA have agreed to collaborate on joint programmes and projects for the benefit of both sectors and their respective members.

After the coffee break, Simon Campbell-Whyte Executive Director of the DCA presented an overview of the mechanics of DCA Certifications. He thanked DCA members for contributing and especially PTS Consulting, Future-Tech, CS Technology and Cerios Green for their expertise and assistance in developing the programme. Simon showed how the DCA Certifications is designed to be industry led, meeting the demands of fast evolving technology and innovation.

Customers of data centre will be able to trust the DCA Certification as a "quality mark" on their data centre facilities because it means the facility has been assessed by an approved auditor and that their findings have then been independently reviewed by an external DCA Accreditation Board. The benefit to operators of having their data centre facilities DCA certified is to clearly demonstrate that the published data on the specific facility has been externally verified. This verification covers the four critical areas demanded of data centres which is Reliability, Operational professionalism, Physical Security and Energy Efficiency.

Simon outlined the benefits to the industry's consumers by assuring them that a data centre 'does exactly what it says on the tin', safe in the knowledge that the facility is reviewed annually to ensure that the advertised standards are maintained. Simon also showed the critical "golden rules" of the scheme to ensure it is trusted which include; Independence, transparency and affordability.

After Simon's presentation debating continued into a panel session, chaired by

Lord Redesdale

Matt Pumfrey, which included on the panel Martin Essig, MD of Telecity GmbH, James Wilman of Future Tech, Steve Hone of DCA, Grant Morrison of PTS Consulting and Frank Verhagen of Cerios Green. The DCA would like to thank all the speakers and participants who contributed to a stimulating and inspiring afternoon.

Do you really have Resilient Cooling?

By David King, Senior Consultant Engineer, Future Facilities Ltd.

RESILIENCE AND REDUNDANCY are often treated synonymously, but they are not the same thing. While the dictionary tells us that resilience refers to something's toughness, it informs us that redundancy refers to an object's expendability. To the engineer it means this: a system with redundancy built in is not necessarily a resilient one.

In the data center, being resilient means that all of the IT equipment housed in the facility will continue to function in the face of a power outage, cooling failure or other serious disruption. That is, to have a system such that any element can fail and there is another with enough spare capacity to ensure resilience.

Consider a data center with a 2N redundant power system. There are separate, expendable paths for electricity to flow, all the way from the incoming utility to the individual rack, and each is capable of supporting the full load.

However, the IT equipment will only be resilient to a power failure if it is plugged in to both of those of power paths. Even if the servers have two power cords, if they are both plugged in to the same power strip, all of that redundancy is wasted and the IT is not resilient. For it to be resilient, the redundancy has to be transferred all the way down the chain to the IT without a single point of failure.

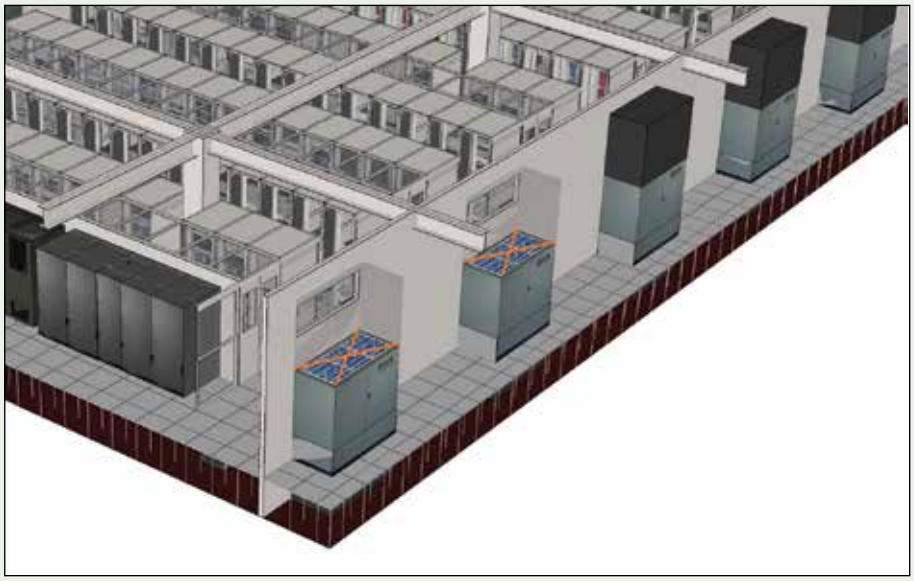


Fig 1. Airflow under normal operations

For a power system, or even a network system, the resilience of the IT can be checked relatively easily; both of these services are delivered by wired connections all the way from the utility entry down to the IT. Diagrams of how these connections

are wired to the rack should be part of the data center operations manual, and regular audits of connections within the racks avoid unknowingly relying on single points of failure.

It is not so easy to identify the link between the redundancy in the cooling infrastructure and the resilience of the IT to a cooling failure. It is not possible to document how the cooling moves from the cooling units to each individual server because the final stage in the delivery of the cooling is done through the invisible medium of air. You may have four redundant cooling units but how do you know if the air will be delivered to where it's needed when you come to rely on them?

The use of air brings with it the other complication of variability. Cooling units in the data center supply air to a common area, and the air paths that form are all dependent upon one another. Take one (or more) units offline and the flow from the others rushes to fill the space left, changing the whole distribution pattern!

You may still have enough cooling for the space, but that not-so-critical hot spot might have just moved a lot closer to your core network switches. The inherent variability of airflow means that the only way to be certain about your IT resilience today is to deliberately fail your number of redundant cooling units in the worst case combination to see what happens.

Doing this in an operational data center is generally not an option. So for the majority of data center operators - who are generally familiar with power and networking - the answer to the question, "Do you have resilient cooling?" is a re-statement of the system's redundancy. However, the true answer is that they do not know.

This is why so many operators remain nervous about their cooling performance and insist on an expensive, potentially-ineffective and overcautious approach that consists of over engineering a lot of cooling headroom. It is only those who have experienced a cooling failure who will really know whether their cooling system is resilient. Given the mission critical nature of nearly all data centers, what can be done?

We can learn from other industries that are faced with the same problem – industries where operators need to know what will happen in exceptional circumstances, but do so without having to experience it for real. In the automotive industry, for example, they use crash test dummies in a real car to find out what will happen to a car's occupants during an accident without having to put any real people at risk. This shows us how using a model (instead of a real passenger) is a risk-free method of understanding the resilience of a complicated system during a potentially catastrophic event.

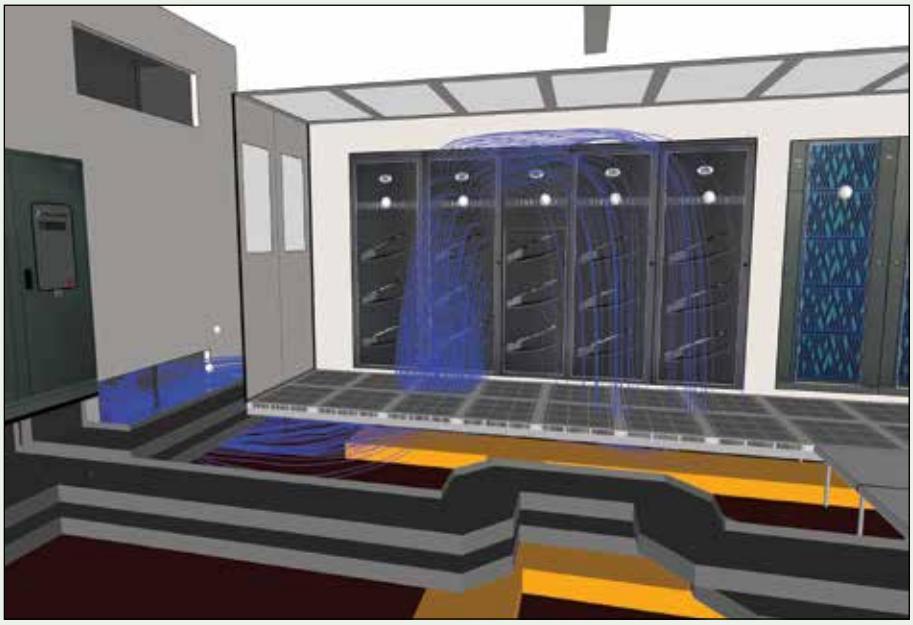


Fig 2. Airflow during failure

For data center cooling, testing can be done quickly and affordably in a computer model. It's a proven science; virtual testing and prototyping with computer models is used in a vast array of applications where physical testing is not feasible.

Crowd movement at major events is a good example of this. When planning a large event like a street marathon or concert, planners need to ensure the safe flow of people.

Much like airflow in a data center, in an emergency situation this flow is likely to change from planned. For example, a fire may cut off certain routes. Computer simulations are used to make sure there are no pinch points that could cause a crush and that escape plans are resilient to the most likely crowd responses without putting real people at risk.

The one-off, upfront crash testing carried out before a car makes production is sufficient because the car is not intended to undergo any significant changes throughout its lifetime that would render the testing results irrelevant. The same could be said about the large scale crowd movements at major events. But a data center is different prospect altogether: over a long period of time, the configuration of the data center is expected to deviate from its original design.

The churn rate of IT within a modern mission critical data center means any physical "crash testing" of the cooling resilience done at the design stage quickly loses relevance. Daily IT deployment operations will change cooling demands throughout the data center.

Only by testing the cooling system regularly can the IT resilience to failure truly be known. Computer modeling and simulation offer a way to run those tests at any point in the data center's life without any risk to the devices and applications they are supporting.

Air movement around an entire data center can be accurately modelled using computational fluid dynamics (CFD). Working in the virtual world means air paths can be traced, allowing the cooling system to be visualised. Worst case cooling failure scenarios can be analysed to see the impact on the IT equipment, without putting any of it at risk in real life.

Like a single line diagram, it allows operators to see where there are single points of failure. But, even more than that, it also allows them to investigate why they have occurred and test out potential solutions.

Using CFD, cooling resilience moves from being an unknown quantity to a metric that can be calculated using physics-based simulations, helping operators make the most of their data center infrastructure and performance.

Improved resilience through reduced complexity and increased training

By Beth Whitehead, Sustainability Engineer, Operational Intelligence Ltd and David Cameron, Director, Operational Intelligence Ltd.

THERE IS SUFFICIENT RESEARCH into the causes of failure to assert that any system with a human interface will eventually fail. In the data centre, as with other industries, human error is believed to account for as much as 80% of downtime. Limiting these interfaces and the design complexity, and continually training the humans that operate them is therefore imperative for resilient data centres.

The biggest single barrier to risk reduction is knowledge sharing and lack of risk awareness. Many sites document risk analyses, but often these are not shared with all the operators and therefore their impact is limited. The accumulated experience of a company and the depth of experience of the individual, interact on the universal learning curve, and are important both in reducing risk and addressing energy wastage.

Knowledge sharing becomes more important as the complexity of systems increases, particularly where operators lack experience with the installed system.

Knowledge sharing

The educational theorist, Kolb, says that learning is best achieved when we move through all four quadrants of the Kolb Learning Cycle: reflection, theory, practice and experience, shown below.

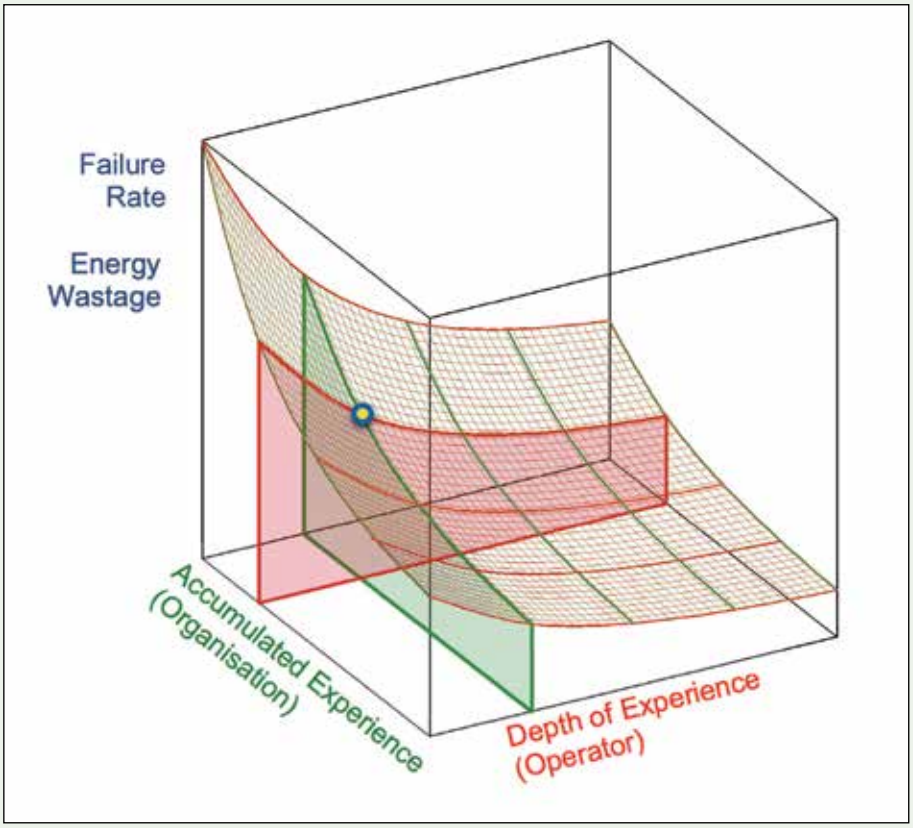
It is interesting to compare this process with how technical information is transferred on a construction project. Each quadrant is inhabited by a different role, between which contractual boundaries exist, making knowledge transfer difficult. Of particular interest is the handover from installation to operations teams. Much of the knowledge imbedded in the project is lost and the operations team is left to look after a live, critical facility with only a few hours of training and a set of record documents to support them.

Integrated systems testing (IST), used contractually to ensure systems work as designed to, is now common on data centre projects, but generally includes only limited involvement of the operations team, and therefore limited knowledge transfer. Furthermore, many facilities have little or no communication with the original designer or installation contractor, again limiting opportunities for knowledge transfer.

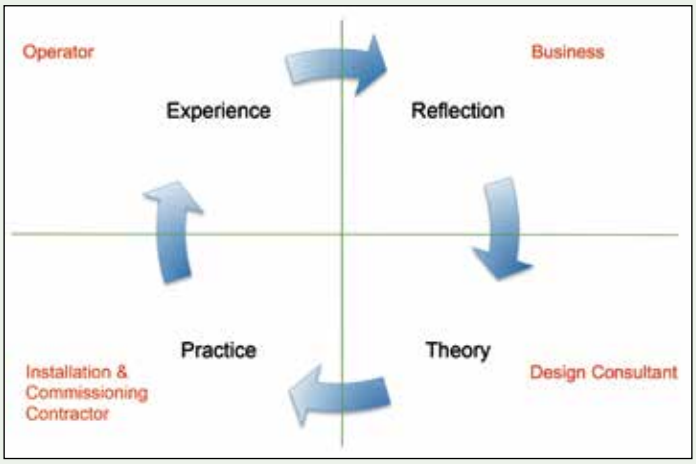
Consequentially operators are not engaged, and don't feel sufficiently informed to make changes to optimise system performance, and improve the energy performance of the facility, for fear of introducing risk. This lack of awareness can lead to operational errors, leaving the facility particularly vulnerable at times of reduced resilience, for example during maintenance. As the complexity of a facility increases, so too does this risk of operational error. It is clear that most failures in the data centre are due to human error.

The human element

Site-specific, facility-based training is therefore paramount in reducing the risk of failure from human error. In addition, itÕs important that teams are trained on more than just the area of the facility that they operate, and at every level of the team from manager to site operative. This approach helps them to operate the facility holistically, understanding how each system interacts, and promotes communication between different levels and teams.



Traditionally, however, this approach is rarely adopted by the industry. In addition to this, a learning environment, which promotes continuous improvement, is recommended to allow teams to learn from the failures and near misses that do occur. This increases knowledge and awareness of possible failure scenarios.



Complexity

A 2N system is the minimum requirement for a SPOF-free (single point of failure free) system, in which two or more simultaneous events result in a failure. Traditional risk analyses, such as FTA (fault tree analysis) are not applicable to human error in which data is subjective and variables, infinite. In a 2N scenario, the two discrete systems can be designed to have no interaction. This creates a simple design with limited complexity. However, facilities are rarely designed in this way. For example using BMS controlled automatic disaster recovery changeovers, rather than simple mechanical interlocks. Although the design remains 2N, the number of variables and complexity has increased exponentially. The training and knowledge requirements to run the systems are therefore increased. Research has also shown that failures are often due to an unforeseen sequence of events. Until it has occurred there is no knowledge of it's potential. The Austrian physicist, Ludwig Von Boltzmann, developed an equation for entropy that has been applied to statistics, and in particular, to missing information. The theory can be used to determine the number of questions needed to determine which box, on a defined grid, a coin is placed. If we substitute system components for the boxes, and unknown failure events for the coins, we can consider how system availability is compromised by complexity. It can be seen that with fewer unknown failure events, the number of ways in which a system can fail are reduced. Increasing our detailed knowledge of systems, and discovering unknown events will therefore reduce the combinations in which the system can fail, thereby reducing risk.

Conclusion

Human error is indisputably the largest contributor to data centre downtime. Continual, site-specific training is therefore of paramount importance in reducing facility failures. Furthermore, reducing complexity not only reduces the number of unknown sequences of events that cause a failure, it also reduces the amount of training required. Finally, it is important that particular attention is paid to the processes used when handing over a live site to the operations team to ensure knowledge is not left with the installation and commissioning contractors.

What makes a data centre stand out from the crowd? **The People!**

By Mike Bennett, VP of global data centre acquisition and expansion at CenturyLink Technology Solutions EMEA.

What is it that makes a data centre stand out from the crowd? Connectivity, cooling and power are (of course) fundamentals but it's the people inside that are the real differentiators. They have the power to evolve a facility; they have the power to make a good data centre great or a potentially great data centre average.

Many providers build a data centre and have someone else manage it. They effectively outsource the running of the facility, while they sell the space in it. They are essentially property companies and that's ok, if it works for them.

However, the knock-on is that the staff members that are brought in are very limited in what they can do to make positive change. They may only be on site for a three-five year contract (of for even less if they come in half way through) and so there is little incentive to improve the smallest things, that ultimately pay dividends later on down the line.

On the other hand, permanent dc workers are able to take real pride in where they work and make a high personal investment. They know that they can make a serious difference and it feels like 'their' facility. If they discover a more effective way of doing something, they test it and if works, before you know it, it's rolled out globally. You can be sure that the rightful credit is given and that person gets the recognition they deserve.

The ability to make a real change is a powerful motivator and helps attract the best from other mission critical industries. Those coming from manufacturing backgrounds (to pick but one example) have a huge amount of transferable skills and bring trade secrets that, on the surface, appear to be completely unrelated to the dc space. One such recent example is someone that came from a chocolate factory.

The factory could never shut down as the chocolate and sugar would freeze in the pipes, bringing manufacturing to a halt for weeks. You better believe such an environment taught him the importance of zero downtime and how to keep things running smoothly!

It's not just about the quality of staff; it's about enabling those talented individuals to constantly improve to the benefit of everyone involved. And when data centre engineering staff can stay with their company for 25 years, even the smallest things are worth doing. There is an important distinction between a data centre and a professional data centre operation and, more often than not, it's the people.