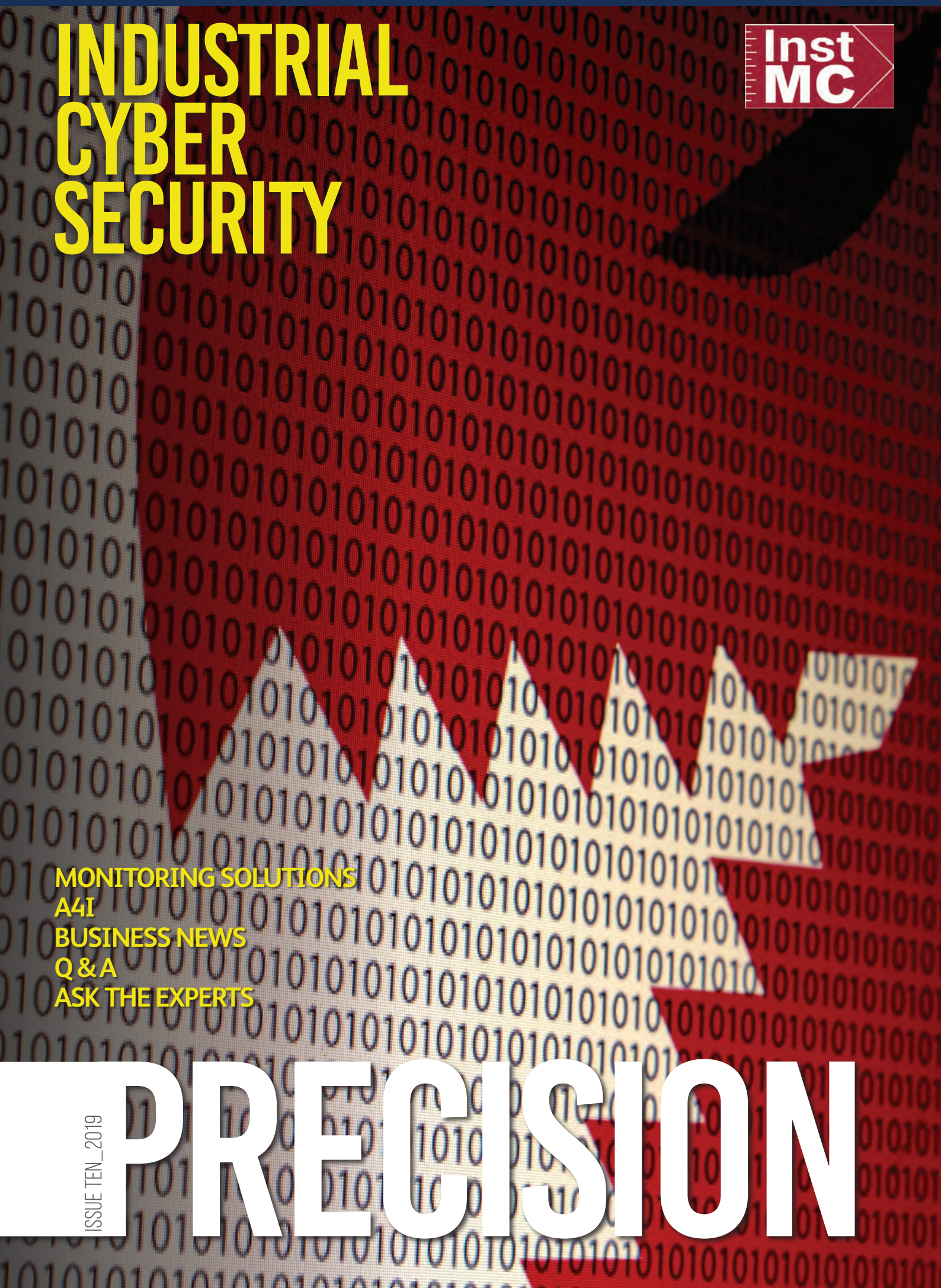
THE MAGAZINE OF THE INSTITUTE OF MEASUREMENT AND CONTROL INSTMC.ORG

INDUSTRIAL CYBER SECURITY



MONITORING SOLUTIONS
A4I
BUSINESS NEWS
Q & A
ASK THE EXPERTS

PRECISION

ISSUE TEN_2019

THE INSTITUTE
OF
MEASUREMENT AND CONTROL

75th ANNIVERSARY

75TH ANNIVERSARY DINNER

In 2019 we celebrate 75 years since the founding of the Society of Instrument Technology, the forerunner of the Institute of Measurement and Control.

The Institute would like to invite you to join us to celebrate our anniversary with a formal dinner.

SAVE THE DATE

2 MAY 2019 | 7.00PM

London Royal Lancaster Hotel
LANCASTER TERRACE LONDON W2 2TY

Book your place at www.instmc.org/events

DIVIDE ET IMPERA

InstMC

INTRODUCING THE SIG MANAGEMENT BOARD

The Institute has launched/ reconstituted a number of Special Interest Groups (SIG) that operate under the auspices of a new SIG Management Board (SIGMaB).

This management board is formed from the chairs of the SIG executive/ steering committees. The intention is to bring a consistent approach to the management of the SIGs, to regulate their constitutions, to share good practice and to exploit opportunities for collaboration where appropriate.

The board has now issued model terms of reference for the SIGs and a model constitution. The executive committees are charged with adopting these models, tailoring and branding them as appropriate and issuing them for endorsement by the board before releasing them into the wild.

One of the key aspects of the model constitution is a 'sunset clause' that promotes rotation of representation in key roles; members may hold office for up to 2 terms of 3 years but are then required to stand down unless there is no other willing candidate. This is consistent with the requirements for other key positions throughout the Institute and promotes the introduction of 'fresh blood' to help keep our groups invigorated and relevant.

It is, of course, the member volunteers that are the 'engine' of the Institute's SIGs; their engagement is critical. It is typically the involvement of one or more 'champions' with support from actively engaged members that drives the ambitions and performance of any such team.

Membership of the SIGs is freely available to all members. Interested members that would care to take a more active role may wish to consider joining a SIG executive/ steering committee as and when any opportunity may arise. Committee members are typically recruited from members that have demonstrated an active interest and engagement with SIG concerns. Our aim is to have a balanced representation to reflect academic, industrial and government interests.

Harvey Dearden
CEng, Chair of SIG Management Board

CONTENTS

ARTICLES

Q&A

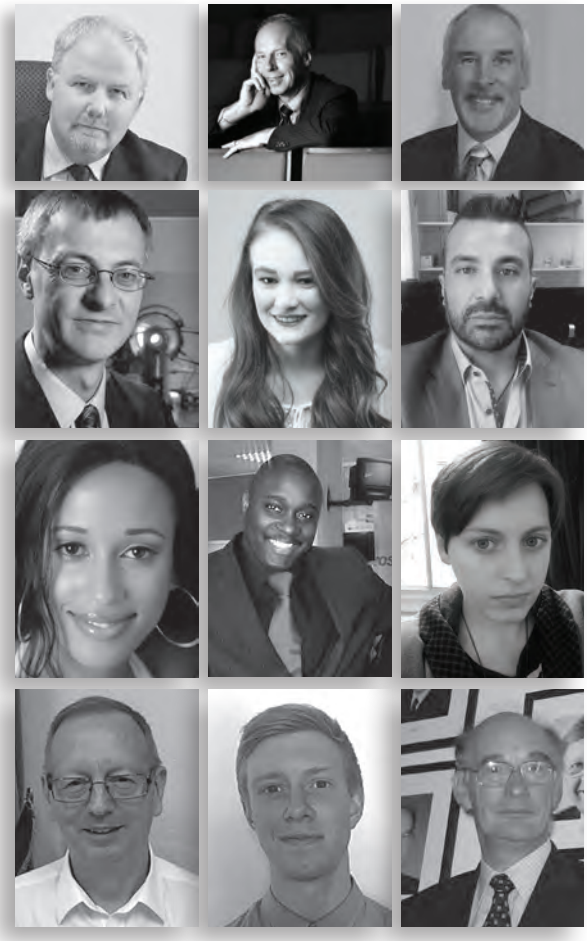
QUICK-FIRE QUESTIONS FOR BEN SIMPSON

16-17

This month's interviewee is Senior Lecturer in Mechanical Engineering, Ben Simpson at Nottingham Trent University

MEET THE TEAM

22



REGULAR

ASK THE EXPERTS

Our experts wade through our 'post bag' to find interesting questions to answer. The query this issue is:

I see instruments occasionally described as "smart" or "dumb". What does this mean and why does it seem important?

20-21

PRECISION

The magazine of the Institute of Measurement and Control

Published by: Institute of Measurement and Control
297 Euston Road,
London NW1 3AD
T: 0+ 44 (0) 20 7387 4949
www.instmc.org
www.facebook.com/instmc
www.linkedin.com/groups/117672

Chief Executive
Patrick Finlay PhD CEng
Email: ceo@instmc.org

Design, print & mail fulfilment by HMCA Services Ltd
Tel: 01423 866985
Email: enquieries@hmca.co.uk

Advertising sales in partnership with HMCA Services Limited
Carol Rees - Allott & Associates Ltd
Telephone: 01423 867264
Email: carol@allottandassociates.co.uk

INDUSTRIAL CYBER PHYSICAL SECURITY ENHANCEMENT PART I

Cevn Vibert, Industrial Cyber Physical Security Consultant and Co-Chair of the InstMC Cyber SIG issues a call to action in the first of a two-part article which will be concluded in the next issue.

Introduction

Our modern society is built on automation, control systems and their management. The "Things", mentioned often in the Internet of Things (IOT) and the Industrial Internet of Things (IIOT), are becoming smarter and more ubiquitous. If you think about all the automation controlled "Things" that have contributed to your day and try to list them, you may be surprised and perhaps a little worried to know that they are also being invisibly attacked. Food manufacturing, transport, clothing, water treatment, waste processing and management, pharmaceutical manufacturing and testing, logistics, medical device manufacturing, power generation, transmission and distribution, defence, healthcare, cashpoints, and beverage dispensers are just some of the examples of this melange of "Things" in our personal lives.

Critical national infrastructures are under immense pressure from governments, regulators and themselves to enhance their defences, improve cyber monitoring and to re-work the gargantuan quantities of legacy systems. This is not an easy task with industrial IT, due to a range of largely legacy problems. The aging and legacy industrial systems were not designed to be monitored and interrupted and scanned by active defence solutions.

These security problems are procedural, legislative and technical, so all end-users are now having to review remediation against enormous business and operational risks. The rise in attacks on these 'Things' has started to concern people.

History

Historically the first Cyber Attack was in 1988: "The Morris worm - one of the first recognised worms to affect the world's nascent cyber infrastructure - spread around computers largely in the US. The worm used weaknesses in the UNIX system Noun 1 and replicated itself regularly. It slowed down computers to the point of being unusable. The worm was the work of Robert Tapan Morris, who said he was just trying to gauge how big the Internet was. He subsequently became the first person to be convicted under the US' computer fraud and abuse act. He now works as a professor at MIT." [1]

The first Cyber Hacker publicly convicted: "1999: 46 months prison plus 3 years' probation 1988: One year prison. Kevin David Mitnick (born August 6, 1963) is an American computer security consultant, author and hacker, best known for his high-profile 1995 arrest and later five years in prison for various computer and communications-related crimes. He now runs the security firm Mitnick Security Consulting, LLC" [2]

Cyber Language

We now know of many new cyber perpetrators and threats, and there is a veritable 'cyber zoo' of attackers: Yetis, Bears, Dragons, Dragonfly, Worms, Penguins, etc. A whole new cyber genus perhaps yet to come? There are also many new words and references in our evolving cyber weapons vocabulary: cyber zombies, watering holes, Slammer, Nachi, Mahdi, Shamoon, Industroyer, Petya, Red October, Conficker, Duqu, Flame, Havex, APTs, blasters, dumpsters, drive-bys, honeypots, Pastebin, Phishing, BotNets, Trojans, Heartbleed, Modbus, CANbus and

> Critical national infrastructures are under immense pressure from governments, regulators and themselves to enhance their defences, improve cyber monitoring and to re-work the gargantuan quantities of legacy systems.

so on, all being aired or created on social media and on news sources around the world.

Targets

An abbreviated history by SANS has researched and listed quite a catalogue of Industrial attacks over the years starting with: 1982 Uncorroborated report of a Trojan program inserted into SCADA system software that caused a massive natural gas explosion along the Trans-Siberian pipeline in 1982. 'Farewell Dossier [3]. Also listed are attacks on sewage works, gas operational systems, rail signalling and despatch, bulk electric controls, auto manufacturing, water plants, air traffic control breaches, PowerGen, tram switching, utilities extortions, offshore oil platform leak detection, smart meters and petrochem OPC SCADA servers. There are estimated to be many more attacks not publicly reported or known.

The fabled first big Industrial Cyber Attack was StuxNet 2010 (2005 variations), since then there have been a wide range of new attack vectors with ransomware, exfiltration, darknet resellers, custom hack sites, etc. These have now led to some stringent data law sanction proliferations due to the slow speed of response in industry compared to the high rate of advancement by the attackers. Huge rise in attacks and a quantity and quality adjustment over the years is shown on many graphs such as the data provided by the Hackmageddon website. [4]

The hacks on industrial systems, like commercial systems, are becoming simpler, using social engineering compromises, and more widespread. Some attacks, such as zombie denial-of-Service (DDOS) attacks are largely automated. A recent, much publicised attack on the Ukrainian Grid involved multiple coordinated attack vectors. This resulted in widespread impact and greatly hampered any recovery or mitigation efforts by the defenders.

"We are all going to die!" was the repeated phrase at a recent Cyber Security Conference Key note address by Eugene Kaspersky of Kaspersky Labs. He said it tongue-in-cheek as most of the presentations at Cyber Conferences are focussed on doom and gloom so he offered positives.

Cyber Attacks on Industrial Control Systems are increasing both in complexity and in frequency. All the statistics from the industry back this up. The attackers don't need high complexity or advanced skill sets to attack most Industrial Control Systems. "It's almost child's play", he said.

Attackers used to be a wide range of groups from a script-kiddie to nation-states but now the primary volume of successful attacks are from organised crime. Crime gangs have widened their business models to now include Hacking-as-a-service (HAAS) where you can define your attack and target and strategy online with an Attacking Service and pay for the attack, delivery, telephone support and service level agreement SLA, all online, using PayPal or similar simple payments.

Many conferences now are haranguing the audience as being 'incompetent', again tongue-in-cheek, but aiming at both the vendors and integrators who do not implement Security-by-Design in their products and systems together with the security industry which has not yet eradicated cyber-attacks by Leap-Frogging the bad guys with new innovative defences and solutions.

The industry must now stop talking about Stuxnet and start talking about Innovation and new ways of thinking. Keynote speakers are talking about the soft skills of the cyber war. Cyber-attacks are made by humans, often exploiting human weaknesses as key building blocks of their attacks. The cyber defence industry must recognise this more and build security improvement programs which include humans as the core to the solution.

"The hacks on industrial systems, like commercial systems, are becoming simpler, using social engineering compromises, and more widespread."

Industrial Control Systems owners cling to the myths because the current ICS OT systems work well and they do not see lots of local news about their neighbours and competitors suffering the negative consequences of cyber-attacks. The cost of a Security Enhancement programme is often seen as prohibitive by the Board and Senior Management. What is not so well recognised are the business and operational improvements a Security Programme will bring about, including reduced insurance premiums, reduction in the cash safety float, improved operations and increase resilience. These business improvements are often enhanced by better staff moral and a much clearer understanding of Operational Technology and the current risks landscape. In fact, over 60% of Information breaches take months to be discovered, not days or hours or minutes. Around 70% of respondents to a recent survey admitted being victims to a cyber-attack. Organisations are not reporting the attacks, the effects or the remediations carried out, due to strict corporate embargoes.

The Way Forward

The steps to climb the stairway to security can be very high, certainly for organisations with extensive legacy systems, but the steps need to be climbed, and sooner rather than later.

The best approach is often to build small steps, parallel steps and think differently.

Remember, the bad guys are always improving, so it is essential for organisations also to keep improving, but more than that, looking for that giant leap ahead in defences. There is talk of new Secure Operating Systems, new Secure Trusted Computer Systems, and of the increased lock-down and monitoring of the Internet. All these advances are being made but are they appearing on the market quickly enough to make that giant leap forward in the cyber arms race?

We are now into what is being called the Fourth Industrial Revolution with Industry 4.0 (2011 – 2014+). This revolution brings enormous commercial benefits but at a cost. Often the cost of implementing greater automation omits the cost of securing that automation. Companies have relied on the IT Department doing something clever, within their annual budget, to secure all new development in corporate systems. This is obviously not the case to those who think about the holistic nature of automation enhancements within the corporate boundaries of data, interactions and information assurance as much more must be done to include people, informational and operational security in the life-cost of new systems and not just a thin spread of IT Security.

Physical Security

Physical Security is just as necessary as Cyber Security since a network or datacentre can be compromised much more easily by someone connecting devices, logging in directly to a terminal or stealing hardware for later analysis. Physical security can also help to protect staff who may be compromised through force or coercion by intruders.
The logs and records of physical security systems can be a valuable component of a forensic analysis, or the status of cameras and intrusion detection systems can be valuable situational awareness for a real-time event.

Physical security may include a wide range of technology such as CCTV, intruder detection, fence alarms, break-beam or IR detectors, radar, ground seismic sensors, thermal imaging, vehicle identification systems, card readers, biometrics, audio sensors, chemical and radiological sniffers, x-ray and radiometric sensors and air force or pressure sensors. There are many different technologies deployed to detect changes or unknown people or vehicles around and inside perimeters. The sensors are usually networked and collated into an intruder detection system, access control system or a PSIM (Physical Security Information Management) system.

The Security guardroom or control centre of a facility may have several computer screens dedicated to security management with an Access Control screen, PSIM screen, numerous CCTV screens, a card reader management screen, public address, radio communications management, fire management and Building Management System display. The diversity of each system, from different vendors with different Operator Interface standards, methods and operations makes the life of the security staff more difficult than it should be. Operator standards have been known, defined and standardised nationally and internationally for a variety of industries. The Security vendors are most often not cognisant or have chosen to ignore such standards. Each system requires both education and experience to use effectively hence creating many opportunities for ineffective operation. This is an area for significant improvement where PSIM systems are starting to take on more and more management functions for all the other systems in the Security Room.

References

1. http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm
   Accessed Sept 2018
2. https://en.wikipedia.org/wiki/Kevin_Mitnick
   Accessed Sept 2018
3. https://ics.sans.org/media/An-Abbreviated-History-of-Automation-and-ICS-Cybersecurity.pdf
   Accessed Sept 2018
4. http://www.reuters.com/article/us-tech-cyber-microsoft-idUSKBN15A1GA
   Accessed Sept 2018

In Part 2 of his article, Cevn Vibert, will look at some of the ways in which organisations can improve their cyber security.

“The diversity of each system, from different vendors with different Operator Interface standards, methods and operations makes the life of the security staff more difficult than it should be.”

IChemE ADVANCING CHEMICAL ENGINEERING WORLDWIDE

Advances in Process Automation and Control 2019

18–20 November 2019
Manchester, UK

Spend three days with leading figures from the field of process automation and control as you review best practice and emerging technologies, learn from others' experience and network with experts and peers.

This innovative conference will look at themes as diverse as:

- cyber security and new architectures
- education, training and research
- sustainability
- operator 4.0 in emerging technologies
- business integration and the complete digital twin

Call for papers now open - showcase your latest research, innovations and projects.

Visit www.icheme.org/advances2019 for more information

MB0113_19

KEEP YOUR COOL BY USING SMART BRITISH MONITORING SOLUTIONS

In a regulated facility like a hospital, or food manufacturing or processing plant or a pharmaceutical factory, there is no hiding place from a visit by an inspector. They will be looking for a chink in the organisation's temperature control protocols that could put the public's health at risk.

Unlike the hotel inspector episode of the classic sitcom Fawlty Towers, where chaos reigned due to mistaken identity, it makes sense to be prepared for officials from regulatory organisations seeking to ensure that the strictly enforced standards for storage conditions are being adhered to.

Medicines and Healthcare Products Regulatory Authority (MHRA), Hazard Analysis and Critical Control Points (HACCP), Care Quality Commission (CQC), Good Manufacturing Practices (GMP), British Retail Consortium (BRC) and Food Standards Agency (FSA) will turn up, often unannounced, checking that everything is in order.

Getting in a flap like Basil Fawlty won't help, but keeping tabs on environmental conditions will! Whether storing supplies of blood, vaccines or fresh produce, ensuring that temperatures are being maintained at the correct level is vital. The earlier a problem

is identified the quicker it can be rectified and issues avoided.

Centralised environmental monitoring is invaluable, not only in the pharma and food industries but in non-manufacturing sectors like heritage, to avoid a potential disaster from equipment failure, but also to save time and reduce the chance of human error. Fridges, freezers, incubators, air flow chambers, water baths and cryogenic chambers are just some of the items of equipment that can be monitored via a single system with sensors calibrated to each individual application, and brought together at one or more instantly accessible points such as a PC or tablet. Any compromised conditions trigger immediate alarms and the comprehensive data collection and analysis provides evidence for the regulatory authorities whilst significantly reducing paperwork.

Slack monitoring procedures in pharmaceutical or healthcare facilities could potentially lead to a crisis if a rise in temperature or equipment failure causes damage to products, resulting in major drugs trials being delayed or hospitals cancelling and postponing operations.

In the food industry a supplier or retailer risks ruin if a major product recall or significant waste is caused by environmental failings.

Quick intervention thanks to accurate, real-time monitoring of temperatures can save the day and maintain the supply of vital products. That is where wireless environmental monitoring comes into its own. Innovative early warning systems that can also instantly produce historical data in the event of an industry audit or inspection have been developed to provide maximum flexibility and enhanced control of events from anywhere in the world via cloud or server-based configuration.

Now, what about the bit in the middle of a supply chain? Perhaps the biggest challenge in maintaining temperature integrity is when transporting products from one distribution centre to another location. Data loggers are typically used for delivery applications, which then require manual processing. Unfortunately, this data only shows a retrospective view and any damage is already done. In fact, it's quite possible that by the time the information is properly processed the product may have already been sold and consumed – or at least be on the way to another location.

The situation can be easily remedied, as there are many environmental monitoring solutions available which would provide better protection for temperature-sensitive products. However, the most effective and reliable are wireless transmitter-based solutions, rather than those using WiFi technology which are less reliable.

British manufacturers are world leaders in wireless environmental monitoring solutions, developing new, state of the art software platforms that provide real-time data and audit reporting capabilities for multiple sites, zones, and sensor groups. These are all accessible by unlimited users with controlled permissions, at any time and anywhere across the world. The best solutions are allied with long range wireless penetration through buildings, high quality sensors and even, in one case, a ground-breaking smart app for critical environment alerts at the touch of a button from anywhere in the world for users without access to networked software. All this, but still at an affordable price.

This will not change despite all the uncertainty surrounding Brexit. I am confident that British-engineered environmental monitoring solutions will still be in demand worldwide for helping organisations meet the needs of strict pharma, healthcare and food industry regulations, and providing valuable peace of mind, whatever happens when the UK exits the EU.

Common sense, coupled with innovative temperature monitoring solutions, mean not just keeping up with trends across multiple markets but in fact anticipating ever-increasing legislation and regulations. The technology available is extremely flexible and highly responsive, ensuring that the management of complex systems incorporating differing environments has never been so easy.

In the past the NHS, for example, would have employed someone who would routinely take temperature readings from fridges by opening the door. The temperature might be creeping up but still within the regulations so nothing was done. Today, a hospital can take immediate action if the real-time data recording an upward trend is potentially a cause for concern.

Having well-documented records and data on how storage equipment is performing over a continuous period of time is a significant advantage that can save time, costs and of course reputation. Regulation is a driver for improvement so monitoring cold storage solutions every minute, 24/7, 365 days a year provides an extra layer of protection for medical supplies and food products alike – and helps take the heat out of even the most unexpected inspection.

Marcus Bradbury
UK Commercial Manager
Hanwell Solutions

Common sense, coupled with innovative temperature monitoring solutions, mean not just keeping up with trends across multiple markets but in fact anticipating ever-increasing legislation and regulations.

ANALYSIS FOR INNOVATORS (A4I) 2019

Do you want to solve an issue that is impacting your productivity and sales? It might be a problem with product reliability, manufacturability/ cost of product or product lifetime.

This month NPL in partnership with Innovate UK, LGC, NEL and STFC are delivering the fourth round of this highly successful A4I programme. A4I gives UK businesses access to cutting-edge R&D, expertise and facilities to help solve analysis or measurement problems that can't be cracked using standard technologies and techniques. This popular funding programme is aimed at businesses of any size and, in the first instance, to apply you only need to explain your problem.

The programme is expected to appeal to manufacturing companies, especially those involved in complex supply chains, although companies of any size with any type of measurement or analysis problem, across sectors, are able to apply. So far, the scheme has helped over 100 companies, unblocking the road to commercialisation or improving productivity – from moisture in straw bales for construction, to testing the finish on cashmere fabrics, to analysis of bicycle lubricants and understanding quantum technology.

During 2018, Adaptix, a medical imaging company, who are developing an innovative new technology which could revolutionise medical imaging took advantage of the programme. Principal Scientist, Aquila Mavalankar, said: "The great things about NPL is they have lots of tools under one roof, so they form a team to come at a problem in multiple different ways. You end up really understanding the issue. We expect to have prototypes in manufacture very soon , and from there we hope to move first into dentistry and then into the clinical applications, capturing a share of the $12bn X-ray imaging market. The work with NPL will dramatically reduce the time it takes us to get to that point."

And, Bramble Energy has created the world's first fuel cell which can be manufactured in established production facilities, eliminating the need for expensive, purpose-built factories. Erik Engebretsen, Head of Engineering at Bramble Energy, said "The A4I project has been invaluable in unlocking world-leading facilities and expertise which would have otherwise been inaccessible to us. NPL's combination of materials testing and corrosion expertise make them well equipped to do this type of analysis. The knowledge gained helped us overcome a problem in our manufacturing process, improving the durability of our fuel cell and making it a much more competitive technology."

You can read more about the scheme at Analysis for Innovators and as Round Four of the scheme is about to kick off – to receive further information about this programme as it becomes available, please visit www.npl.co.uk/analysis-for-innovators to register your interest.

Q&A

Ben Simpson

This month's interviewee: Ben Simpson, Senior Lecturer in Mechanical Engineering - Nottingham Trent University

What was the root of your interest in science?

I grew up on a diet of science fiction novels, which described a future where science had enabled us to spread through the universe, exploring strange planets and meeting exotic aliens. These stories inspired me to want to be part of this exciting future and I wanted to help bring this future to a reality by building self-contained biospheres and rocket ships. My enthusiasm was further fuelled by high profile news stories of the voyager space probes reaching out to the edge of our solar system and the launch of a reusable Space Shuttle.

This boyhood fascination pushed me towards maths and physics at school and into an aerospace degree at university. In fact, my first job with Dowty Aerospace was in their space systems division. Although, at university and in my early career I realised the world is actually very complex. This complexity fascinated me but inevitably meant that building a spaceship to take us to the stars would require a bit more time and thought.

What is your vision of Engineering in Britain in 2020?

Arguably, the world has never faced so many significant challenges. The ever-increasing world population continues to put strain on our food, energy and water resources. The planet is suffering. This is evidenced by climate change, plastics strangling our waterways, habitat loss and loss of biodiversity. Our digital age makes us more informed and yet strangely less informed. It also shrinks the world and yet isolates us at the same time. However, the good news is that I meet young engineers almost every day who not only express concern over these issues but also have a quiet determination to tackle them.

Britain has a rich heritage of engineering innovation. This innovation was built on our ability to revolutionise manufacturing, our primary resources and a relatively large home market, boosted initially by the commonwealth community and then our association with the larger European community. Yet , in 2019 we find our circumstances have changed. Our primary resources have dwindled, our home market is now smaller than many of our competitors and globalisation has led to most of our goods being manufactured overseas. This makes me think that maybe it is time for us to introduce new paradigms to the discussion. Britain has a large number of thriving small to medium enterprises (SME). What our SME's lack in scale, they make up for with creativity, flexibility and potential. In the digital age, these are essential ingredients. Indeed large companies often find it hard to adjust their focus to make use of new technology, materials and sudden market changes. In 2020 and beyond I see Britain as being the place where great ideas become realities. Britain has the opportunity to create, test and build its way to a new future. I believe manufacturing in Britain will thrive where automation and very highly skilled workforces are required. To support the upswell of engineering innovation, new business models will have to be developed and Britain needs to be connected, the partner everyone wants to deal with, operating on a world stage not in isolation.

What should the UK government do to address the shortage of UK engineers?

Schools, universities and the Government have recently tried to boost the number of students choosing STEM courses through many creative initiatives. The message has been good but still the numbers of students are too low. I believe the image of an engineer and, more generally, that of engineering is at the centre of the problem. Engineering needs to be seen as a professional career with the right level of respect and remuneration. Furthermore, engineering needs to be seen as exciting, but most importantly, it needs to be seen to be at the core of solving both local and world problems. Engineering is so much more than just function and form. Engineers have to produce ever more creative solutions and be familiar with the context of their solutions. This means understanding business, human nature and environmental issues.

We live in an age of multiple careers, and many engineers take the opportunity to change careers by taking roles in areas such as business, education, government or management. However, it seems very few people in these roles ever consider moving into engineering. Therefore, another initiative that would help boost our engineering workforce is to provide accessible sponsored pathways for current technology based workers to re-skill or upskill and become professional engineers.

What do you do in your free time to relax?

I relax by listening to audiobooks. I now have over 300 books in my collection with a leaning, as you might expect, towards science fiction. Having a story brought to life by a skilled narrator is completely immersive. Master storytellers such as Alastair Reynolds and Peter F. Hamilton bring such depth to the characters and futuristic worlds that I challenge anyone's imagination not to be set on fire.

I also like to be in nature, whether it is while visiting my mother in the beautiful Devonshire hills, or simply walking the dog with my wife. Taking time to be outside, to breathe fresh air and listen to our surroundings can be the best antidote to our busy stressful lives and the seemingly never-ending to do lists.

Given one wish what would that be?

My one wish would simply be for everyone to be a good neighbour. A good neighbour to each other and to every living creature. A good neighbour cares, respects and supports others. A good neighbour is driven by curiosity and doing the right thing, not by hatred, envy, fear or greed.

... or maybe the ability to fly, clearly the coolest superpower.

> Our digital age makes us more informed and yet strangely less informed. It also shrinks the world and yet isolates us at the same time. However, the good news is that I meet young engineers almost every day who not only express concern over these issues but also have a quiet determination to tackle them.

KEEP CALM AND CARRY ON DEALMAKING

Roger Buckley, Corporate Finance Partner, BDO LLP reviews Mergers and Acquisitions in the Test & Measurement market in 2018

You could be forgiven for expecting to see a decline in the M&A market through 2018 given the prevailing geo-political climate: Brexit, trade wars, stock market volatility, climate change and national security issues are a daunting ensemble of perils. But in fact the reverse has been true. Businesses and financial investors have been stolidly standing by a "keep calm" mantra, pragmatically focused on the opportunity to carry on building great businesses.

The final quarter of 2018 finished with a flurry of deals. 748 UK transactions completed in Q4, a prodigious rise of 21% according to the latest analysis from accountancy and business advisory firm BDO LLP. Q4 was by far the busiest quarter of the year, with both trade and private equity seeing significant increases in deal volumes. Overall, 2018 saw 2,569 deals complete, representing an 8% increase on 2017 volumes. The resilience of buyers and dealmakers has defied prevailing economic and political uncertainties.

Likewise, valuation multiples held firm, with private equity continuing to pay higher multiples on average than trade. Trade multiples, represented by the Private Company Price Index (PCPI) rose slightly to 10.4x while the Private Equity Price Index (PEPI) saw a small increase to 12.1x in Q4, confirming the abundance of investment capital available and the willingness to pay well for attractive assets.

Test & Measurement Q4 deals: volumes sustained at record-breaking levels

As with the overall market, deals in the Test & Measurement sector saw another strong year in M&A, with 377 deals completing across the globe in 2018. Following three years of double-digit growth between 2014 and 2017, 2018 volumes sustained at record-breaking levels.

North America continued its impressive growth trajectory, contributing 20% increase in deals in the year. Accounting for half of all M&A activity in 2018, the US & Canada continue to lead the market in deal volumes and deal values.

Transaction volumes in UK and Europe retained their strength and were broadly flat year on year.

Big ticket deals in the quarter include Amphenol's acquisition of SSI Controls Technologies for $400m, a manufacturer of sensors and sensing solutions for the global automotive and industrial markets, also MKS Instruments' acquisition of Electro Scientific Industries for $1bn, which will strengthen expertise in the photonics and optics market, enabling the development of systems to address evolving technology needs.

US buyers have been equally keen on the UK market. Examples include the acquisition of Malvern-based Pulsar Process Measurement, a manufacturer of ultrasonic and radar based non-contact level and flow measurement instruments, by US flow measurement specialist ONICON, and the acquisition of Devon-based Aero Sense Technologies a manufacturer of custom sensors for industrial and aerospace OEMs, by Bridgepoint-backed Safety Technology Holdings. These UK deals add many new opportunities for the acquirers including new technologies, new markets, while magnifying global reach.

The UK remains a hub of quality T&M businesses and continues to attract a high proportion of overseas investors. Yet in 2018, UK buyer appetite increased significantly: compared with 2017, there was a 25% increase in the number of UK acquirers completing transactions in 2018. UK businesses have been spurred into action by future threats, pressing on with acquisitions to solidify their domestic presence and shore up their interests abroad ahead of Brexit. Examples include Chelsea Technologies Group joining forces with Sonardyne International to extend its reach in environmental sensing technologies, and Cohort's acquisition of Chess Technologies to create its fifth advanced technology business.

The rise and rise of private equity

A stand out feature in the last year has been the tremendous increase in private equity investment flowing into the T&M market. Compared with the previous year, 2018 saw an 84% increase in deals backed by private equity investors, and in Q4, they accounted for over a fifth of all deals.

In the UK & Ireland, Battery Ventures continued to build its T&M platforms in Q4, firstly with the acquisition of Mecmesin, a provider of force and torque testing by Battery's Physical Properties Testing group, then with the acquisition of NTRON, a global provider of gas measurement sensors and process oxygen analysers by Process Sensing Technologies. These deals follow hot on the heels of the acquisition of Dynament and Status Scientific Controls, manufacturers of infrared gas detection sensors and instruments, deals on which BDO advised earlier in the year.

New capital continues to flood the market, and is not expected to dry up anytime soon. BDO carried out a straw poll of PE houses which revealed that the amount of capital allocated to the UK middle market would stay strong through to 2025. The UK comprises a large, highly evolved market full of innovative and entrepreneurial people, and good returns are still expected in spite of Brexit. Will there be a little more caution? Perhaps. According to market rumours, Spectris, the UK listed instrumentation and controls business, was in sales talks with Bain Capital and Advent International in December, but a deal reportedly floundered amid the Brexit uncertainty.

So what will 2019 bring in the T&M market?

There are signs of stronger headwinds as we look ahead through 2019. Towards the end of Q4, the FTSE all share index dropped to 11.5x, the lowest level seen in four years, and potentially a harbinger of a valuation decline in private company M&A. BDO's latest Business trends report also indicated a degree of sliding market confidence. However, strong fundamentals remain in the T&M market which should sustain its treasured status. The robust regulatory drivers, emerging requirements driven by Industry 4.0 and high growth potential underpinning much of the T&M market mean that it will remain highly attractive to investors.

Roger Buckley, M&A Partner at BDO LLP, commented:

"The M&A market has remained resilient, with strong transaction volumes and values persisting through to the end of 2018. 2018 saw huge capital flows in the market fuelling demand and outstripping supply. While there may be some market challenges ahead, our experience as the no.1 UK M&A advisor in 2018 leads us to be cautiously optimistic about deal flow in the T&M market through 2019."

ASK THE EXPERTS

I see instruments occasionally described as "smart" or "dumb". What does this mean and why does it seem important?

Yours sincerely,
Angry of Mayfair.

Tom S Nobes of Central North-West Local Section replies:

Background

The origin of instrument measurement principles was essentially all mechanical. Measurements were made by say; how a diaphragm deflected under pressure, how a fluid expanded when heated and the height of a weir when water was flowing. These were all "dumb".

Over time, instruments became more complex, the first breakthrough being pneumatic instruments in the 1950s.

The advance of analogue electronics in thermionic-valves and later transistors enabled instruments to become "electronic" in the 1960s.

By the 1980s; digital electronics were used in instrumentation. The digital processing including a digital signal protocol – HART™.

By the late 1990s; bus systems were part of instrumentation; including ProfiBus™ and Fieldbus Foundation™.

Now wireless is increasingly popular; including WirelessHART™ and ISA100Wireless™.

All these developments have of course provided the user with improved accuracy, diagnostics, reduced costs, reduced physical size and the ability to implement complex control strategies.

The confusion starts because almost all the above technologies are all still available!

The first questions is "does this instrument contain a microprocessor?". This only has a yes/no answer.

If yes, the second question is "how large or complex is the software inside the microprocessor?".

A smart instrument

A smart is defined as meeting the following criteria:

- To measure or directly control a single process variable.
- It uses at least one microprocessor.
- It is 'commercial off the shelf'.
- It includes flexibility in its use due to parameters set by the manufacturer or user.
- Its lifecycle includes generic firmware (aka Fixed Programming Language) produced by the manufacturer followed by particular configuration by the user.
- Smarts are not restricted to just measurement, i.e. transmitters, but include actuators, valves, motor variable speed drives and other control equipment.

Examples of what equipment would be categorised as a smart:

- Pressure, temperature, flow, level, density, pH, and conductivity transmitters.
- Process controllers, three-term (PID), recorders and data-loggers.
- Gas detectors, cameras, etc.
- Motor starters, speed controllers, and 'soft' starters, control valve actuators.

Examples of what equipment which would not be categorised as smart equipment:

- Instruments not containing microprocessors like pressure gauges, variable-area flowmeters (Rotameters), flow-switches, etc.
- Large assay type special instruments (very complex, custom built instruments, etc.). These often have unique requirements and feature voluminous, novel or custom firmware (called Full Variability Language) often running on a full PC.
- DCS, PLC or SCADA. Having a configuration unique to a particular plant and affecting many variables and loops.

As a guide to naming the ascending order of complexity might look like –

Dumb (D) > smart (S) > programmable electronic system (PES).

Why it's important

The main area where the definition is important is functional safety. To take part in an instrument loop delivering functional safety (alarms, trips, interlocks, etc.) an instrument must have a known reliability and its' potential failure-modes known.

Dumb instruments are simple by nature, have relatively few components and probably already have a long proven-in-use history. Where such data is not available, it's relatively easy to stress-test dumb instruments (heat/cold, vibration, over-ranging, etc.) to provide a bench-mark.

Smart instruments will by nature be more complex. Most importantly, they will contain software. Proving the reliability of software has historically proven to be difficult. It's fair to say software can produce non-repeatable apparently random errors (think of your work IT where occasionally you can't print or open a document, only for the fault to disappear as quickly and mysteriously as it arrived). IEC61508 and it's supporting IEC61511 contain guides on how to produce reliable software for use in safety systems.

regards,
Tom S Nobes. C.Eng. F.InstMC

Smart instruments will by nature be more complex. Most importantly, they will contain software. Proving the reliability of software has historically proven to be difficult. It's fair to say software can produce non-repeatable apparently random errors (think of your work IT where occasionally you can't print or open a document, only for the fault to disappear as quickly and mysteriously as it arrived).

Do you have questions for the our experts? Please send them to publications@instmc.org

OUR CORE TEAM

OFFICERS

President
Professor Graham Machin

Honorary Secretary
Dr Graeme Philip

Honorary Treasurer
Colin Howard

Engineering Director
Dr Maurice Wilkins

Chief Executive Officer
Patrick Finlay
Tel: +44 (0)20 7387 4949
patrick.finlay@instmc.org

Accounts Manager
Ernest Kyei
Tel: +44 (0) 207 387 4949 Ext 4
ernest.kyei@instmc.org

Bookkeeper and Subscriptions Manager
Roy Ginn
Tel: +44 (0) 20 7387 4949 Ext 1
accounts@instmc.org

Head of Communications & Marketing
Stephanie Smith
Tel: + 44 (0) 207 387 4949 Ext 5
steff.smith@instmc.org

Business Executive
Sydney Reed
sydney.reed@instmc.org

Head of Operations
Aytan Malka
Tel: +44 (0) 20 7387 4949 Ext 7
communications@instmc.org

Head of Membership
Leila Atherton
Tel: +44 (0) 20 7387 4949 Ext 3
membership@instmc.org

Membership Support Officer
James Sinton
Tel: +44 (0) 20 7387 4949 Ext 4
admin-subs@instmc.org

1680m²

DEDICATED VALVE OVERHAUL,
REPAIR & UPGRADE FACILITY

kentintrol

INDUSTRY LEADING OEM VALVE SERVICES FOR YOUR APPLICATION

Our team of specialist engineers have overhauled, repaired and upgraded valves from our fully equipped aftermarket facility for our global client base for more than 50 years.

ENGINEERING EXCELLENCE SINCE 1967

KOSO

OUR VALVE SERVICES:

- OVERHAUL & REPAIR
- UPGRADES & RETROFITS
- SERVICING & MAINTENANCE
- FAST TRACK SPARES
- VALVE DIAGNOSTICS
- VALVE TESTING
- SHUTDOWN PROJECTS
- VALVE MAINTENANCE TRAINING
- ASSET LIFE EXTENSION

EPIMJQS

kentintrol.com/services

T: +44 (0)1484 710311 | E: info@kentintrol.com

C&C
TECHNICAL SUPPORT SERVICES

TÜVRheinland®
Precisely Right.

FS Engineer & Technician (TÜV Rheinland) Certificate Training 2019

FS Engineer SIS:

Aberdeen: **4-7 March, 3-6 June, 23-26 September & 2-5 December**
Weekends: **(11-12 + 18-19) May & (9-10 + 16-17) November**
London: **25-28 March & 9-12 September**
Manchester: **1-4 July**
Paris: **18-21 June & 26-29 November**

FS Technician:

Aberdeen: **13-16 May & 11-14 November**

Introducation to Functional Safety:

(The ideal 1 day workshop to prepare for the FS Engineer course, or for any staff/managers)

Aberdeen: **7 June & 13 September**

C & C Technical Support Services is an accepted course provider of the TÜV Rheinland Functional Safety Training Program.

Please contact us to register or for more details:

Email: *info@silsupport.com*
Or Tel: +44 (0) 13398 86618

View our full Global schedule at:
www.silsupport.com