Informing the electrical industry for **140** years

Electrical Review

January/February 2019
Volume 253 | No 1
www.electricalreview.co.uk

Test & Measurement
Why primary injection has the edge

Power
Unleash the untapped potential of your UPS system

Connected Vehicles
How autonomous vehicles are changing the data centre as we know it

Feeling like a boss?

5 Year Warranty on UPS

You just bought a new UPS with a 5 year warranty as standard. Now that's a smart move!

riello ups

Reliable power for a sustainable world

5 year warranty as standard on all UPS models up to and including 3kVA.

EDITOR: Elinore Mackay
020 8319 1807
elinorem@electricalreview.co.uk

EXECUTIVE EDITOR: Claire Fletcher
clairef@electricalreview.co.uk

PRODUCTION MANAGER: Alex Gold
alexg@sjpbusinessmedia.com

GROUP SALES MANAGER: Sunny Nehru
+44 (0) 207 062 2539
sunnyn@sjpbusinessmedia.com

SENIOR ACCOUNT MANAGER: Amanda McCreddie
+44 (0) 207 062 2528
amanda@electricalreview.co.uk

PUBLISHER: Wayne Darroch

PRINTING BY
Buxton

Paid subscription enquiries
Tel: +44 (0) 1635 879361
electricalreview@circdata.com
SJP Business Media
Unit K, Venture House, Bone Lane,
Newbury, RG14 5SH

Subscription rates:
UK £221 per year, Overseas £262

Electrical Review is a controlled circulation monthly magazine available free to selected personnel at the publisher's discretion. If you wish to apply for regular free copies then please visit: www.electricalreview.co.uk/register

Electrical Review is published by

2nd floor, 123 Cannon Street
London, EC4N 5AU
020 7933 8999

ISSN 0013-4384 – All editorial contents © SJP Business Media

Average net circulation Jan-Dec 2016 6,162

Follow us on Twitter @elecreviewmag

Join us on LinkedIn

86% think energy companies must do more to tackle meter cheating

Almost nine in 10 (86%) UK billpayers think that energy companies should be working harder to tackle energy theft, according to a research report.

The study was commissioned by outsourced utility customer engagement specialists Echo Managed Services and Grosvenor Services Group and endorsed by Crimestoppers UK.

It surveyed 2,000 UK residents and found widespread public support for greater measures to be taken against the crime. Current statistics show that 150,000 cases are investigated annually, but only around 1,500 people are charged.

Amongst those who advocate further action, 43% said it's because energy companies have a social obligation to combat meter cheating, given that meter cheating leads to at least one injury or death every 10 days in the UK, due to electric shocks, fires and gas explosions.

A further 43% of people stated it's because of the extra financial burden that energy theft places on their own bills. The practice currently amounts to £400 million in stolen gas and electricity every year, adding around £20 to every household's annual bill. Experts also suggest that this figure is continuing to rise.

The survey also looked at media visibility of energy theft and found that only 14% of UK residents recalled seeing any news coverage of the crime in the past 12 months.

This may be part of the reason for low awareness levels across the board, with 80% of people saying they were unaware of the financial implications of energy theft, and 39% of those surveyed stating they weren't aware of the risks it causes to public safety.

Lloyd Birkhead, managing director of Grosvenor Services Group said, "The overwhelming sentiment from UK billpayers is that energy companies should be doing more to tackle this problem and that it is their duty to do so.

"Whilst there is an obligation under licence condition 12 to take action, investigation activity varies considerably across the sector, with only some suppliers meeting the Ofgem theft incentive target.

Birkhead concluded, "More must also be done to increase the visibility of energy theft and make it a mainstream crime issue. This can be achieved through reactive reporting – for example, when convictions are secured – but also through proactive public campaigns.

"These need to drive home the financial harm and public safety risks of tampered meters, as well as raise further awareness of confidential reporting lines, such as the Crimestoppers Stay Energy Safe helpline."

Rogue trader jailed following investigation

A man has been jailed for carrying out dangerous work while posing as a registered electrician.

John Draco, 35, of Rowan Place, Newton Aycliffe, pleaded guilty to fraud and consumer protection related offences after falsely claiming to be a qualified electrician.

He advertised his services on Yell.com as accredited by ELECSA and Trustmark-despite not having either accreditation. He also claimed to be NICEIC registered.

He was jailed for 13 months following a trial at Durham Crown Court in January.

The court heard how Draco had offered to complete a full rewire of a property for £3,000, but had left it in a highly dangerous state.

When his shoddy work was challenged by the homeowner, he abandoned the job and kept the full sum.

The homeowner got in touch with Hartlepool Trading Standards who took on the case with help from ELECSA.

Such was the poor standard of the installation an investigation by an electrical engineer ordered it not to be used as it posed a serious risk of fire and electrocution.

Work to rectify the problems left by Draco ran into thousands of pounds. Draco, who traded under the name J and A Electrical Solutions ended up paying the victim back £3,820.

Ian Harrison, Hartlepool Borough Council's trading standards and licensing manager, said, "This successful prosecution sends out a strong message that the courts will not tolerate rogue traders conning people out of their hard-earned cash.

Kevan Parker, interim managing director of Certsure, which operates the ELECSA and NICEIC brands added, "We take a dim view of those who pretend to be registered electricians when they are not.

"We will work with the appropriate authorities to protect those contractors who are legitimately registered with us and have the quality of their work assessed on a regular basis.

"Anyone thinking about using our logo fraudulently will be caught and dealt with appropriately by the courts."

100 years of electrical safety

EXPECT EASIER, SAFER, FASTER INSTALLATIONS.

Choose our Instinct keystone module with angled data outlets.
It's safer and sleeker with less bend to cables than traditional models.

INSTINCT. MAKE A CHOICE FOR THE BETTER crabtreecommercial.co.uk

Crabtree

Top ten UK cities for tradespeople revealed

New research from Sanctuary Bathrooms has revealed the best locations in the UK for those working in the trade industry.

The new ranking analysed the average wages of electricians, as well as plumbers, joiners, and painter decorators, alongside cost of living data, university building course ratings and the percentage of workforce in trades for each city.

The data revealed that the best opportunities for tradespeople are concentrated in the North of England, with seven of the top ten cities located above the Watford Gap. The top 10 cities are:

1. Liverpool
2. Newcastle
3. Glasgow
4. London
5. Birmingham
6. Leeds
7. Nottingham
8. Cardiff
9. Manchester
10. Bristol

The rankings also revealed that Leeds has the highest concentration of tradespeople in the workforce, making up 10.3% of the city's working population.

As for the best paid? The top spot goes to Glasgow, with electricians reportedly earning an average annual wage of £28,683.

James Roberts, director of Sanctuary Bathrooms, commented on the findings, "As a company with our roots tied into the trade sector, both through our employees and our clients, we wanted to look where to find the best opportunities for tradespeople in the UK."

"The results are a useful resource for those wanting to embark on a career as a tradesperson, and also highlight important hubs for related businesses to expand into."

Cutting the cord on electric vehicles

A new technological breakthrough could change the way we power electric cars. New polymer-based flexible solar panels could eventually cover the outside of your vehicle, allowing it to charge as you drive.

This significant breakthrough could have wide repercussions on how we power a range of technologies.

Dr Franky So, inventor and chief technology officer (CTO) of NextGen Nano, explains how combining organic semiconductors and photovoltaics will allow us to cut the cord on electric vehicles.

Although renewable energy in the form of solar and wind now contributes more to the grid, a growing demand for EVs will not only place a burden on the generation network, it will also require a comprehensive overhaul of the charging infrastructure.

If this demand outstrips industry's ability to put in place the network sustainably, we may face challenges in the widespread adoption of EVs.

One possible answer is to shift the generation directly to the vehicle at the point of use. Although the technology for solar powered vehicles has been around for a while, it has traditionally failed to be commercialised for automotive use in the same way that internal combustion technology has, due to a variety of factors.

These include things like efficiency, range, battery technology, the cost of manufacturing and recyclability. This is not ideal because commercial-grade second generation solar photovoltaic cells deliver efficiency of around 20%.

They are also rigid, heavy and use costly rare-earth minerals that would be expensive

to recycle at the end of the vehicle's lifecycle. The production of silicon-based solar panels also incorporates the use of toxic chemicals that are very polluting to the environment.

Now, a new breakthrough technology from NextGen Nano expects to tackle many of these issues.

The company has developed a polymer semiconductor that is alterable in material design, is lightweight, flexible, semi-transparent and cheap.

When paired with photovoltaics it allows for the creation of polymer solar cells. This is a new exciting class of energy harvesting technology that has the potential to revolutionise the way we power things like electric vehicles.

The technology works by layering different materials to make up the solar cell. The NextGen Nano substrate consists of five layers.

The first layer is the electrode, followed by a charge-conducting interlayer, a light-absorbing layer made of organic semiconductor material, another charge-conducting layer, followed by a transparent electrode layer and the whole assembly is finished in an outer layer of flexible plastic.

The possibilities for this technology are endless. Instead of strapping rigid and heavy solar panels onto a car, cars can be covered by this flexible solar-power-generating sheets. This will take advantage of every available inch of surface area to generate energy.

In essence, this technology could become the material of choice for car bodies. Not only could it lead to the development of a new range of electric vehicles that could charge themselves as you drive them, it would increase their range and eliminate the need for costly infrastructure developments.

As new polymer solar cell technology gains traction, it's not only the electric vehicles that will be cutting the cord. Anything with a reliance on the grid for electricity could be transformed.

Don’t pay the price for poor power quality.

Reduce energy costs and increase load capacity with ABB’s power factor correction solutions.

Inductive loads such as motors, pumps and fans can cause your site’s supply power factor to drop, reducing the amount of the power supplied that you can effectively use and potentially leading to financial penalties from your utility. Since the introduction of DCP161 by OFGEM in April 2018, many industrial and commercial businesses with half-hourly (HH) metered supplies are now finding unpleasant surprises in their utility bills. This is because DCP161 imposes excess capacity charges, potentially in excess of 100%, on any location that exceeds its agreed electricity consumption level. **abb.com/powerquality**

ABB

GOSSAGE

Like father, like son

When I first wrote this Diary, Margaret Thatcher was Prime Minister, and Peter Walker her maverick Energy Secretary. Way ahead of his time, he was a great champion of renewable electricity. It was an enthusiasm not shared at the Treasury, then run by arch climate change denier Nigel (now Lord) Lawson. He went out of his way to block any renewables progressing. Even so, Peter Walker would litter his speeches with ecstatic hymns of praise to various embryonic renewable electricity initiatives.

One that used to feature regularly came from Cornwall. Called Hot Rocks. And he would always introduce references to this concept by saying that "this name has always enthused my teenage son Robin, as he keeps thinking it must be a new sensational pop group."

I was reminded of this when I saw that two wells are now being drilled by Geothermal Engineering near St Day in Cornwall. The deepest of which will reach 4.5km underground. The objective being finally to demonstrate the potential of geothermal electricity.

I do hope that somebody within the company has as long a memory as I have. And will to invite the Minister for Exiting the European Union to visit. His name? Robin Walker. Who, just as his father did, represents Worcester in Parliament. And I am sure is now every bit as keen on the prospects for geothermal energy as he was on pop music as a teenager.

Heads I win, tails you lose

There is one forgotten beneficiary from the arrival of all these new entrants into the electricity supply market. As we stand, it is any customer of theirs.

After all, the only reason for signing up with these Two Men and A Dog start-up companies is their discounted prices for electricity. It is most unlikely to be their customer services standards, which are frequently lousy. But the monthly payments will surely be far lower than buying from the Big Six.

I heard about one small firm, running a scheme where customers pay £1,000 up front for a year's electricity and gas, locked in at the "cheapest fixed- energy tariff in the country." And on top of that, each customer gets no less than 12% annual interest on the credit balance – a sizeable further discount.

Guess what happens if/when that company also goes bust? Does the customer lose the deposit money? No way. OFGEM operates a compulsory levy scheme, placed upon all suppliers. A piggy-bank which the regulator will raid, in order to reimburse in full the by-now ex-customer of the collapsed company. Paid for by the more responsibly run suppliers.

So the cunning customer has the reassurance of having been in-pocket from the start-up's special deal. And never being out of-pocket for paying ahead. Plus, another opportunity to start playing the system again, by signing up with the latest "leccy cheap as chips" offer around.

Is small beautiful?

Spark Energy. Extra Energy. Gen4U. Future Energy. Usio Energy. Iresa. National Gas & Power. These seven small companies have one thing in common. During 2018, each ceased providing electricity supplies to British customers.

During last year there were no fewer than 73 active electricity suppliers licensed by the regulator Ofgem. In 2017 there were 60. This time seven years ago, there were just 14.

This churn has set alarm bells ringing at the regulator Ofgem. Belatedly it is now seeking to require prospective new entrants to demonstrate they have the money and the resources to operate for at least a year, before being granted a licence.

Small suppliers have been feeling the bite of rising prices and inadequate balance sheets. Often in combination with poorly executed hedging strategies, and a lack of market expertise.

The news that some are unlikely able to pay what they owe under the Renewables Obligation scheme compounds their survival challenge – and may have compelled Ofgem to act. There is currently £59m missing that suppliers should have paid into the scheme that Ofgem is responsible for administering.

While several suppliers are known to be a bit behind with RO payments, the regulator was already investigating Spark Energy over its non-payment before it crashed out of the market. I understand it has specifically instructed two others, Ure Energy and Eversmart, to pay in monthly instalments what they owe by 31 March.

Trump sees the light

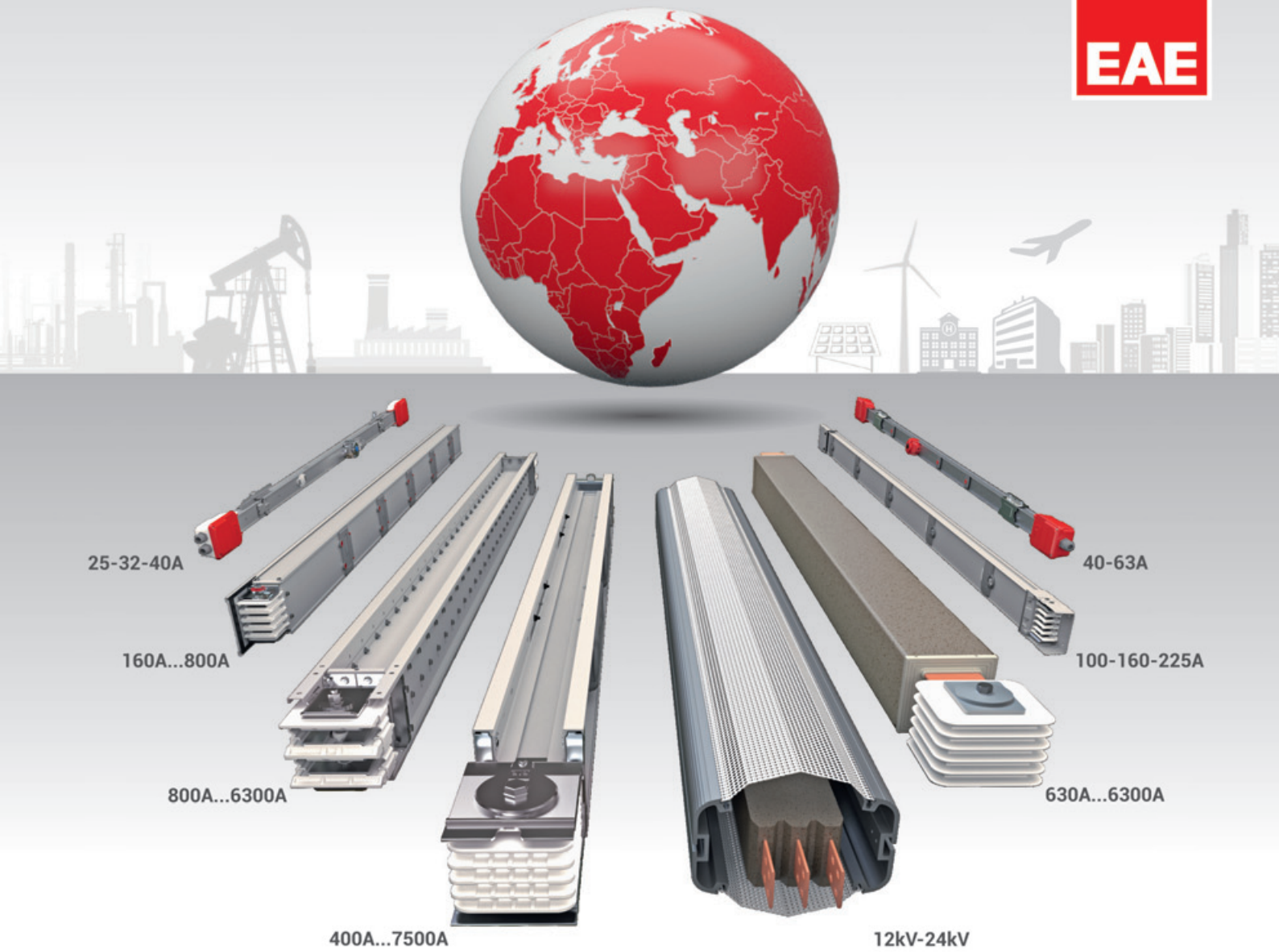
Here is a warning from the world's most powerful man, the Tweetmaster-in-Chief. It concerns the merits (or in his view the demerits) of installing LED lamps.

I quote verbatim from a tweet issued at 8.39 a.m. on October 17. It reads:

"Remember, new 'environment friendly' lightbulbs can cause cancer. Be careful - the idiots who came up with this stuff just don't care."

You couldn't make this rubbish up, could you?

EAE



Commercial & Residential | Oil&Gas | Data Centre | Industrial | Airport

Busbar Power Distribution Systems

Serving industries worldwide

Founded in 1973 EAE Elektrik is a worldwide manufacturer of electrical products.
For the past 25 years we have successfully supplied power distribution products to major UK Infrastructure and Datacentre projects. "Lean Production" and "Innovative and Customer Driven Product Development" approaches are the key values utilized in designing and manufacturing the product families in compliance with ISO 9001, ISO 14001, OHSAS 18001 and ISO 27001. Accredited by main contractors and end clients our product quality and service has been widely recognised. With full UK based project management and service resources, EAE is poised to support you on your next project.

DATA CENTRE WORLD LONDON | 2019
Visit us at STAND D820

www.eae.com.tr

For Enquiries
sales@elbagate.com
+44 (0) 1527 575075

If you sell products or work on projects within **Power, Lighting, Fire Safety & Security, Test & Measurement, Energy Efficiency** and **Data Centres**, make sure you enter:

ER EXCELLENCE AWARDS 2019

Electrical Review

In partnership with riello ups

In association with DCR Data Centre Review Magazine

ENTRIES ARE NOW OPEN

visit **www.electricalreview.co.uk/awards**

Your business and your team could be celebrating in the spotlight at the ER Excellence Awards Gala Dinner on 30 May 2019 at the Four Seasons Hotel in Central London!

In partnership with: riello ups

2019 Award sponsors: HEATLOAD by Mafi Mushkila Ltd, WAGO, SMART GRID FORUMS Driving Clean Energy, RecOlight WEEE? GOT IT.

Following the success of the inaugural 2018 Electrical Review Excellence Awards, we invite electrical manufacturers, contractors and project owners to enter the 2019 Awards.

The recipients of 2018 Awards included: Noriker Power battery storage facility - Entry by Vertiv; Indectron Shield House data centre - Entry by Sudlows; The Queens Hotel, Penzance - Entry by Chubb Fire & Security; Project Beagle, Ingenuity House - Entry by zencontrol ltd; Chertsey Water Treatment Works - Entry by Danfoss Drives and Heathrow Airport, Electric vehicle charger installation - Entry by R.L. Freemantle Electrical Ltd

SPONSORSHIP OPPORTUNITIES AVAILABLE

Contact us +44 (0) 207 062 2526

All winning entries will also be considered for two additional awards – Project of the Year and Product of the Year, both presented by Riello UPS – and recipients will be announced during the Awards evening.

The Awards include the following categories:

Power - Product of the Year
Power - Project of the Year
Lighting - Product of the Year - Sponsored by Wago
Lighting - Project of the Year
Fire Safety & Security - Product of the Year
Fire Safety & Security - Project of the Year
Test & Measurement - Product of the Year
Energy Efficiency - Project of the Year - Sponsored by Recolight
Innovative - Project of the Year
Sustainable - Project of the Year - Sponsored by Smart Grid Forums
Data Centre Design & Build - Product of the Year
Data Centre Design & Build - Project of the Year - Sponsored By Heatload
Data Centre Cloud - Product of the Year
Data Centre Cloud - Project of the Year
Data Centre Colocation - Supplier of the Year

If you would like to be involved as a sponsor or supporter, please contact
Sunny or Amanda on +44 (0) 207 062 2526 or
email **sunnyn@sjpbusinessmedia.com / amanda@electricalreview.com**

Circuit breaker testing library for CIBANO 500

When it comes to speeding up circuit breaker (CB) tests, OMICRON has the answer.

A tedious, time-consuming and error-prone task, CB testing has always involved the need to search and enter the circuit breaker-specific parameters by hand.

OMICRON saw room for improvement, and decided to speed things up with its circuit breaker testing system CIBANO 500 and the operating software Primary Test Manager (PTM).

Since version 4.40, the PTM software now contains OMICRON's new circuit breaker testing library (CBTL) for use with CIBANO 500.

CB DATA WITH THE CLICK OF A BUTTON

When using the CBTL, you will now be able to load all of the asset-specific default data into PTM with just the click of a button.

All you need to do is look up the CB's serial number, perform any necessary modifications on the default data, and then you're ready to test.

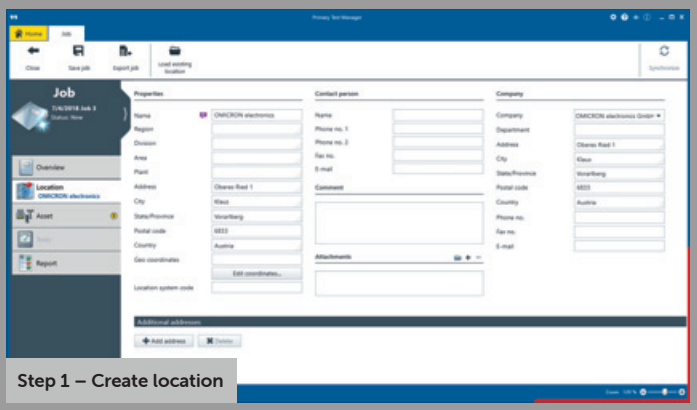
ADDITIONAL INFORMATION ABOUT THE CB

A CBTL data set also contains further valuable information such as mounting instructions for motion sensors, assessment limits from manufacturers and conversion data for motion measurements. This data is important for converting the rotary movement of a motion sensor into the linear movement of a CB's main contact.

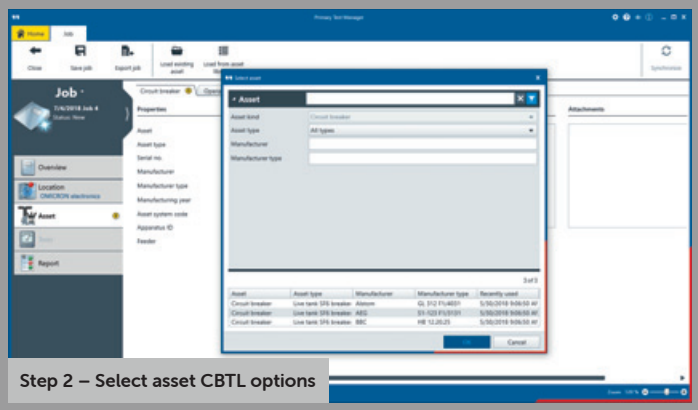
With CBTL, you can speed up your testing procedure considerably by using an optimised workflow:

1. Select your test location
2. Select your CB type and load pre-defined data from the CBTL, the associated test template will be loaded automatically
3. Execute all tests at once
4. Generate your reports automatically

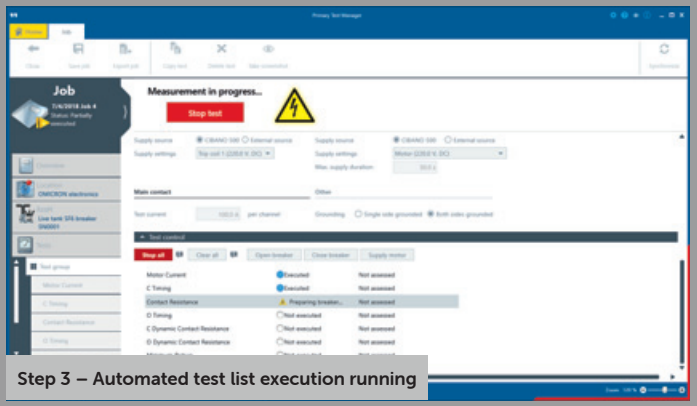
The CBTL will be available as an individual software license. The growing data pool will be maintained by OMICRON's team of developers and new data sets will be added on a regular basis.



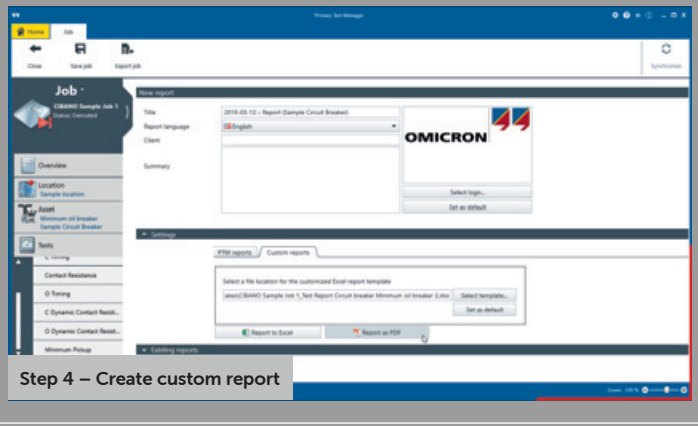
Step 1 – Create location



Step 2 – Select asset CBTL options



Step 3 – Automated test list execution running



Step 4 – Create custom report

Alexander Herrera
Application Engineer

Safe testing of GIS circuit breakers

I often heard test engineers complain about timing tests on GIS circuit breakers which were hard to perform or more or less unsafe. Our experts worked hard in order to overcome the existing technical challenge. Now I'm happy to share that we recently successfully demonstrated our new solution and it was both easy to use and safe. With its flexible design it can be performed on almost any kind of GIS circuit breaker while the test engineer stays safe due to grounding on both sides.

www.omicronenergy.com/GIS-breaker

OMICRON

Empty threats

David Manning, managing director at MIGSOLV, one of the UK's most secure data centres, gives us an insight into how he ensures the data in his facility is kept safe from physical threats and fire.

Despite enabling almost every aspect of modern life, data centres are something most people know exist, but few have considered. Data centres like our Gatehouse in Norwich, house servers and other IT hardware for businesses and organisations.

In turn, the hardware stores and processes critical data which enables many of the products and services we all use each day. Physical security is paramount to protect from threats like intruders, terrorists and natural disaster.

IT cannot function without electricity, so as well as drawing power from the grid, we also have enough backup power generation for eight days. Heat is harmful, so data halls are climatically controlled to prolong the life

"Location may seem like an unlikely component, but where a data centre is situated can have a significant impact on security"

of hardware. With electronics, also comes the additional threat of fire and the risk of water damage from traditional fire suppression. Fire protection is also critical and complex.

Let's start by considering physical security. We have to provide a deterrent and protect our client's hardware from people who might seek to harm it.

Our security centre is manned 24 hours a day, seven days a week, 52 weeks of the year. A team of three guard the entrance and patrol the perimeter which is protected by a 3m high fence, razor wire and microwave movement sensors. CCTV with 100% coverage and 93 days retention, provides an added deterrent and reference, should it be needed.

Data centre customers need access to their hardware to make changes and perform maintenance. Visits must be pre-booked and the security guards meticulously check photo ID. Once a visitor is cleared, they are given a proximity card which provides restricted access only to the areas they need.

Once cleared, they pass through a heavy turnstile and across the forecourt to the data centre building. If vehicle access is required to drop off or collect hardware, a vehicle trap ensures a heavy security gate (capable of deflecting a speeding vehicle) shuts behind them before the inner gate opens.

Not only is the entrance of the data centre building itself secure, but so is each internal door and final access to the data hall where we physically store and protect the IT and data. Final access to the data hall itself is gained by an additional iris recognition and proximity card check.

Once inside the data hall itself, security is no less rigid. Rows and rows of racks containing the IT hardware are split into self-contained aisles. Each aisle has security doors. Visitors can only access the aisle containing their equipment and a further card swipe will only open their specific rack.

Though the security in the Gatehouse is truly world-class, similar levels of security can be found in other purpose-built commercial data centres. The next threat is fire.

With gigawatts of electricity flowing though thousands of electronic devices, fire is a risk and must be contained. Smoke and

heat detectors throughout the building are linked to a complex building management system and two forms of fire suppression.

Electrical equipment and water don't mix well. Use of a typical water sprinkler system can cause significant collateral damage. Instead, the data hall uses inert gas which targets the location of the fire and starves it of oxygen. IT and hardware outside the affected area can continue to function normally for our customers.

The data hall is just one element of a data centre. To provide uninterrupted electricity should the mains supply fail, we have three large diesel generators with enough fuel for eight days at full charge.

Before they begin, a Rotary Uninterrupted Power Supply and banks of batteries seamlessly take the load. Temperature and humidity in the data halls is controlled by free cooling chillers which provide more than 340 days of low-energy cooling each year by harnessing the lower outside temperatures.

Plant and office areas are protected from fire by more inert gas or a dry pipe pre-action mist system. The sprinkler system is filled with compressed air which is released first before water flows, eliminating the risk of water leaks which could harm the sensitive equipment.

Location may seem like an unlikely component, but where a data centre is situated can have a significant impact on security. Flood plains, estuaries and coastal locations can provide an unnecessary physical risk.

Likewise, built up areas and proximity to bustling cities can also increase security risks. Our Gatehouse data centre is situated on a quiet trading estate in Norwich, Norfolk – statistically one of the safest areas in the UK.

Though the reality is complex, a data centre's purpose is simply to house and protect critical IT equipment and the data being stored and processed within. Nothing is more critical than physical security and fire protection.

Renovated at a cost of £12M in 2012, our Gatehouse data centre represents some of the latest and highest levels of security and fire protection protecting any physical asset in the UK, Europe and beyond. ER

Battling the breach

In this exclusive Q&A, Daryl Crockett, CEO and founder Valid Datum discusses the nefarious nature of the modern-day hacker, what our rights really are when it comes to GDPR and explains why something called 'micro-tokenisation' might well be the key to keeping breaches at bay.

What sort of things do hackers use our data for?

Hackers can have several motives for obtaining your data:

1. To sell your data to another criminal: If you are part of a mass data breach, then the most likely path is to sell it on the dark web. Stolen personal data can sell for $5-$6 USD. Stolen data can be sold many times over and can linger on the dark web for years.

2. To gain access to your banking or credit card info: Stolen data such as login IDs and passwords obtained from one site can be used to try as logins on higher value sites which contain financial information such as bank accounts or credit card info. The credit card information can be used to;

3. To gain access to your business or your employer's data: People are the weak link in a company's security, so thieves often target employees to gain access to corporate data.

4. For gaining access to a broader audience: Thieves steal your identity to take control of your email contact list and your Facebook and Instagram contacts to be able to mass market without your permission.

5. Personal maliciousness or mischief: Some hackers target high profile individuals as a form or personal or political vengeance or just for the sport of landing a big Phish.

Can GDPR actually help protect us from breaches? Without the correct ▶

Power For Our Generation

There are many ways to store or produce energy but when it comes to guaranteeing standby or emergency electrical power, in terms of cost, flexibility and responsiveness, there's no better option than a generator set from FG Wilson.

Our products range from ready-to-run generator sets to complete bespoke turnkey power systems with remote monitoring, all with lifetime product support from our dealers.

Based in the UK for the last 50 years, we've worked together with a multitude of customers in all environments globally and since 1990 have installed more than 625,000 generator sets around the world, with as much combined power generation capacity as the entire UK power grid.

To find out more,
visit us at **www.fgwilson.com**

FG WILSON

implementation, surely it's just four letters that don't mean a great deal?
The regulations alone which comprise GDPR do not protect consumers from data breaches. The simple fact is, even if an organisation reaches GDPR compliance, this achievement alone does not guarantee protection of personal data.

What the regulation does provide is an assurance that a GDPR "compliant" organisation identifies and maps all data sources and repositories, prescribed documentation, and that data risk assessments are created and maintained, and appropriate security controls are implemented.

The aggregate effect is a greater level of data privacy for EU citizens, however, the one advanced technical measure, called "micro-tokenisation" (a form of pseudonymisation) would most certainly protect personal data from the risk of mass data breaches. Micro-tokenisation is now drawing major interest from within the US military and other Government sectors and is garnering notice from commercial sectors as well.

ValidDatum strongly advocates the implementation of advanced technical controls for personal data which has been classified as "high risk". And not all software which pseudonymises data is created equal. Advanced technologies such as micro-tokenisation encryption (MTE) generates the strongest form of data pseudonymisation. That said, under GDPR, pseudonymisation is only "advised", not required.

Say a company does suffer a breach and our bank details are released, what rights do we actually have as the customer? This has happened to me personally and I was simply told 'contact your bank' which I (and I'm sure many others) don't think is good enough.
Under GDPR and DPA 2018, the language regarding communications to data subjects as a result of a data breach seems relatively straightforward:

"Where a personal data breach is likely to result in a high risk to the rights and freedoms of individuals, the controller must inform the data subject of the breach without undue delay."

But is there any recourse for the data subject whose bank details were compromised? As Europeans start to flex their collective data subject "muscles" by exercising their rights as EU subjects under GDPR, scenarios such as the breach of bank details as described will result in a significant increase in class action suits.

The British Airways data breach in September 2018 led to a massive class action suit. The results of this suit, and many others (unfortunately, the courts are now choked with these suits), will be watched closely (there have been no rulings on class action suits since the inception of GDPR). If the suit against British Airways is successful, each data subject will be able to claim £1,500

Frankly, the teeth behind GDPR data subject rights will only bear fruit if/when companies receive large fines (only small fines have been levied to this point) and courts rule in favour of class action suits, or a competitive market advantage is eroded.

> "It is critical that we do not confuse compliancy with security"

When it comes to the physical data centre wherein much of our private personal data resides, what levels of security do you feel are necessary to avoid a breach or attack?
Data centres should adhere to a list of standards and best practices, necessary to protect your firm's intellectual property, and sensitive personal data.

The list includes SSAE 16 (Type II), ISO 27001, SOC 2 Type 2, SOC 3 Type 2 and PCI DSS for those that require payment card information to be secured, and HIPAA compliance for those that are securing healthcare information as well as self-certifying to the EU-U.S. Privacy Shield Framework.

In addition, many organisations adhere to ISO "27K" standards, which is a series of standards which relate to process and physical controls of information security systems (there was initial confusion when GDPR was enacted – some organisations believed if they were ISO27001 certified, by default compliance with GDPR was obtained – but this is not true!)

It is critical that we do not confuse compliancy with security. While compliancy is a first step, and certainly a requirement under GDPR, do not be fooled into thinking your data centre is safe from malicious actors.

Additional security, such as implementation of a shared Digital Vault, private Digital Vault, and or deployment of technology such as MicroToken Exchange, provides unassailable data protection.

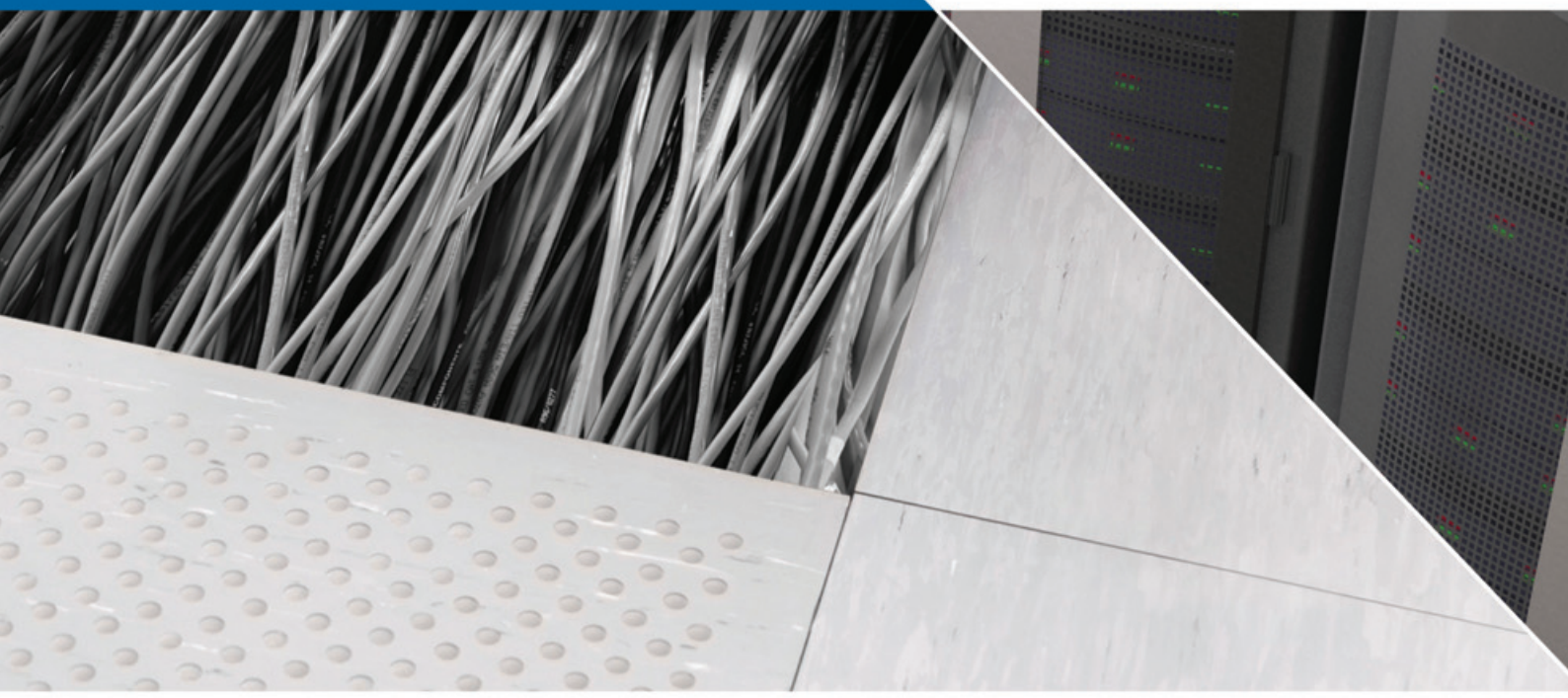
While many are lulled into a false sense of security assuming encryption minimises a firm's security risks, this is simply not the case. We read about firms almost every week who are encountering mass data breaches, due to the use of non-effective encryption schemes (the recent Marriott data breach being good example – PCI data, such as credit card numbers, were encrypted, but there is suspicion the attackers were able to access the two data silos containing the encrypted data and the encryption keys, which could allow them to re-identify the card numbers).

Should a hacker wish to infiltrate a data centre, how are they likely to approach it?
The hacker has many options relative to compromising a data centre. Let us focus on three popular techniques used by hackers in 2018:

- DDoS attack; a distributed denial of service attack utilises botnets (which attach to a machine as a result of malware) to overwhelm targeted web servers with traffic. A DDoS attack alone will not cause a data breach, but if control of a system is obtained a vulnerability can exist, leading to other methods causing the actual breach.
- Web application attack; hackers use methods such as SQL injection, cross-site scripting, and cross-site forgery to compromise applications and steal data (this method played a role in the British Airways data breach).
- Brute force and weak authentication; many systems still enforce single-factor, password-based authentication. Hackers utilise a host of methods, to simple guessing, stolen credentials, and automated password compromising tools. ▶

Hundreds of power whips.

Or one simple solution.



Increasing power density within data centres is an ongoing challenge for facilities managers. And the continual cycle of increasing power requirements has too often translated into more cables and whips under the floor. But Starline Track Busway is self-contained, customisable and flexible. So you can avoid a jungle of wires, and enjoy power expansion in minutes, not weeks. To learn more about our maintenance-free, reliable systems, visit **StarlineDataCentre.com/ER**.

STARLINE
TRACK BUSWAY

Cybercriminals generally fall into two main categories: State-sponsored cyber-terrorists and those attempting to monetise the activity. The hackers of today target all types of personal information for financial gain, but the most lucrative category of personal data is in the healthcare sector.

It is estimated a cybercriminal can sell healthcare data on the dark web for £200-300 per record, while credit card data fetches only £5-6 per record.

Do you think there is a skills gap present in the IT industry currently? Do 'the good guys' have the necessary skills to keep hackers at bay?

Not only is there a skill gap in the IT industry, but a shortage of cybersecurity professionals which has reached critical mass around the globe. A recent survey indicated 60% of companies across the globe feel they are at moderate or extreme risk of a cyberattack due to shortage of trained personnel.

> **60% of companies across the globe feel they are at moderate or extreme risk of a cyberattack due to shortage of trained personnel**

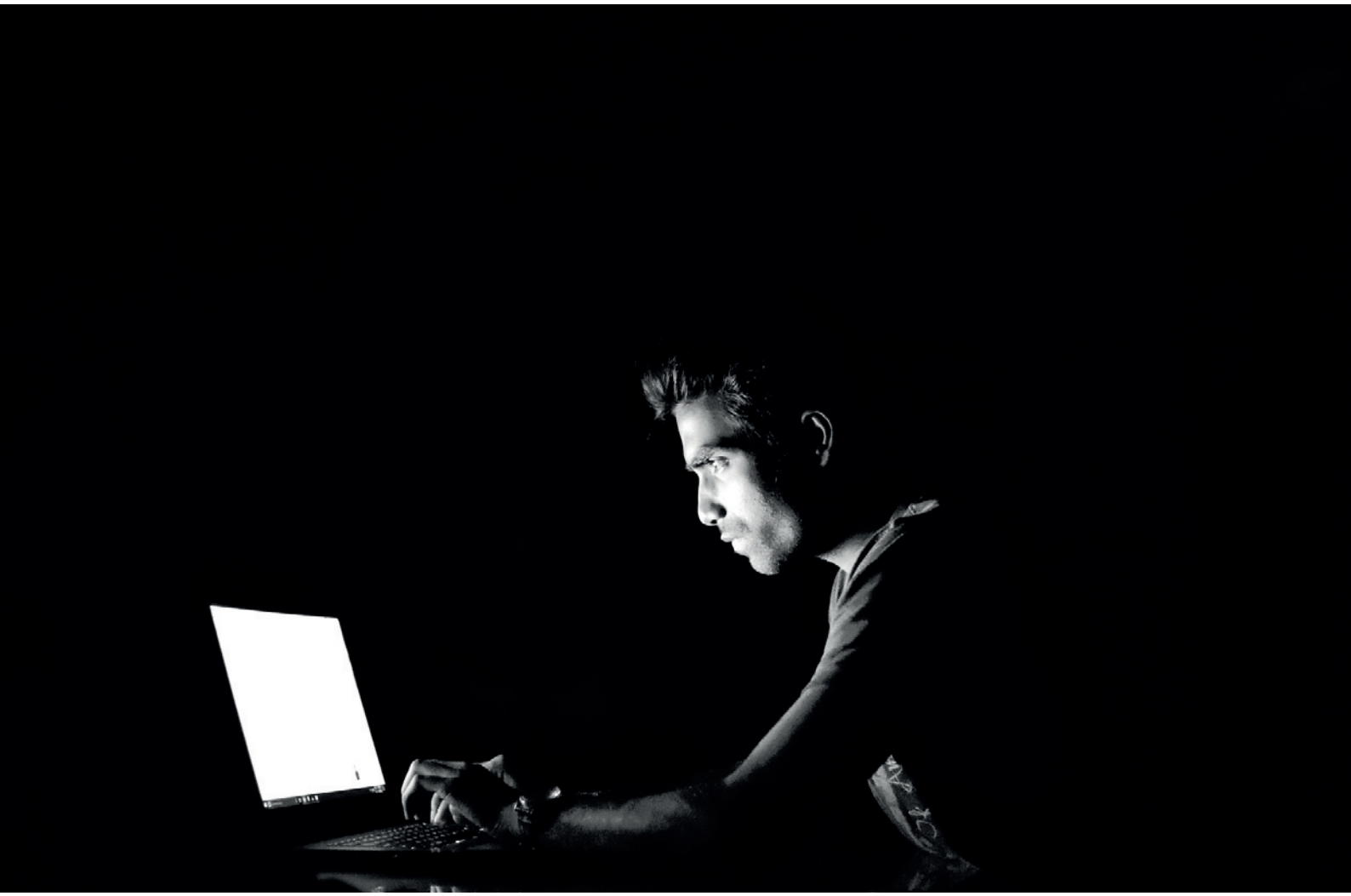
Final word: What needs to happen next to ensure our data remains safe?

Data privacy laws such as GDPR, have certainly increased personal vigilance relative to data privacy. The law has provided the consumer the opportunity to take more responsibility and ownership of how their personal data is utilised.

Not to be overlooked, these new laws have forced companies to place greater emphasis on consumer data privacy by increasing budgets to implement programmes and controls and creating new positions (such as Data Privacy Officer under GDPR) to comply with regulatory authorities.

As privacy and security by design principles are incorporated into new software and networking solutions, the risk of data hacks will be reduced. However, this transition will not occur overnight.

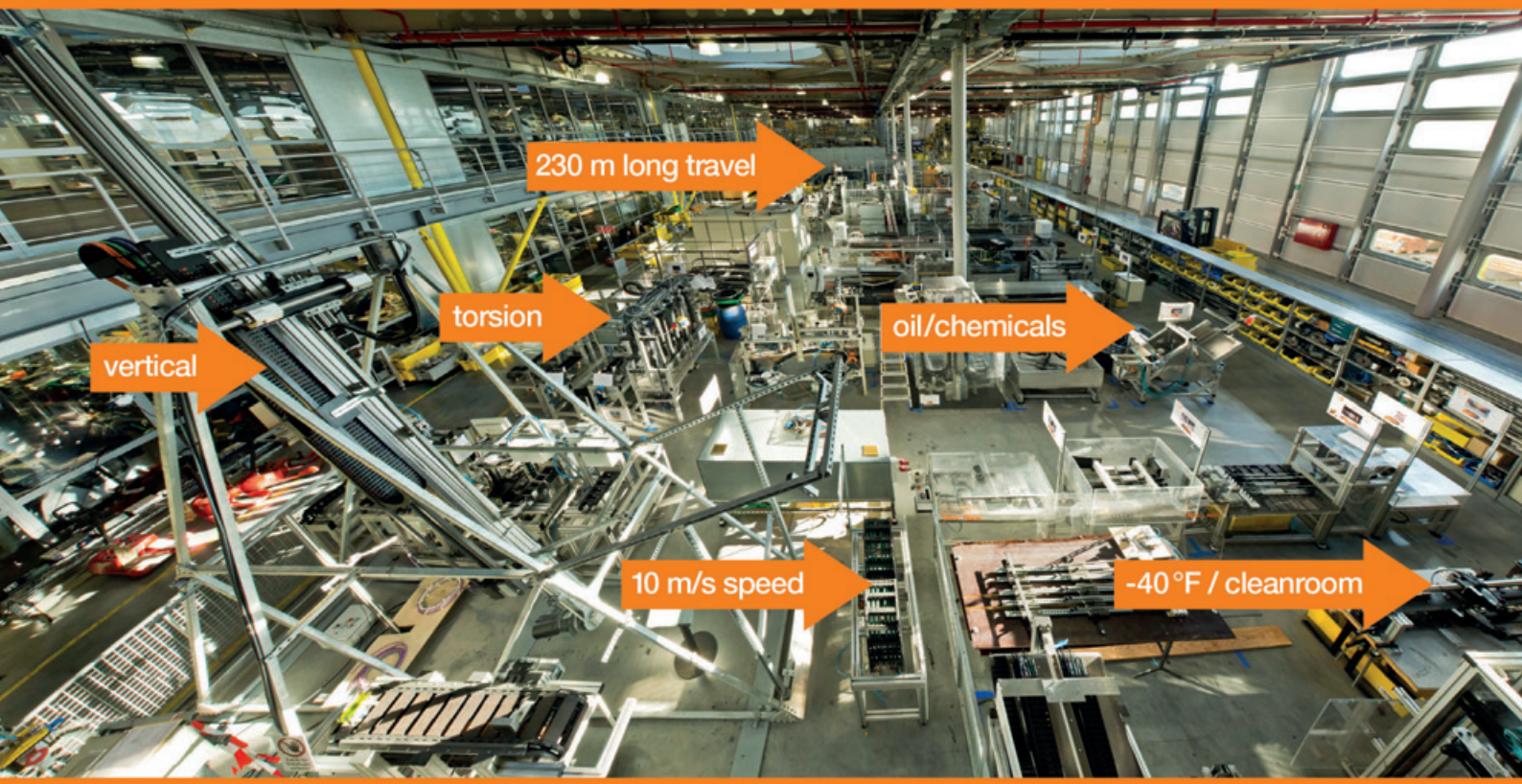
Many archaic systems are in place and budgets to upgrade can be limited. The first step without overhauling a system (assuming a GDPR compliance programme has already commenced), is to secure private data by using the strongest form of tokenisation method for both data in transit and data at rest.



Largest test lab for continuous-flex cables

#1

... number one in moving cables



Widest selection. Unmatched Testing. 36 Month Guarantee.

Guarantee igus chainflex 36 month guarantee

Reduce downtime with chainflex®
- Developed & tested in the 2750 m² lab
- 600 tests run in parallel
- 1.4 million electrical measurements/year
- 2 billion test cycles/year

Shop now: www.igus.co.uk/chainflexshop
Free samples available: www.igus.co.uk/cf-sample

igus®
plastics for longer life®

sales@igus.co.uk
Tel 01604 677240

What protects your fire protection?

Matt De Frece, divisional director at Power Control discusses the role of the UPS system in ensuring your fire protection system is failsafe.

Fire and methods of fire protection have been a hot topic uttered by many FM's, data centres, business owners and landlords following the tragic Grenfell tower incident. Fire suppression systems in particular have been a key focus when discussing businesses' fire protection strategies as being one of the most vital forms of fire safety.

Not to be confused with sprinkler systems, fire suppression systems can use a number of different extinguishing agents, and although parts of their systems may look similar, the way in which they extinguish or control fires and their applications are very different.

Most commonly found in server rooms, data centres and areas containing electrical or flammable equipment, a fire suppression system is the only viable option for fire protection actuating early in the event of a fire to protect the data and IT equipment. Water sprinkler systems would cause irreparable damage to the property it is intended to protect.

Moreover, when using fire suppression in a care home or residential environment, protecting the lives of those who live and work there is the highest priority. Primarily, fire suppression systems allow residents a delayed evacuation process, providing them with valuable extra minutes to exit the building before the blaze takes hold. As it is likely residents in a care home have limited or no mobility, this extra time is crucial. The likelihood of a power outage during a fire is high, making a form of backup power a vital piece of equipment for the care home.

> **"The likelihood of a power outage during a fire is high, making a form of backup power a vital piece of equipment"**

Despite their differences, both fire sprinkler and fire

suppression systems require mains power to interface with the fire alarm system. A power supply is vital for providing electricity to enable the releasing panel to interact with the fire alarm detection system, open pre-action valves, sound pre-discharge alarms, shut down ventilation and numerous other actions. Without a reliable power supply, the suppression system would not function if a fire broke out.

> **A power supply is vital for providing electricity to enable the releasing panel to interact with the fire alarm detection system**

As stated within the BS EN 50171, central power supply systems are intended to energise electrical circuits of automatic fire extinguishing installations, such as fire suppression systems, in the event of a mains power supply failure. A UPS system is commonly used as a method of backup power, where this system is used to feed essential safety systems, it must comply with EN 50091-1 and its relevant parts. This is in addition to the requirements set out in EN 50171.

Specialising in power protection for over 80 years, Italian UPS manufacturer Borri Spa has recently introduced their range of ECS (Emergency Central System) uninterruptible power supply units. Encompassing their proven industry leading UPS technology with a slightly modified twist for supporting emergency and life safety systems, Borri's ECS range of units meet both the Product Standard IEC/EN 62040 and the EN 50171 Standard. This provides versatility to use the UPS as a CPSS (Central Power Supply System) greatly reducing maintenance costs.

As the exclusive UK representative for Borri Spa, Power Control provides turnkey backup power solutions for emergency and life safety applications. Due to the high inrush currents required to start a pump, there are many pitfalls to be avoided in providing UPS solutions to support fire suppression systems. Many other UPS providers will either fail to take these start-up currents into consideration leading to an unreliable solution or an oversized UPS unit.

Specialising in all aspects of power quality and reliability, Power Control can provide a VSD (variable speed drive) alongside the ECS UPS. This means the start-up current is limited to 1x the running load preventing the need to oversize the UPS. Combining this technology with Borri's excellence in manufacturing, Power Control is able to offer the full package.

Power Control exclusively supplies, installs, commissions and maintains an extensive range of Borri UPS units within the UK market. These include 3 phase systems from 10kVA to 6.4MVA.

For more information please visit www.powercontrol.co.uk, email info@powercontrol.co.uk or call the office on 01246 431431

PowerControl

Shifting gears

Natalie Sauber, market intelligence lead at Arcadis, explores how autonomous and connected vehicles are driving a new generation of data centre requirements.

When it comes to the future of transport, Connected and Autonomous Vehicles (CAVs) are among some of the most disruptive technologies we're seeing today. This gradual shift towards driverless vehicles brings many potential benefits, not least of which in helping to increase road safety, reduce traffic congestion and pollution, minimise fuel consumption and greatly improve the passenger experience.

The huge amount of investment from major automotive manufacturers coupled with new entrants from the technology sector brings the potential for truly transformative change in the way that people and goods are transported.

By 2025, the industry predicts that CAVs are estimated to generate over $200 billion in annual global revenue for auto manufacturers and others. However, a less obvious consideration is that these vehicles will also transmit over 100 petabytes of data to the cloud each month.

To put this in perspective, a petabyte is just over one million gigabytes (the equivalent of digitising approximately half of the printed material ever published). Furthermore, by 2050, the data volume between vehicles and the cloud will require 10 exabytes per month, approximately 10,000 times larger than the present volume. One exabyte is around a thousand petabytes, and equivalent to 250 million DVDs of data.

Clearly, the transfer and management of this volume of data will create unprecedented challenges. But, for every challenge there is an equal opportunity, ▶

Megger introduces next-generation digital multimeters.

Electrical test equipment manufacturer Megger has launched its new series of next-generation AVO800 multimeters, designed to provide electrical contractors and field service technicians with best-in-class level of data & results validity as well as a comprehensive host of new and advanced product features.

NEW TECHNOLOGIES

In line with the firm's focus on creating easy-to-use and safe portable test solutions, Megger's two newly released units – the AVO830 and the AVO835 – combine the renowned build and performance of the historical AVO units with new, proprietary technologies such as simultaneous AC&DC voltage measurements, smart capacity discharge function and non-contact detection of live circuits and conductors.

"We are excited to bring to market two state-of-the-art product solutions to truly help our customers make vital decision about their most important assets with peace of mind, which adds complimentary value to our new AVO800 series and takes 'the Megger way' of testing to the next level once more." – states Simon Wood, European Distribution Manager at Megger.

PROTECTION

As Megger remains devoted to safe working conditions, the new AVO800 instruments have the highest level of protection in the industry – CAT III 1000V & CAT IV 600V rating. In addition, a phase-sequence indication function proves invaluable on three-phase systems, ensuring the correct run of operations without the needs of additional test leads or probes.

For more information about Megger's new AVO800 series, please visit uk.megger.com/AVO800 or email: uksales@megger.com

Megger

and data centre providers must prepare themselves for this growth, both in the cloud and at the edge.

CONNECTING AT THE EDGE

Connected and autonomous vehicles will soon communicate in real-time between each other (V2V) and vehicle-to-everything (V2X) for enhanced safety and convenience. For CAVs to operate safely and efficiently, reliable ultra-low latency vehicle-to-infrastructure (V2I) communication is critical.

As it stands today, the 4G cellular network can facilitate management of certain tasks back to the CAV, such as weather and road conditions and real time information on accidents. However, providing high definition maps and identifying obstacles and objects moving near the vehicle requires constant reliable processing with low latency.

Far better is the 5G network currently being rolled out, which processes data up to 1,000 times faster than the existing 4G networks. The 5G cellular base station network will support connectivity and control for the CAVs, as the V2I wireless system will be capable of managing all the different tasks required by the AV, while at the same time operating under constant network connectivity.

IMPACT ON DATA CENTRE INFRASTRUCTURE AND MANAGEMENT

The transfer into hyperscale cloud facilities for big data analytics and management precedes a fully integrated (V2X) eco-system. However, delivering that data to the data centre is challenging, with estimates suggesting that approximately $1 million needs to be spent on data centre infrastructure for each AV.

If we believe the predictions that 10 million self-driving cars will hit the road by 2020, data centres are going to require immense investment in computer tech, networking, storage and other infrastructure. We seem to be at a crossroad, as there is a dire need for new approaches on data centres to meet the demands of the new mobility value chain, from data ingest to deep learning and simulation capabilities.

We know that data centres continue to see huge levels of investment across the world. The hyperscalers and cloud providers are bringing more capacity online at an unprecedented rate, pushing the boundaries of lean construction methods.

Colocation providers are developing ever more sophisticated systems to allow their customers to manage data generated traditionally in servers, as well as that created at the edge. There is also a need to carry out analytics in real time, as well as the big data crunching that is carried out in the cloud.

> **By 2025, the industry predicts that CAVs are estimated to generate over $200 billion in annual global revenue for auto manufacturers and others.**

Consequently, the use of Artificial Intelligence (AI) will shape a new generation of data centres equipped with new hardware and software architectures enabling large-scale, real-time analytics and machine intelligence. Soon, computer and storage will be optimised by introduction of edge and quantum computing to work seamlessly as an extension of the overall IT system. There is a definite need to increase network capacity between vehicles and the cloud by implementing edge computing and more efficient network designs.

MARKET INVESTMENT

Dedicated data centres or research institutes for CAVs are scarce. Only recently did the UK see a significant financial investment made towards elevating this to the next level. The West Midlands Combined Authority (WMCA) will receive up to £20 million to allow Warwick Manufacturing Group (WMG) to create the UK Mobility Data Institute; a focused research centre to collect, process and analyse transport data generated by autonomous vehicles, along with smart charging of electrified vehicles.

OEMS HAVE TAKEN CONTROL AND OWNERSHIP OF THEIR DATA CENTRES

A number of car manufacturers have also pledged to build data centres over the coming years. In 2016, Toyota announced plans to build its Data Centre for Connected-Car Data. Meanwhile BMW is planning to use IBM's cloud infrastructure to deploy its new platform for collecting data from connected cars. In 2017, Ford announced plans to build a $200m data facility centre to store connected car data in Detroit. The American manufacturer predicts that their data storage requirements will rise from today's 13PB to an astounding 200PB by 2021.

FUTURE PROOFING

The recent increase in data centre construction activity is clearly accelerated by the industry readying itself for these data consumption increases, and the draw on construction resources is going to increase in line with demand.

Future proofing global supply chains is going to be an essential step in meeting these requirements, as is careful site selection due diligence, which enables access to the best site locations and the critical infrastructure necessary for their future data centre needs. By effectively bridging the gap between data centre providers and city policy makers, can we improve network implementation times and significantly make a difference to the industry. ER

We really hate interruptions.

But we quickly wanted to inform you of our new name.

Uninterruptible Power Supplies is becoming Kohler Uninterruptible Power.

WHY THE CHANGE?

It is a decade since we joined Kohler Co., one of the largest privately held companies in the US, and nearly 100 years since they first stepped into power products. And with our solutions now spanning UPS, generators and emergency lighting inverters, plus class-leading 24/7 service, it is simply time our name reflected who we are and all we do today.

Uninterruptible Power Supplies Ltd
A KOHLER COMPANY

KOHLER POWER uninterruptible

kohler-ups.co.uk

IT innovation: Paving the road to self-driving cars

Jack Pouchet, vice president, Market Development, Vertiv and Jodie Bare, deputy program manager, Smart Columbus, explore why the change to transport as we know it may well be imminent.

After just three turns in any given chess match, there are 121 million possible outcomes. Think about that. Two players, 32 pieces, on a board of 64 squares. And just three turns into the game, there are roughly as many potential outcomes as there are people in Japan.

Now think about your drive to work. The average person's commute is about 25 minutes. How many data points are processed in those 25 minutes? We're constantly calculating and adjusting to countless variables – speed, road conditions, traffic signs and signals, pedestrians, other cars on the road, even animals that dart in and out of traffic.

> **On your daily commute, your average driverless car will generate data equivalent to about 2,000 movies. That's every car, every hour.**

Every decision we make – those we consider and the others that take place virtually subconsciously – adds countless possible outcomes to our daily drive. That we manage this every day, mostly without incident, is a marvel of the human brain that we take for granted.

Now consider this: More than two decades after a computer named Deep Blue defeated world chess champion Gary Kasparov in a game of chess, we are on the verge of a similar breakthrough with our cars. Self-driving vehicle pilots are taking place in 19 cities, with infrastructure and industry insight expanding daily to enable future deployments.

Columbus, Ohio, is one of those cities. Smart Columbus is using a $50 million grant from the US Department of Transportation (USDOT) and $522 million more in private-sector investments to explore and evaluate advanced transportation systems, including self-driving vehicles.

The pilot sponsored by Smart Columbus and Drive Ohio involves a self-driving shuttle that transports passengers to and from popular downtown destinations. It launched in December and is an educational milestone on the path toward future deployments in Columbus neighborhoods and beyond.

The infrastructure challenges associated with an autonomous future are real, however. All of those variables and decisions we make during that 25-minute drive to work require constant data transmission and analysis and real-time adjustments. That requires sophisticated computing not just in the vehicles, but along the roadside – every roadside, everywhere.

Autonomous vehicles will generate almost two terabytes of data just on that drive to work. That means on your daily commute, your average driverless car will generate data equivalent to about 2,000 movies. That's every car, every hour.

The IT systems needed to make that a reality must be incredibly powerful, small enough to mount on light poles or stored in ubiquitous, nondescript roadside enclosures, capable of low-latency transmission, and uncompromisingly reliable. That last part requires power protection, thermal management and, importantly, remote monitoring, management and service capabilities. These sites will make up a micro-edge, capable of instantaneous computing and networked not just with each other, but with data centres and cloud resources around the world.

Smart Columbus is working with a number of partners to find solutions to those infrastructure challenges and other speed bumps on the way to a driverless future. One of the most powerful tools in that effort is the Smart Columbus Operating System, an open source data platform that provides open access to the city's latest mobility data.

The operating system aggregates data from a wide variety of sources, allowing Smart Columbus to glean insights from across the community and from outside resources through USDOT. It is revealing important data about driver behaviour, traffic and parking patterns, and technology performance, all of which will contribute to a more effective strategy for implementing self-driving vehicles.

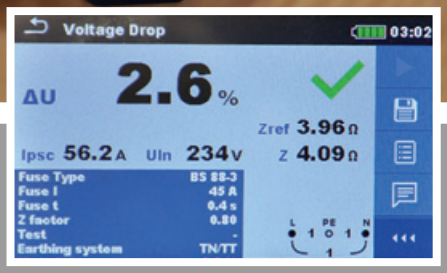
For its part, Vertiv is engaged not just with Smart Columbus, but across the industry to develop intelligent, reliable infrastructure solutions that support 5G and edge networks. Those efforts will enable self-driving cars, Smart Cities, virtual and augmented reality platforms, and widespread applications of the Internet of Things.

As much as the car is the natural focus of so much discussion on this topic, the reality is this is a data centre and IT challenge that carries with it all the individual issues driving data centre innovation every day. Those include: how to effectively store, analyse and move mountains of data, how to reduce latency and move that data quickly, and how to ensure those systems that are becoming absolutely mission critical remain online at all times and in all conditions.

Bottom line: We're moving closer to an autonomous reality. Data centres and advanced networks will make it possible, and our Deep Blue moment is closer than you think. ER

Why all the fuss, asks METREL®

The current spat between tester manufacturers over the suggested need for voltage drop measurements and power quality in the 18th Edition amendment 1 is unfounded according to Metrel.



"Users of Metrel's multifunction testers are having difficulty understanding the spat between some of the other manufacturers," commented Brendan Beaver, sales manager at Metrel, electrical test solutions provider.

The spat in question, is over the recent exchanges concerning the need for voltage drop measurement capability which have appeared in the media, at exhibitions, within on-line forum sites, and in printed statements distributed amongst the wholesaler community.

"So what if the 18th Edition's amendment 1 does or does not require the ability to perform voltage drop measurement and power quality analysis."

"When the regulations do change, be it Amendment 1 or Amendment 2, Metrel users will have been ready for some time. In fact, when the concept of voltage drop was introduced in the 17th Edition Amendment 3, Metrel engineers responded and introduced the function to their multifunction testers."

This modification showed the benefit of using modern display technology. Introducing the new tests was relatively easy with the dot matrix displays. It was a matter of changing the firmware and designing new screen layouts for the user interface. The use of a touch-screen display meant no restriction due to the use of rotary switches.

Our engineers are not limited by the old-fashioned custom LCD displays and rotary switches, so they can respond rapidly to changes of regulation.

Metrel customers are the winners as they can be assured that their testers are future-proofed.

Electrical SafetyUK

Consultancy | Training | Assessment

The UKs foremost exponent of **ARC FLASH** technology

Early Bird Offer save 15% (Ends 31st March)

Arc Flash International Conference

Manchester, Radisson Blu Hotel Manchester Airport

Tuesday 24th September 2019

9am to 4:00pm - £275.00+VAT

The NEW 2018 IEEE 1584 – Changes | New Arc Flash Calculations | How it Affects Europe

Key Note Speaker

Jim Phillips

Jim is Vice-Chair of IEEE 1584 and International Chair of IEC TC78 Live Working. For over 35 years, he has been helping tens of thousands of people around the world understand electrical power system design, analysis and safety. Having taught over 2500 seminars during his career to people from all seven continents, he has developed a reputation for being one of the best trainers and public speakers in the industry. For more information about Jim, visit www.Brainfiller.com

Conference Agenda

Jim will discuss the changes, walk you through the calculations using his new worksheets and explain how the 2018 edition is used in arc flash studies. Jim will cover:

- Overview of changes to the 2018 Edition
- Arc Flash circuit dynamics and testing
- Electrode Orientation VCB, VCBB, HCB, VOA, HOA
- Enclosure size correction factors for different sizes
- New Interpolation Method for improved accuracy.
- Working distances, gaps and arc duration
- New Incident energy and Arc Flash boundary calculations
- Arcing current variation factor
- And Much More – Full agenda available upon registration

NOT TO BE MISSED

This unique conference is a superb event which pushes the boundaries of all arc flash conferences previously delivered in the UK. The program and expertise on offer will establish current best practice and provide ground breaking information to assist professionals in all sectors of industry in the management of the arc flash hazard.

CONTACT US for the full conference details or to book your early bird space

0800 652 1124

+44 (0) 1709 961 666

info@elecsafety.co.uk

www.elecsafety.co.uk

Proudly Sponsored by

EasyPower Power made easy.

ROSS Quality Protective & Safety Wear

Electrical Safety (UK) Limited, 2 Genesis Park, Sheffield Road, Rotherham, S60 1DX. United Kingdom

Secrets to success

Darren Watkins, managing director of Virtus Data Centres analyses the struggles and successes of data centre infrastructure management and takes a look at what makes an ideal DCIM strategy.

It's no secret that the driving force behind Data Centre Infrastructure Management (DCIM) is the need for complete visibility into a data centre in order to better manage costs and capacity.

An ideal DCIM strategy should enable the centralised monitoring, management and intelligent capacity planning of critical systems – helping data centre managers address difficult challenges, including escalating energy costs, tight budgets, dwindling network capacity, limited floor space, and pressure for more uptime. Leveraging DCIM, companies can find new ways to maximise data centre ROI and achieve much greater levels of efficiency.

So, if it's well recognised that DCIM brings a multitude of benefits, then why is it not yet used by everyone? Why has it simply not reached its potential? And what can the industry do to ensure businesses are benefiting from the rich analytics that DCIM offers?

What's the issue?

There's been a tendency to be downbeat about the subject. Some naysayers, who believe that DCIM is failing, suggest the fault lies partly with the industry for over-hyping the tech's potential, and partly with customers for not really understanding the exact challenges they were seeking to solve with data centre management software.

Although it's a fairly straightforward technology, there is a fundamental awareness problem amongst IT departments. If customers don't know what the software is and how it can save on their power usage and overall costs, there's a risk it will be overlooked and under-utilised, as is evident at the moment.

> **Put simply, if you do not measure, you cannot manage.**

Even if the benefits of DCIM are known, barriers to adoption still remain. This is particularly true for older generation data centres, not originally designed for DCIM, which struggle to install it.

The ability to flex power and usage requirements up and down come into direct conflict with many commercial data centre models, which rely on long term, costly and inflexible contracts to safeguard their operations. This means that having DCIM under these conditions becomes ineffective unless customers have the power to amend their contracted usage commitments to reflect actual real-time usage.

Issues over cost are further complicated by the fact that DCIM spans both IT and Facilities – two areas which don't normally overlap. This has been known to create disagreements, for example, over whose budget should be used to pay for DCIM, with neither side stepping up to take responsibility.

So, what's the answer?

There are two issues for the industry to solve here. The first is a fundamental one – understanding what DCIM is – not a single piece of software, but a software category consisting of two core building blocks: DCIM monitoring, and IT Asset Management (ITAM). Businesses must also determine how to implement DCIM, and who takes responsibility for the tools. For

many, a successful DCIM strategy involves three key stages:

Strategic: Developing a robust business case for investment in DCIM.

Tactical: Scope and specify a DCIM system and select the solution that has the best match to your requirements.

Operational: The process of assessing your existing data centre, rack-by-rack and shelf-by-shelf to populate a DCIM with accurate data.

This is a logical approach and will pay dividends for companies who will then be able to reap the rewards of DCIM.

The second hurdle to overcome is more complex and requires the IT industry to communicate better with its customers. We need to ensure businesses fully understanding the benefits of the technology, and why it's imperative to their data centre strategy.

DCIM software monitors all the critical systems in a data centre in real-time, so users know how to optimise the use of space, power, cooling, and network capacity. What's more, DCIM monitoring generates an alarm when something is headed for disaster, before the catastrophe happens, so changes can be made to reverse the risk.

Whilst it's important for data centre operators to gain access to what's happening in their facility in real-time, DCIM can also help with future planning. When data centre managers know what equipment they currently have, how much power it's drawing and where that power is coming from, amongst other vital information, they'll be able to determine how much more equipment their facility can handle. And by optimising capacity, they can delay, or altogether eliminate, the need for constructing a new facility.

The collaboration story

So, DCIM is important. But its benefits don't just apply to one organisation, but for entire industries.

In a digital economy, we know that businesses are increasingly relying on their data centres – and so, the space, power and cooling demands placed on them have also increased exponentially. To tackle this global problem, data centre providers and customers need to collaborate and examine how they can work together to increase efficiencies – reducing spiralling energy consumption and cost.

> **Although it's a fairly straightforward technology, there is a fundamental awareness problem amongst IT departments.**

DCIM is an important way of facilitating this collaboration. Traditionally, data centre providers have been quick to highlight if customers need to buy more capacity, but not as quick to advise when to scale down requirements. DCIM creates this visibility and puts the control firmly back into the power of the customer – giving them greater visibility into their daily usage and ▶

allowing them to manage their capacity in real-time and act on the analytics.

Of course, this is only useful if they have the flexibility to scale down their contracts in the event that they're not using the initially agreed amounts. Several innovative providers are already offering this capability and actually using DCIM to create new commercial models, which makes choosing the right intelligent data centre provider more critical than ever.

What's in it for providers?

If these hurdles are overcome, we believe that DCIM will cement its place as an essential part of the intelligent data centre. With more customers come more demands and they will expect their providers to offer the most advanced solutions available.

The benefits for providers are also clear. Supplying visibility also creates value to providers – it creates trust and strengthens the customer relationship. And rather than this perceived fear that DCIM reduces the control of operators, it is simply a realigning of focus – giving the customer access to what is rightfully theirs. It's their data, their power consumption, why shouldn't they be allowed to both monitor and control it?

Through the use of DCIM, operators will be able to ensure that they only use the amount of power absolutely required by their customers, and the customer will be able to scrutinise this usage. In order to fully benefit from the use of DCIM, data centre providers will need to allow their customers to act on the results and scale their usage up or down accordingly.

Conclusion

So, whilst we believe that there are still hurdles to adoption, the future is bright for DCIM. Put simply, if you do not measure, you cannot manage.

DCIM software has the potential to reduce energy consumption and reduce the management overhead associated with planning the deployment of new IT systems within existing data centres. It provides a more granular approach to data centre energy management and potentially unites the IT and Facilities view. It offers benefits to providers too, strengthening customer relationships exponentially.

It's vitally important we overcome DCIM issues in order for the entire industry to benefit.

Outperform the rest with the CM Series

Get the right tool for the job with the new range of Martindale clamp and flex meters

TRUE RMS

Whether it's low current AC, DC for PV and battery systems, or leakage current measurement to troubleshoot RCD tripping, get the job done with the CM Series.

- AC, DC, leakage clamps and flex meters with ranges from mA to kA
- Pocket sized, tough and easy to use
- Autoranging True RMS measurement for reliable results every time
- High resolution to measure the smallest of currents
- Flex sensors for large and hard to reach conductors
- Two year warranty and clamp meter case

CM57 AC

CM69 AC Leakage

CM79 AC/DC

CM95 Hi Res AC Flex

Available from your wholesaler and online

www.martindale-electric.co.uk

Call: 01923 441717 **email:** sales@martindale-electric.co.uk

MARTINDALE ELECTRIC

Digital disruption increases need for fibre

Dr. Rick Pimpinella, Panduit fellow, Panduit Corporation discusses why our penchant for data means the need for multimode fibre in the data centre is now more prevalent than ever.

Digital disruption across most market sectors is continuing to drive the need for higher performance infrastructure within the burgeoning data centre market. Enterprises in financial services, media, e-health and retail, especially online, are at the forefront of phenomenal growth in data traffic.

A consequence is a future where a high percentage of that traffic will be within the data centre environment across machine-to-machine applications, utilising technologies such as AI (Artificial Intelligence) and ML (Machine Learning) to communicate petabytes of data daily. Physical infrastructure architects are now scrutinising the latest and next generation products and platforms to ensure data centres have the capability to scale exponentially to satisfy this data traffic requirement.

The challenges for the network are ever growing demand for faster speed, 40GE (Gigabit Ethernet), 100GE today and 200GE and 400GE within three years, and the physical distances to be covered. The connectivity to the server stack is changing,

with 25GB servers already deployed in web platform data centres. As a result, cable and switching fabric must have the capability to service the roll out of 50GB server technology, which is already underway.

By their nature, AI and ML solutions rely on large data sets, preferably multiple terabytes and soon to be petabytes, to analyse and learn. This quantity of data already requires 50GE and the demand curve is forecast to rise sharply to 100GE.

Expectations are that Ethernet based networking will continue to provide near-linear scalability, however, the volume of data traffic generated can be significant. Therefore, intelligent handling is required to ensure the network is not overwhelmed, resulting in latency and even outages.

Already 50GE and 100GE ASICs (Application Specific Integrated Circuits) are deployed by hyperscale data centres. This creates another pressure point for network architects to dynamically meet this growing diversity of communications patterns across the network, with different traffic classes having separate networking requirements for throughput flows, deadline flows and interactive flows.

A clear demonstration of this move towards increased performance is the growth in higher speed port shipments, with 25GE and 100GE port speeds combined at 46% share, will match the shipments of 10GE ports by 2021. The direction of travel for speed and capacity is only going one way and the networking technology that organisations trust to scale linearly is Ethernet, whether on single-mode or multimode fibre optic cable.

With 40/100GE already being deployed and the standards for 200/400GE under approval and published by the IEEE, Ethernet is the preferred networking platform. It can deliver data centre architecture and design to meet future application needs whilst providing low operating costs today.

Multimode fibre will continue to be the predominant fibre optic cable used in the market as it continues to offer key benefits to most data centre builders and operators. Multimode fibre provides a lower cost solution over single-mode as it utilises cheaper laser transceivers, its installation allows wider alignment tolerances, and it consumes less power. Single-mode fibre is

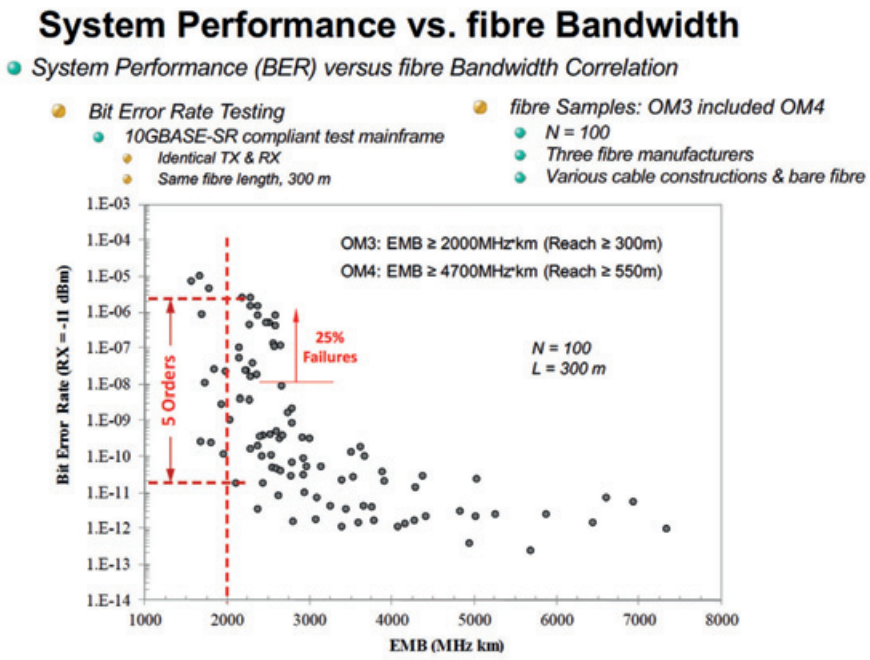


Figure 1. Channel Performance vs Fibre Bandwidth (EMB – Effective Modal Bandwidth)

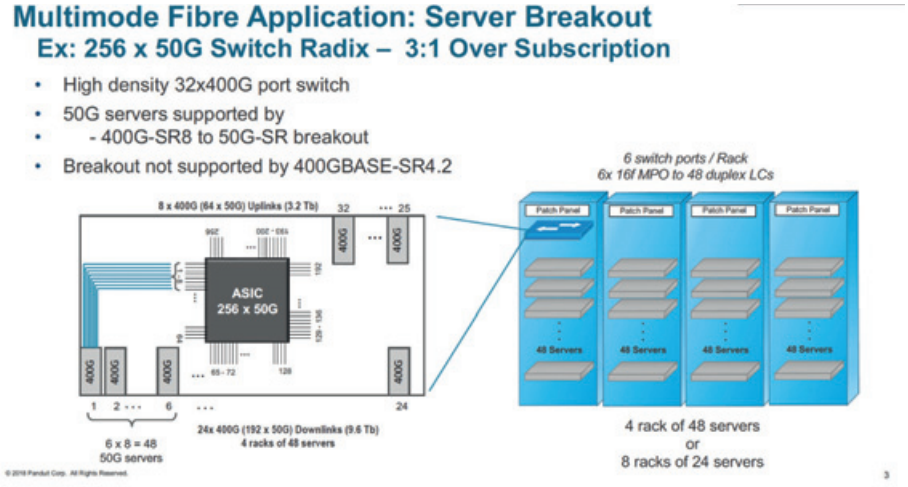
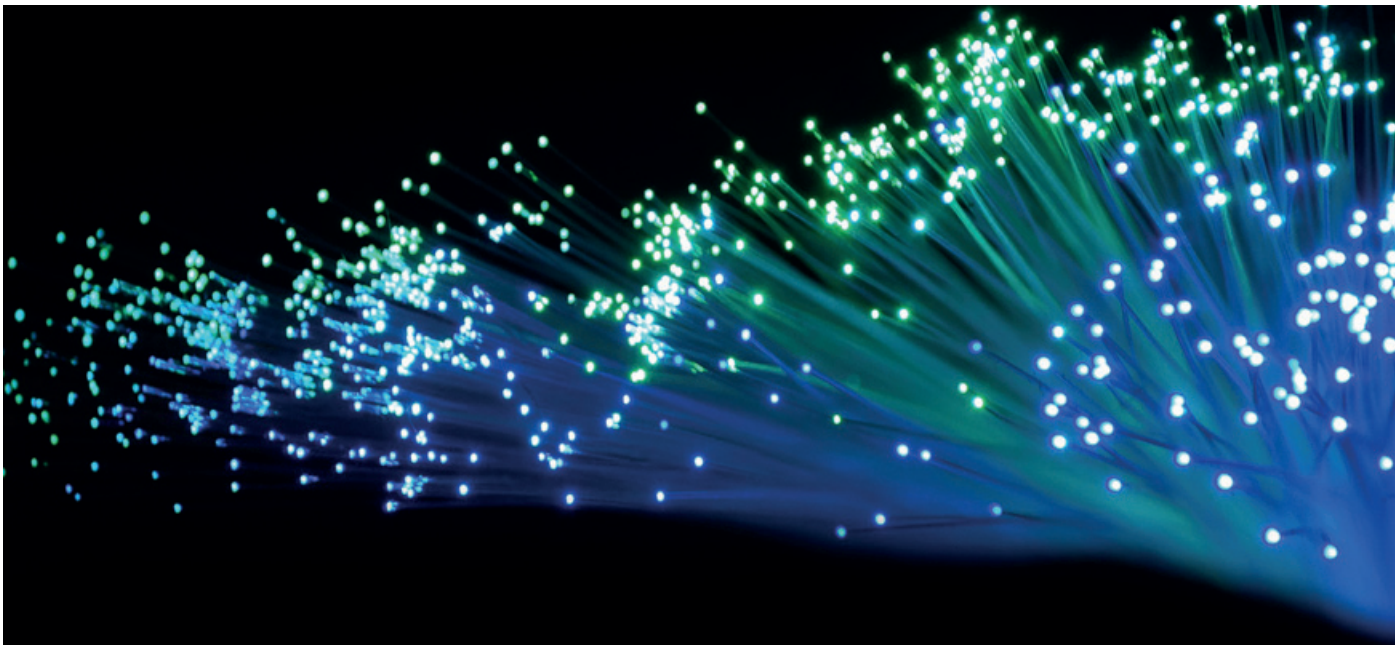


Figure 2. Multimode fibre switch to server breakout application

a less robust connectivity solution, whilst multimode is more tolerant to dirt and dust, it does not require high return loss, is resilient to multipath interference and is more forgiving to long-term connector degradation.

Although infrastructure within the data centre accounts for around 2% of the build cost of the site, once operational the percentage of outages where infrastructure is the cause is much higher. As the monetary cost of outages increases and reputational damage can be even more financially severe, the advantages for installing the highest quality infrastructure solutions become obvious.

As the market for fibre optic cable technology has advanced, it has become clear that the variation in the quality and capability of the various manufacturers' cabling solutions has diverged. Recent market testing of cable illustrates the importance of understanding the specification and identifying the capabilities of the manufacturers of the fibre optics being supplied. ►



THE FUTURE OF MULTIMODE FIBRE

For short reach applications less than 100m, such as switch to server and server to server (machine to machine) interconnections, multimode fibre adds real benefit inside the data centre. Industry standard fibre which is laser optimised now provides a scale of fibre capabilities to assist data centre operators to plan successful infrastructure installs and upgrades dependent of operational requirements up to at least 400 Gb/s.

As per table 1, OM3 and OM4 are designed for high bandwidth at 850nm, whilst OM5 is specified for longer wavelengths (953nm), SWDM-4 applications. The dispersion compensating OM4+ is an essential element for single wavelength and BiDi systems applications.

In technology development terms, the move to 40Gbps saw the emergence of parallel optics. This was because the VCSELS (Vertical Cavity Surface Emitting Laser) used in fibre optics transmits at 10Gbps. To achieve higher data rate transmission, aggregated lanes are used. To reach 40Gbps four parallel fibres aggregate 10Gbps per fibre.

The addition of lanes had an unforeseen benefit. It allowed switch manufacturers to increase port density. This was possible because each lane in Ethernet is independent. So, instead of building switches with 96x 10GB ports, this was condensed to 32x 40GB high density ports. This is known as breakout and is important because everything that has been worked on to develop standards to get to 40Gbps, 100Gbps, 200Gbps and 400Gbps is breakout compatible.

This year 50GE, 100GE and 200GE multimode fibre standards will be ratified. Over the next three years 100Gbps breakout at 4x 25G lanes and 200Gbps breakout at 4x 50G lanes will be widely deployed.

Currently a new IEEE 802.3 task force has been established (802.3cm), in which Panduit is a key contributor to define and propose standards. One objective is to define 400Gbps across eight separate 50Gbps lanes to be used for connecting servers and switches, figure 1. There is also a specification for 400Gbps over four lanes at 100Gbps per lane, each lane carrying two wavelengths – which Panduit supports, but will not support breakout solutions defined in IEEE.

Table 1. Laser optimised Multimode Fibre types

Fibre Type	EMB at 850 nm (MHz·km)	EMB at 953 nm (MHz·km)
OM3	2000	NA
OM4	4700	NA
OM5	4700	2470
Dispersion compensating OM4+	5500	2000

THE PATH TO 800GE

Forward towards 800Gbps and beyond will also likely be breakout compatible. This is a sensible path that will reduce 800Gbps switches down to 32 ports. This can be achieved by specifying 100Gbps serial transmission per lane. Feasibility of this solution was demonstrated recently at the 2018 Optical Fibre Conference (OFC) by Panduit researchers. Breakout at 800Gbps will be far more efficient in terms of heat dissipation, eye safety, and space and power densities. It will also bring down the cost of manufacture.

CONCLUSION

Multimode fibre is essential for high speed data traffic in data centres. The next step up is already in discussion by the Ethernet Alliance and an IEEE ad hoc group which are mapping a journey to 800GE and 1.6TE networks.

There are however questions on the suitability of multimode fibre beyond 800GE for server to server connectivity due to its relatively short reach. At that point, Panduit is proposing multiple lanes 100Gbps serial data transmission, as it believes that utilising 100Gbps serial and bi-directional SWDM2 a data rate of 1.6Tbps can be achieved. Until then, multimode fibre's position as the choice for most data centre infrastructure is confirmed. ER

OLSON®

SEE US AT STAND
D848
REGISTER FOR
YOUR FREE TICKETS!
12-13 March 2019 ExCeL London

DATA CENTRE WORLD

POWER DISTRIBUTION UNITS

NEW INTELLIGENT POWER MANAGEMENT

- Remote Monitoring
- Remote Switching
- Local Coloured Display
- Programmable Sequential Start
- External Temperature & Humidity Measurement
- USB Port for Storing & Recalling Setup
- Can Be Specified With Any of Olson's Data Centre Products or as Part of a Bespoke Design or an In-Line Version for Retrofits

MORE FROM OLSON

- Sequential Start
- Combination Units
- International Sockets
- Automatic Transfer Switches
- 19" Rack & Vertical (Zero U) Units
- Custom & Bespoke Design Service

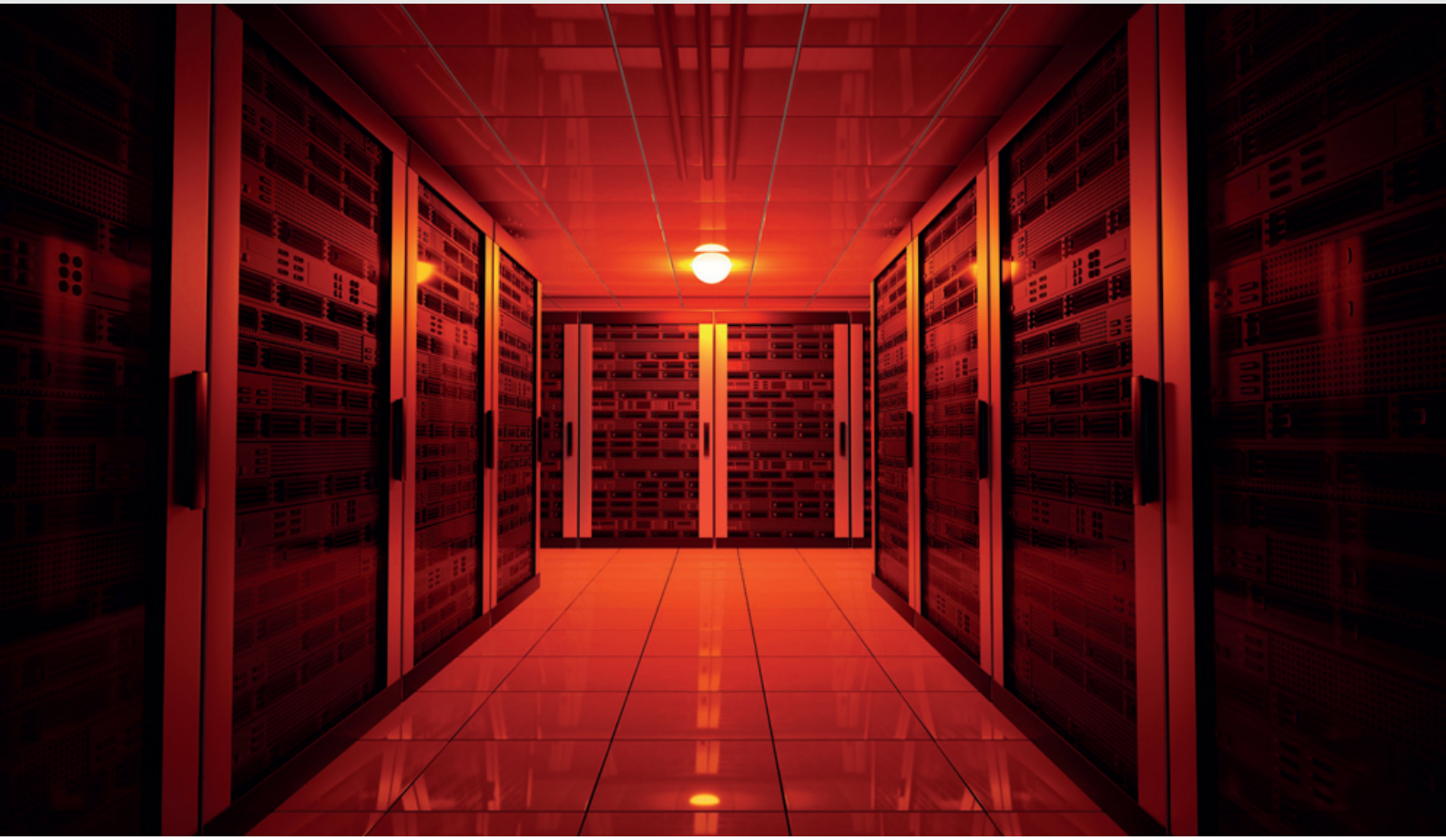
Designed and Manufactured in the UK

+44 (0)20 8905 7273 | sales@olson.co.uk | www.olson.co.uk

SINCE 1961

UP(SOS)

Alex Emms, operations director at Uninterruptible Power Supplies Ltd., highlights the untapped potential of your UPS system, during mains presence, as well as in blackouts, and outlines the importance of selecting on-line systems.



Most people in IT are aware that UPSs use batteries to seamlessly take over the critical load if the incoming mains supply fails. While they do indeed fulfil this role, UPSs also perform an equally critical protection function throughout normal operation with mains available.

This is because any mains supply is liable to many types of disturbance apart from total blackout – and these have the potential to damage or destroy any unprotected sensitive load.

Data centre loads are typically described as critical, both in the sense of their availability to the application relying on them, and of their own dependence on high-quality power at all times. On-line processing and e-commerce applications are good examples of this, because of their obvious requirement for uninterrupted availability.

Other equally critical applications include data processing computers, precision manufacturing equipment, medical devices in applications like life support and patient monitoring, telecommunications network equipment and point of sale (POS) terminals.

POSSIBLE CONSEQUENCES

A power supply transgression's immediate effect could be to cause an equipment failure arising from component damage. However, even if the supply problem only halts the load, rather than damaging it, the consequences can still be serious.

An unexpected hardware stop will cause a software crash leading to data loss or corruption. Business transactions will be interrupted and lost, exposing the enterprise to wider financial implications and loss of reputation.

In August 2018, for example, an internal power failure caused by maintenance activities at the Reserve Bank of Australia (RBA) interrupted its Sydney data centre, severely affecting payment systems and fixed phone lines. RBA's payment system includes clearing and settlement for cards, cash, cheques and electronic funds transfers. The outage was severe enough to affect all financial institutions across Australia.

In a manufacturing environment, the results could be equally (if not more) serious; control systems could be driven into inappropriate operation, for example. Both production

equipment and the product can be damaged, with time needed for cleaning up as well as repairs.

So, how serious is the threat to your particular installation, and what can you do to mitigate it? The answer depends on three factors; the type of power disturbances that could appear on your mains supply, the type of equipment to be protected and its susceptibility to these problems, and the steps you take to provide protection.

Let's look at these factors, see how they interact, and draw some conclusions on providing protection appropriate to your circumstances.

POWER PROBLEMS

Spikes

Figure.1 shows the problems most commonly experienced. Spikes are short duration rapid voltage transitions superimposed on the mains waveform. They can inflict both positive and negative voltage excursions, damage or destroy electrical and electronic components, and corrupt software. Software problems may be particularly difficult to track down and rectify, as they may not show until some time after the damage occurred.

Spikes are typically caused by thermostats or other equipment switching high electrical currents, or load switching by power companies. Locally-grounded lightning strikes are without doubt the most serious and dramatic cause of spikes, particularly when induced into telecommunications cables.

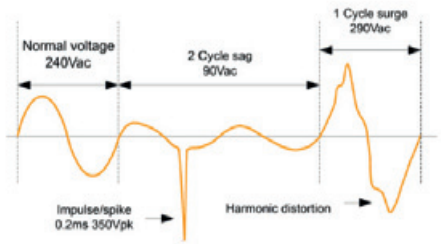


Figure.1: Power problem summary

Electrical noise

Electrical noise caused by disturbances between the supply lines and earth is called common mode noise. Conversely, normal mode noise, which arises from disturbances between line-to-line and line-to-neutral, can originate from sources such as lightning strikes, load switching, cable faults and nearby radio frequency equipment. Electrical noise can cause computers to hang and corrupt data.

Surges

Surges are voltage increases above normal mains levels that exceed one cycle. They typically appear after a large load is switched off or following load switching at substations. With long duration, voltage surges can degrade a computer's switched mode power supply components and lead to premature failure.

Sags

Sags are drops in the mains supply that can last for several cycles. They are generated in a similar way to negative spikes but have a much longer duration. Sags are very common occurrences that are usually the result of switching on large loads like air conditioning equipment, or starting rotating machinery.

Sags can cause a computer reboot if the mains voltage falls so low that the computer believes it has been switched off.

Harmonics

Harmonics are generally caused by non-linear loads, which draw large peak currents from the mains supply. Loads containing controlled rectifiers, switched mode power supplies, or rotating machines are particularly noted for generating this type of interference. These include computers, photocopiers, laser printers and variable-speed motors.

Harmonics cause a disproportionate rise in current, resulting in increased temperatures which can cause component failure and general equipment overheating.

"As well as filtering out events like spikes, the UPS also protects against excursions beyond a preset voltage range caused by surges or sags."

Brownouts

Brownouts are identical to sags but are of much longer duration and generally more serious. They arise when the mains supply cannot cope with the present load demand, so the generating company drops the overall network voltage. Brownouts can last for several hours in extreme circumstances.

Blackouts

Blackouts are complete power losses, where the mains supply fails totally. Caused by supply line faults, accidents, thunderstorms and a range of other conditions, they have an obvious and sometimes devastating effect.

GENERAL EQUIPMENT SUSCEPTIBILITY

Computers typically have specified upper and lower limits for steady state slow averaged rms line voltage variations of between ±5% to ±10%, depending on the manufacturer, but will tolerate short duration line voltage excursions outside those limits. The shorter the duration of the excursion, the greater the excursion that can be tolerated.

Some computers have sufficient energy stored in their internal power supply reservoir capacitors to sustain the dc supply to logic circuits during line voltage sags and power line interruptions of up to a 1/2 cycle (10ms), although not all units have this much ride-through capability. ▶

UPS PROTECTION

From the above, we can see that computer equipment resilience to mains disturbances is very limited; protection from the mains supply at all times is essential.

The most important measure is to select a UPS with on-line double conversion topology, as shown in Figure.2. This provides the highest level of power protection because it positions the rectifier and inverter as barriers between the supply and the load; these remove mains-borne noise and transient voltages.

> **To provide true UPS protection against all potential supply contingencies, selecting a system with dual on-line topology is essential.**

In fact, the load is not connected to the mains supply at all – instead, it is driven by a pure, well-regulated sinusoidal output from the inverter. Importantly, the inverter maintains its level of supply regulation, even when it is operating from the UPS battery during a power failure.

As well as filtering out events like spikes, the UPS also protects against excursions beyond a preset voltage range caused by surges or sags. It does so by switching to battery power, as it would for a complete blackout.

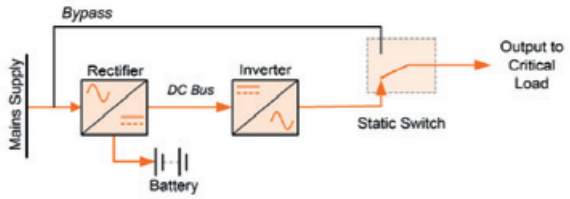


Figure.2: On-line double conversion UPS topology

Externally-connected components can complement the UPS's protection role. Radio frequency noise interference and spikes can be substantially reduced by fitting suitable filters and some form of isolation transformer in the supply line. Surge suppression components can also be fitted.

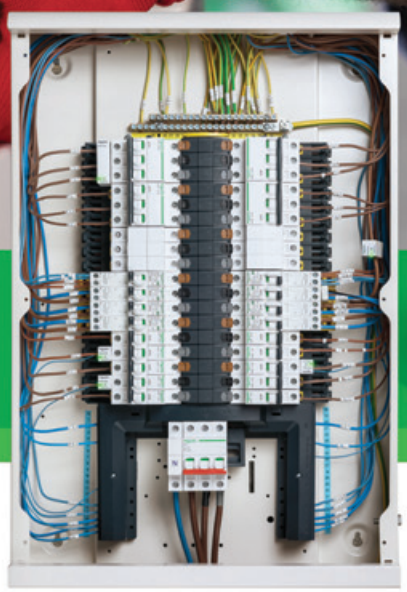
CONCLUSION

Above, we have seen how a critical load can be threatened as much by live utility mains supply problems as by blackouts. It also becomes clear that to provide true UPS protection against all potential supply contingencies, selecting a system with dual on-line topology is essential. Users then enjoy both protection from mains aberrations and battery autonomy during blackouts.

Acti9

Isobar P

Quick smart solutions



Acti9 Isobar P distribution boards now offer new and unparalleled reliability, protection and simplified installation whilst building on our existing market leading Isobar solutions.

Through over a quarter of a century of market leading innovations, Isobar distribution boards have come to represent a premium level of performance.

Our latest addition, Isobar P, further enhances this reputation by launching the first plug-on neutral & functional earth RCBO.

- **Time saving** due to the quick and simple plug on technology
- **Fast and efficient** due to absence of functional Neutral and Earth wires to unravel and straighten
- **No need to cut**, dress or terminate any functional wires

schneider-electric.co.uk/isobar-p

Life Is On | Schneider Electric

Primary protection

When you need to test a relay protection system, particularly during commissioning, you need to decide early on whether to use primary or secondary injection. Both approaches have their merits, yet according to Marius Averitai of Megger, there are many cases where primary injection has the edge.

To test a relay protection scheme you can either inject large currents into the primary circuits or much smaller currents directly into the relays.

On the face of it both approaches will give you similar results, so why would you lug around a large and heavy primary injection test set rather than its much smaller and lighter secondary injection counterpart?

THE GOOD

There are actually a lot of good reasons why you might choose to go for primary injection, but one of the most convincing is that it's a much more comprehensive test. To illustrate this, think of a very simple example: a circuit breaker with an overcurrent trip relay that operates via a current transformer (CT).

You could inject your test current directly into the relay (secondary injection) and this would indeed show you whether or not the relay was operating correctly. But it would tell you nothing about the CT and the connections between the CT and the relay.

If you inject your test current into the primary circuit (primary injection) however, your results will confirm not just that the relay is operating correctly, but also that the CT is serviceable and that the connections to it are present and correct.

Primary injection testing also has other valuable benefits. For example, it mimics the normal operating conditions of the equipment under test much more closely – the high test current will stress the equipment you're testing just as it would be stressed in service. This can make a big difference to the test results.

> **Primary injection provides a much more comprehensive test.**

Primary injection testing can also be less complicated to set up. The equipment under test has to be isolated and heavy current connections made to it, but it's usually only one set of connections. For equivalent secondary injection testing, isolation is still needed, but it will often be necessary to make several test connections to various parts of the equipment to carry out comprehensive testing.

PROGRESS WITH PORTABILITY

You probably know already that primary injection testing is sometimes shunned because of the size and weight of the equipment needed.

Primary injection tests typically involve currents of at least 100A, and in some cases up to 20,000A, whereas secondary injection currents are more likely to be a maximum of 50A – the typical nominal rating of secondary circuits is 1A or 5A.

This means primary injection test sets are never going to be as compact as their secondary injection counterparts, but what you may not know is that in recent years there has been a lot of progress in making them more portable.

One way this has been achieved is by using modular current sources, so that for lower test currents only one or two sources are needed, but for higher test currents additional current sources can be added.

Test sets that adopt this approach are often assembled on wheeled trolleys that can accommodate the control unit plus up to three or four current source modules. This arrangement makes it much easier for you to handle the test set.

If you look at the specifications for the latest primary injection test sets, you'll find that weight and size are not the only areas where progress has been made. Another useful development is the introduction of test sets where the control unit can be connected to the current generator by a comparatively long control cable.

This means that you can position the current generator very close to the equipment under test and in doing so minimise the length of the high current test leads, which makes testing easier and more practical.

WHAT SHOULD I LOOK FOR IN A TEST SET?

If you decide to invest in a primary injection test set, you'll want to be sure that it can cope with a wide range of burdens as if it ▶

doesn't, it may not be able to deliver the required test current even if this is within its nominal rating.

A good test set will make provision for this by allowing the output voltage of the current generators to be raised at the expense output current, so that the power the test set needs to deliver isn't increased unduly.

Another option you're likely to find very useful is an integral timer that you can set to inject the test current for an accurately controlled time. This will make it easy for you to inject actual fault currents to perform tripping time tests that include the circuit breaker, the relay and the CTs.

> **On average it takes engineers and technicians less than an hour to learn how to use a manual test set.**

Your test set should also have auxiliary voltage and current measuring inputs so that it's easy for you to test CTs, and the best test sets will provide you with a wide range of data, including impedance, resistance, virtual power, active power, reactive power, and power factor, together, of course, with CT ratio and polarity.

WHAT TYPE?

When you're selecting a primary injection test set, you'll quickly find that they there are two main types – sophisticated fully automatic units, like the Megger SPI225, and simpler manually-operated units like those in Megger's ODEN range.

The right choice for you depends on your application. For tests requiring the recording of multiple results and automated comparison with standard tripping curves, according to the settings of a protection relay, a smart computer controlled unit (SPI225) will make testing and reporting faster and easier. This is also the case when testing multiple MCCBs.

For straightforward applications, however, manual primary injection test sets have a lot to recommend them. First of all, very little training is needed to use them effectively and their operation is largely intuitive.

Megger has found that, on average, it takes engineers and technicians less than an hour to learn how to use a manual test set, and that the company's technical help desk rarely gets queries about these instruments. Other benefits are that you don't need to connect manual test sets to a computer to use them and, of course, they cost rather less than their automated counterparts.

CONCLUSION

As we've seen, primary injection testing has a lot going for it. It tests all of the components of the protection scheme at the same time, and it closely mimics real-life operating conditions, more so than secondary injection testing.

The latest compact test sets are much more portable and manageable than their predecessors, and the best of these test sets offer wide-ranging functionality. So, if you're thinking about investing in equipment for testing relay protection schemes, a modern primary injection test set could well be your best option! ER

"It takes 20 years to build a **reputation** and 5 minutes to ruin it. If you think about that, you'll do things differently."

Warren Buffett

Why risk yours?

Minimise your **risk** when you appoint a contractor for any electrical or electrotechnical work across all aspects of design, installation, maintenance, testing, inspecting and monitoring.*

- ✓ Highest level of industry standard or certification achieved
- ✓ Businesses regularly assessed
- ✓ Quality of work underwritten
- ✓ Completion of work guaranteed
- ✓ Business financial standing confirmed
- ✓ Access to market leading technical support
- ✓ Health & Safety standards confirmed
- ✓ Market leading Risk Assessment & Method Statement software
- ✓ CHAS/SSIP supported

Find an ECA Member today

www.eca.co.uk/find-an-eca-member

info@eca.co.uk **0207 313 4800**

@ECAlive

ECA
Excellence in Electrotechnical & Engineering Services

Luceco illuminates Manchester Royal Infirmary

Luceco and the Estates and Facilities Directorate at the Manchester Royal Infirmary have come together for the greater good, to reduce energy consumed by old lighting technology, replacing these fittings with cost effective LED luminaires from Luceco.

Manchester Royal Infirmary (MRI) can claim many medical breakthroughs and can also boast pioneering energy efficient lighting throughout their estate. Luceco, A C Electrical (North) Ltd and the Estates and Facilities Directorate at the MRI have collaborated in a bid to replace the energy sapping lighting of old, with greener LED alternatives from Luceco.

Richard Horton, national business development manager at Luceco said, "An example would be a typical hospital corridor. We removed 120W wall washers and replaced them with LED asymmetric LuxPanels from Luceco running at 44W, creating substantial savings."

"However, using LiteIP, we have reduced the energy consumption of the 44W luminaires to provide an additional 95% saving by utilising available daylight. The corridor was lit 24 hours a day, 7 days a week, it now operates at 5% for the majority of the burning hours when personnel are not present, illuminating to 100% when traffic is detected."

Richard continued, "Whilst we realise daylight light harvesting will reduce during the winter, the impact on energy consumption along with the PIR control has created massive energy savings."

LiteIP has assisted with these savings and has been included in several new projects at the MRI. LiteIP provides a flexible, intelligent wireless lighting system requiring no complicated electrical installation and no limit to the number of luminaires that can be controlled.

Each wireless luminaire is programmed to operate using drag and drop menus within LiteIP software. Changes to individual luminaire operation, to improve control, can be made without the need to alter any wiring.

Furthermore, emergency lighting tests can be run automatically, with monitoring email alerts and reports generated, avoiding the need for manual recording of results.

The lighting installation is also simple and can be completed as if no lighting controls are required; each luminaire needs only Live, Earth and Neutral, no expensive control cables are needed. This is followed by a commissioning engineer setting up the system on-site, applying settings and grouping luminaires as required. LiteIP is compatible with all driver types including DSI, DALI and 1-10 V. As well as presence and daylight detection,

other features include energy monitoring and reporting.

Formed in 1752, Manchester Royal Infirmary (MRI) began life with just 12 beds, in a small house in the city centre. The MRI is now a substantial teaching hospital for Manchester University's Medical School, and the Accident & Emergency Department sees around 145,000 patients each year. As well as achieving much medical success, pioneering energy efficiency and cost-effective operation is also considered a responsibility of the MRI and Luceco is delighted to be a part of its success.

“As well as achieving much medical success, pioneering energy efficiency and cost-effective operation is also considered a responsibility of the MRI.”

STANDING THE TEST OF TIME

The simple dial and levers on Sangamo's famous Round Pattern Time Switches (RPTS) make setting the switch up for daily fixed timings easy, with no complicated menu options to navigate through.

The switches are split into four categories, each containing both three-pin and four-pin connections:

S250 Range: The basic 'black dial' 24-hour time clock for simple on and off switching of up to 20A.

Q550 Standard Range: The standard 24-hour 'red dial' switch with added 100-hour battery reserve to keep the switch in time if any power outage occurs.

Q550 Solar Range: Specially designed for lighting applications. The Astro/Suntracker switches automatically adjust themselves to follow sunrise and sunset times without need for a photo sensitive cell.

E850 Digital Range: The newest addition combines the high capacity and reliability of the electro-mechanical models but provides full seven-day programming.

ESP • 01527 515150
www.espuk.com

LEAKAGE CLAMP MEASURES UP TO THE 18TH EDITION

Ever had a problem with nuisance RCD tripping? Now the 18th Edition Wiring Regulations and the latest leakage current clamp meter from Martindale Electric, the CM69, come to the rescue.

The 18th Edition now makes it clear; the accumulation of circuit protector currents/ earth leakage currents that are present during normal operating conditions shall not be more than 30% of the rated residual operating current of the RCD.

Rather than estimate the total incorrectly, measuring the leakage current flowing in an existing installation before modifying it, is probably the most effective approach to ensure the final installation is going to be fit for purpose.

The alternative could be expensive call outs in months to come. Selecting the right leakage clamp meter is critical to getting reliable and repeatable results, as many struggle below 10mA and can be prone to interference from other nearby conductors carrying higher currents.

Martindale Electric • 01923 441717
www.martindale-electric.co.uk

CIRCUIT BREAKER TESTING LIBRARY FOR CIBANO 500

OMICRON has sped up circuit breaker (CB) testing with its circuit breaker testing system CIBANO 500 and the operating software Primary Test Manager (PTM).

Since version 4.40, the PTM software now contains OMICRON's new circuit breaker testing library (CBTL) for use with CIBANO 500.

When using the CBTL, you will now be able to load all of the asset-specific default data into PTM with just the click of a button.

With CBTL, you can speed up your testing procedure considerably by using an optimised workflow:

1. Select your test location
2. Select your CB type and load pre-defined data from the CBTL, the associated test template will be loaded automatically
3. Execute all tests at once
4. Generate your reports automatically

Just look up the CB's serial number, perform any necessary modifications on the default data, and you're ready to test.

Omicron Electronics UK • 01785 848100
www.omicron.com

HALVE INSTALL TIME WITH SCOLMORE'S NEW FAST FIT CONNECTORS

In a speed test carried out by Scolmore, the installation times were compared for their new fast fit connectors, versus the equivalent screw terminal version – typically the fast-fit versions were completed in around half the time.

Scolmore's new 20A 3 and 4 Pole Fast Fit Flow Connectors feature push-in, low maintenance terminals to offer a time-saving benefit for the installer, with no screws required.

The new range will be compatible with all current Click Flow products – connectors, splitters, distribution boxes and ceiling rose. They are simple to install in just a few quick steps.

Allowing installers to safely connect/ disconnect luminaires or appliances in areas that require quick installation and regular maintenance, the new fast-fit connectors will be suitable for a range of applications.

Scolmore's Flow Connector range makes the wiring of a lighting circuit easy, using a combination of connectors, hubs and management boxes.

Scolmore • 01827 63454
www.scolmore.com

ELECTRICIAN'S PUBLIC LIABILITY INSURANCE

Public liability insurance is an extremely important cover for electricians and many other trades due to the potential hazards you may come across during your work.

It helps to protect you against any claims made against you by members of the public or third parties who may have been injured, or whose property is damaged as a result of your work.

Having this cover can also open the door to a wider range of clients as for some contracts, public liability insurance is a requirement to work on the site.

Trade Direct Insurance offers cover of £1m, £2m or £5m. Tool cover can also be included between £1,000 and £15,000.

With our plus cover, we provide a limit of £100,000 professional indemnity insurance to cover claims made against your business for losses a third party has suffered due to work or advice you have provided.

If you would like to find out more about our public liability insurance, please don't hesitate to get in touch.

trade direct insurance
The Trusted Trade Specialists

Trade Direct Insurance • 0800 280 380
www.tradedirectinsurance.co.uk

CHOOSING WIRING ACCESSORIES? TRUST YOUR INSTINCT

The Instinct range from Crabtree allows specifiers and installers to remain competitive while maintaining the quality, reliability, style and functionality required in today's highly competitive commercial buildings market.

True to Crabtree's 'Easier Safer Faster' mantra, the range has been designed with over 300 new wiring accessories, packed with innovations including full contact cable clamps, integrated led indicators, and twin action safety shutters.

When it comes to installation, upward-facing inline terminals make the entire range simple and reliable to install, saving time for the contractor as well as delivering peace of mind.

Instinct is the first range of wiring accessories to use full contact cable clamps. These "no miss" terminals offer a more secure, more efficient, method of connection.

The range also features a twin operation multipin safety shutter. Crabtree has developed a shutter with a two-piece mechanism that requires multiple pins to fully operate the mechanisms.

Crabtree • 01543 455010
www.crabtreecommercial.co.uk

FLUKE POWER AND ENERGY LOGGER INCLUDES TRAINING PACKAGE AND FREE ACCESSORIES

Until 30th June 2019 Fluke is offering its 1738 Three-Phase Power Logger with Fluke Connect as a Gold package, offered at lower recommended prices than the standard product, including free accessories, and a free, unique offline training program.

The Fluke 1738 Three-Phase Power Logger Gold Edition (FLUKE-1738/EU-GOLD-E) enables the capture and logging of voltage, current, power, harmonics, and associated power quality values to deliver comprehensive data for load studies, energy assessments, harmonic measurements, and voltage events. It also enables the troubleshooting of more advanced power quality issues.

The Fluke Connect capability allows users to access and share data remotely, or access the logger through the local Wi-Fi infrastructure, so as to maintain safer working distances and make critical decisions in real-time, reducing the need for protective equipment, site visits and check-ins.

Fluke • 0207 942 0700
www.fluke.co.uk

ABB LAUNCHES NEW GENERATION OF POWER QUALITY AND ENERGY STORAGE SOLUTIONS

ABB's new multi-functional power quality and energy storage solution has been designed to mitigate a range of power quality problems for electrical networks.

To be able to manage the complex requirements of an ever-evolving grid, more agile "active" technologies are needed. Products that employ active technology are more compact in size, making them ideal for applications where space is scarce or costly.

ABB's new portfolio comprises five solutions: PQflexC – variable reactive power controller; PQdynaC – ultra-fast reactive power and unbalance controller; PQactiF – active harmonic filter; and PQStorI – battery storage inverter with power quality functions. Finally, PQoptiM controls and monitors power quality parameters.

The product family is further enabled by ABB Ability to allow the devices to be operated and controlled via cloud-connected user platforms to enable real-time access of data.

ABB • 0151 357 8400
www.abb.co.uk

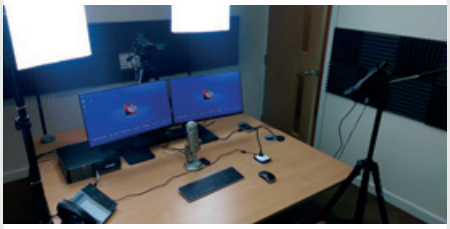
SEAWARD OFFERS FREE PAT WEBINARS

Seaward is offering electricians and those working in the industry the chance to gain in-depth knowledge about the latest advances in PAT testing thanks to a series of free webinars.

Seaward hopes the new webinars will give people the chance to widen their knowledge of PAT testing and keep up with industry standards – as well as providing hints and tips for those who are new to the electrical safety tests.

Portable appliance tests (PAT) are quick and simple checks performed on electrical appliances. Employers are legally required to ensure any electrical equipment they provide to staff is maintained in a safe condition – and PAT tests are the simplest way to do this.

The on-demand sessions cover topics such as legal requirements, industry guidance and common practice, how to perform PAT risk assessments, how to run an efficient PAT system and how to improve safety standards – with new ones added regularly.



Seaward • 0191 587 8741
www.seaward.co.uk

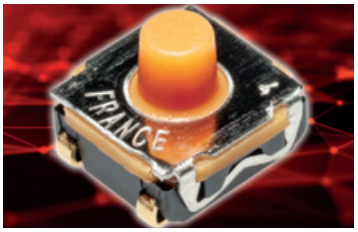
C&K INTRODUCES COMPACT DUAL-CIRCUIT TACT SWITCH

C&K has launched a dual-circuit technology tact switch as a significant addition to its extensive KSC range of tactile switches.

The new KSC-DCT tact switches offer SPDT NC-NO dual-circuit functionality that provides two outputs from a single input. Housed in a tiny 6.2mm x 6.2mm x 2.9mm PCB-mount package, the silicone 70SH actuator included in the package extends the height to 5.2mm above the PCB surface for easy operation and easier integration through pre/post travel.

Rated for 300,000 operations, the new switches require an operating force of 4.75 N and provide a nominal travel distance of 0.85mm. Incorporating C&K Switches' industry-recognised haptics, the KSC-DCT switches provide excellent levels of feedback when pressed.

The new switches are IP67 sealed and operate over the temperature range -40°C to +85°C, making them suitable for use in harsh environments.



C&K • +33 160 245 151
www.ckswitches.com

ERA RAISES OVER £11,000 FOR MIDLANDS AIR AMBULANCE

2018 saw ERA, the Wolverhampton-based security expert, raise £11,262.86 for the Midlands Air Ambulance Charity. At the outset ERA had set a £10,000 target, and staff at the company are over the moon to have exceeded this figure.

Each life-saving mission undertaken by the Midlands Air Ambulance Charity costs it approximately £2,500. The money raised by ERA therefore is enough to cover four such missions.

Employees used their ingenuity to come up with a broad variety of fund-raising activities, including a book sale, a Valentines' raffle, a Grand National competition, a World Cup raffle and sweepstake, a Christmas raffle, a sponsored Snowden walk and the use of collection tins. In addition, ERA's suppliers kindly made donations.

Jon Cottrell of Midlands Air Ambulance Charity said, "Many people are unaware that we are reliant on donations to keep us operational as we receive no government funding. We're extremely grateful to ERA's staff for this contribution, which will help to keep our aircraft airborne."

ERA • 01922 490 000
www.eraeverywhere.com

FIVE TRENDS FOR CLOUD COMPUTING AND DATA CENTRES

Rittal has issued predictions for the data centre sector as the industry moves towards greater AI-based monitoring capabilities and the processing of data in real time with edge computing.

Hyperscale data centres will drive the cloud market and streamlined cooling technologies will boost energy efficiency in data centres.

Meanwhile Nordic countries are continuing to offer attractive locations for cloud-based data centre facilities for those looking to cut costs.

Rittal will be showcasing its expertise in edge computing products and services at Data Centre World (Excel, London, 12-13 March 2019) on Stand D610, where it will be offering an array of solutions for edge infrastructures, ranging from rack solutions to turnkey IT containers with cloud connections.

Rittal • 01709 704000
www.rittal.co.uk

DATA CENTRES CAN EARN REVENUE
AS NEW ENERGY PROVIDERS

Why haven't you started?

Vertiv technologies enable data centres and power intensive facilities to support the grid, bolster the security of supply and reduce energy costs, while financially benefitting from the fast response and capacity market.

See us at
Data Centre World
Stand D720
12-13 March 2019,
Excel London

Power Systems = A New Revenue Source:
A reference 20 MW data centre in Ireland is earning over €1.9 million per year through their UPS systems and diesel generators

Start unlocking new revenue streams through your national grid: **VertivCo.com/EnergyStorage**

VERTIV.