THE MAGAZINE OF THE INSTITUTE OF MEASUREMENT AND CONTROL

INSTMC.ORG

InstMC

WHAT MAKES AN IMAGE SCIENTIFIC?

WE ARE SURROUNDED BY IMAGES IN EVERYDAY LIFE, AND WE EFFORTLESSLY ASSIMILATE VAST QUANTITIES OF INFORMATION AT EVERY GLANCE.

AUTOMOTIVE CYBER SECURITY: CHALLENGES FOR ENGINEERING AND RESILIENCE

SAFETY STANDARDS FOR HOME HEALTHCARE DEVICES

STANDARDISATION OF GRAIN SIZE IN NEW ENGINEERING MATERIALS

WIRELESS GAS DETECTION AND MONITORING IN THE OIL, GAS AND OFFSHORE SECTORS

ARE ALARMS CREDITWORTHY?

MARCH 2021_ISSUE NINETEEN

PRECISION

INSTMC WELCOMES NEW TRUSTEE AND INSTMC VICE PRESIDENT DR. MAURICE WILKINS

I stumbled into process automation and control in 1978, when I was looking for a job after graduating from Aston University with a PhD in chemical engineering. A friend of mine, who had graduated from Aston a year earlier was working as an application engineer at Esso Chemical, Fawley, Hampshire and he told me there was a vacancy. I applied, with very little knowledge of automation, but luckily got the job. With a wonderful group of colleagues around me, I picked up the fundamentals quickly and really enjoyed what I was doing. So much so that I am still working in automation 42 years later and have achieved some of our industry's highest honours and recognitions.

When I started work, it was the dawn of a new age in automation, the introduction of the DCS (distributed control system), so I was involved in many very interesting projects converting panel based, pneumatic controllers to digital and moving operators to blast proof, central control rooms. I learned so much in a short time. I then moved to work for Honeywell, Esso's supplier, where I spent almost ten years, eventually ending up in Brussels, via Phoenix, as a batch control expert. While in Brussels I joined Honeywell's global strategic consulting team, assessing customer sites against best-in-class practices and making recommendations for improvement. Eventually, I set up my own company doing the same thing. One of my clients asked me to 'walk the talk' and implement my improvement plan.

So, in January 2001, my then fiancé and now wife, Sara, moved to Jacksonville, Florida and I was tasked with implementing my strategic automation plan at Millennium Specialty Chemicals, a flavours and fragrances company. I made many changes and improvement to the site before joining the ARC Advisory Group as a consultant in 2006.

In late 2007, my dream job materialised. I was asked by Yokogawa to form a new Global Strategic Marketing Team in Dallas, Texas, reporting to Tokyo. I hand-picked a group of high-profile industry specialists and, as a team we provided input and support to Yokogawa's global regions on standards, market trends and innovations, including cyber security and wireless.

I had been involved with InstMC for many years, but had let my membership lapse, until I was asked to revitalise the Texas section. I became an InstMC Fellow and worked with Walt Boyes and Clive Wilby to start things moving again in Texas, but then moved back to the UK in late 2015, to become Executive Advisor to Yokogawa's marketing HQ.

On my return to the UK, I contacted InstMC and offered to volunteer, having enjoyed my US experience. Patrick Finlay didn't need much convincing and snapped up my offer. I have now had five enjoyable years helping the Institute, as its volunteer Engineering Director and Chair of the Digital Transformation and Standards SIGs and look forward to many more. I have met some wonderful people and am now honoured to have been elected as a Trustee and Vice President and look forward to continuing to mould the future of the InstMC in the coming years.

Maurice Wilkins Vice President
Institute of Measurement and Control

CONTENTS

ARTICLES

PRECISION

The magazine of the Institute of Measurement and Control
Published by: Institute of Measurement and Control
297 Euston Road, London NW1 3AD T: +44 (0) 20 7387 4949
www.instmc.org
www.twitter.com/instmc
www.linkedin.com/company/institute-of-measurement-and-control-the-

Chief Executive Steff Smith
E: steff.smith@instmc.org

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

Cover price, where sold, £15

WHAT MAKES AN IMAGE SCIENTIFIC?

BY DR DAVID M GORMAN,
NATIONAL PHYSICAL LABORATORY

We are surrounded by images in everyday life, from the constant bombardment of adverts to binge watching the latest crime docudrama on Netflix, and we effortlessly assimilate vast quantities of information at every glance.

Even now you are reading images of words which are in turn conjuring images in your mind. Our familiarity with images might make them seem mundane, yet, they have been instrumental in answering some of the biggest questions in science; from vast arrays of radio telescopes that map signals from when our universe was in its infancy, to room filling electromagnets that functionally image living brains and provide insight into the origin of thought; images are a powerful tool for scientific observation. As with most things we are familiar with it is not often that we stop to ponder their nature, but what exactly is an image and, in considering this question, how do scientific images differ from your average photograph?

In the broadest sense an image is simply a representation of something else, a format of data that captures and codifies aspects of an object, concept or process. The format of the image provides an intrinsic layer of information that differentiates image data from simple lists of numbers. The format not only dictates how datapoints should be interpreted, for example converting numbers into colours, but also how the data is discretised and positioned in relation to each other. In a standard digital photograph, and to a first approximation, a pixel represents a region of space, a pyramidal frustum, with adjacent pixels representing adjacent regions. This simple yet important quality of images allows information such as form, texture or any dynamic property of a system to be efficiently encoded in the relationship between pixels. Consider the following binary image, despite the pixels being limited to values of only 0 or 1, black and white, many intricate details of the Big Ben Clocktower (Fig. 1) are still apparent. Therefore, we can say in general terms, images are comprised of data, but they are themselves the synthesis of that data into an ensemble of information. You may then ask, if you repeatedly crop an image until you reach its smallest denomination does it stop being an image? The answer to this question depends on the method used to generate the data and is one of the features of scientific images that differentiate them from the average photograph.

The next picture (overleaf) is the hexadecimal number #c8dfff interpreted in hex triplet format as a single pale blue pixel. This pixel is not an image when considered in isolation, however, could it be? On the 14th February 1990, the Voyager 1 space probe took a photograph of our solar system at ~3.7 billion miles from earth (Fig. 2). By synthesising information of the probes position in space, the direction the probe was pointing relative to the earth and the capabilities and settings of the camera when it took the image, the single pale blue pixel is realised to be an image of the earth. Data associated with an image that is not contained within the image array is called metadata and there is no limitation on what information it can contain. Metadata provides context to an image and, in the current example, has elevated a single hexadecimal number into an image of all life in the known universe.

Figure 1.

Figure 2.

Pale Blue Dot is a photograph of planet Earth taken on February 14, 1990, by the Voyager 1 space probe from a record distance of about 6 billion kilometres (3.7 billion miles, 40.5 AU), as part of that day's Family Portrait series of images of the Solar System.

Formatted image data accompanied by metadata provides a powerful tool for scientific observation, however, to make the best use of this tool requires one further refinement. In the previous example the earth has been approximated as a pale blue dot, profound as this image may be, how certain are we that the image is an accurate representation of the truth? Let us assume we wish to use this image as an exemplar to search for trace amounts of light coming from Earth-like planets in other solar systems. In this scenario we have a high-powered telescope that is very different in construction to the now 40+ years old camera on the Voyager 1 space probe. To ensure agreement between the two systems requires both to be calibrated to a reference standard and corrections applied to any influential factors that may alter the resulting images. To achieve this there is more to consider than just the system optics and the transfer function of the detectors that collect and measure the intensity and frequency of incident light. It is also necessary to calibrate the spatial relationship between pixels to ensure that real space is correctly mapped into image space. Furthermore, the response of the system may vary as a function of time or environmental factors requiring, for example, temperature and humidity measurements to be included in the metadata. In this instance, the temperature measurement is not seen in the image array, yet it is still a part of the information that constitutes the image. In summary a quantitative image is a form of measurement, an ensemble of information that attempts to capture an objective truth. In order to achieve objectivity a calibrated imaging device must simultaneously acquire an image of its subject and itself including any pertinent information required to trace and validate its calibration.

Before a quantitative image can be used it is necessary to consider how information is being changed by the imaging process and assess its suitability to address the question being posed. The parrot montage (Fig. 3) exemplifies four common forms of information degradation that occur during imaging; spatial discretisation, blurring, stochastic noise, and spatial distortion. The top image on the left is the original image. The second row shows the difference between the top row image and the original image and the bottom row depicts the gradient information (edges) of the top row images for each respective column. Most likely you can determine the subject in each of the images, a parrot; after all, you are highly sophisticated image analysis hardware yourself. However, could you tell that the image on the right has been distorted if you didn't have the original? Could you quantify to what extent the information in each image has been degraded? Let us ask a thought-based question; which of the distorted images is the best quality? The answer to this, of course, depends on what you intend to use the images for. Let us assume that the image is both colour intensity and spatially calibrated and consider the following questions; How many stripes does the parrot have around its eye? How long is the parrot's beak? Spatial distortion at this level does not affect your ability to count the stripes. Noise does not affect your ability to count the larger strips but does introduce uncertainty and a detection limit on the smaller ones. Pixilation and blurring both prevent you from counting the stripes, however, high resolution information could be recovered in the blurred image by deconvolving it with the kernel used to apply the blur, whereas pixilation has simplified the data and destroyed that information.

Now consider the length of the beak, this requires the spatial information to be correct and the edges of the features to be measurable. Look at how each distortion effects the edge information in the bottom row. The edges can still be determined in the blurred image, although with greater uncertainty than in the original. Pixilation, noise and spatial distortion either destroy or obscure the edge information. In reality, these modes of information degradation operate in concert to varying degrees and it is the job of scientific image analysists to enhance and extract information from images to best answer specific questions. The challenge is to preserve the quantitative aspect of the initial measurements through the processing pipeline and ultimately propagate any uncertainty to the derived metrics.

So, what make an image scientific? An image needs only to be accepted in support of a scientific hypothesis to be classed as scientific, the hand drawn images of neurons by Santiago Ramón y Cajal are an exquisite example of this. However, there are limits to what the eye can interpret, and the scientific questions being posed, and equipment used to answer those questions are becoming increasingly complex. The whole imaging process from data collection, analysis and application to a specific question must be considered before seeing becomes believing. I hope this article has demonstrated that images can be more than what meets the eye and provides some insight into their use within the sciences.

Figure 3.

AUTOMOTIVE CYBER SECURITY: CHALLENGES FOR ENGINEERING AND RESILIENCE

BY PETER NORMAN, IENG, MINSTMC, MIET

Cyber Security resilience is a critical and increasing challenge for current and future road vehicles due to the rapid growth of connected and autonomous vehicles (CAVs). The more connected a vehicle becomes, the greater the cyber attack targeting risks.

Safety-critical components exist in every top selling make of new car and are directly connected to the internet. Progressive levels of vehicle autonomy will further increase the significance of these connections. The potential for cyber attacks on vehicle networks increasingly threatens the functional safety of targeted vehicles.

Objectives of automotive cyber attacks may include: theft of valuable vehicles; deliberate crashing of vehicles for insurance; and malicious grid-locking of cities by engineering multi-vehicle pile-ups. Many human lives could be put at risk by remotely taking control of vehicles to cause physical injury or death. Traditional computer security strategies based upon the goals of confidentiality, integrity and availability need refocusing to protect CAVs. A great fear is that the in-vehicle infotainment (IVI) system could be used as an access point to harmfully control braking and steering functions.

Maintenance of electronic vehicle security and of the associated Intelligent Transport Systems (ITS) will become increasingly important as electronic/cyber ecosystems develop for CAVs to plug in.

The challenges faced by the automotive industry

Currently, protecting vehicle functions against unauthorised access and unwelcome manipulations is a central challenge for the Engine Control Unit (ECU), also referred to as the Engine Control Module (ECM). The essential function of these control units or modules is to collect engine measurement data from a multitude of engine sensors. The ECU/ECM then controls a series of actuators, on an internal combustion engine, to ensure optimal engine performance. The collected data is stored for interpretation via look-up tables in order to adjust the engine's actuators. Cryptographic functions are required within the ECU/ECM to protect the valuable stored data.

A revolution in modern electronics is in the use of smaller, energy-saving, transistors to increase speed of response along with Cerebras Wafer Scale Engine for Artificial Intelligence (AI). This is leading towards the creation of more complex electronic chips containing 1.2 trillion transistors for vast operational memory and bandwidth. Sensors on vehicles are also increasing as levels of autonomous driving control progress. The Society of Automotive Engineers defines 6 levels of driving automation ranging from 0 (fully manual) to 5 (fully autonomous) within which our vehicles equate to having semi-autonomous features for driver assistance.

Aspects of vehicle vulnerability

Security vulnerabilities were previously discovered by computer scientists within the ignition immobiliser systems of some vehicle manufacturers. Researchers from the University of Birmingham, UK have reverse-engineered firmware and easily discovered encryption keys for vehicle immobilisers. Vehicle thieves, of course, can also wirelessly access signals from vulnerable Smart key devices to gain entry to vehicles.

The presence of 40% electrical and electronic devices and a typical quantity of microprocessors ranging from 50~100 per vehicle raise challenges of complexity within modern vehicles. The addition of AI further exacerbates complexity. Complex vehicles can have 100 million lines of code which continues to grow.

Vehicle to Everything (V2X) is a very promising technology based upon IEEE 802.11 which is part of the IEEE 802 set of local area network (LAN) protocols. The use of V2X, WiFi, Bluetooth, GPS, onboard camera(s), wireless type-pressure monitoring, radar and Lidar by vehicles could render them susceptible to remote, unauthorised access. Vehicles also have USB ports and media players. Electric Vehicles (EVs) could become vulnerable via the EV charging point. There are also remote vehicle connections to the ITS, OEM backend and the service provider. Adverse manipulation of data could occur prior to its transmission and there is much work still to do on the V2X threats to vehicle security.

The benefits of connecting vehicles

V2X permits connection of vehicles to each other and also to the wider world, to enable performance beyond individual human drivers. V2X improves driving safety for actions such as vehicle lane-changing and optimising traffic flow through the use of Cooperative Awareness Messages and Decentralised Environmental Notification Messages for hazard avoidance. Vehicles are already capable of automatically transmitting useful data to emergency services for road accident assistance.

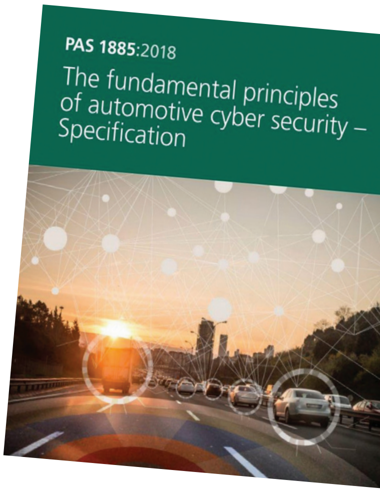
New methods to engineer and ensure resilience

New methods are needed to engineer and ensure resilience, which are essential so that security mechanisms can evolve throughout the vehicle life. This new approach increases the likelihood of detecting and responding safely to threats that were not known when the vehicle was designed. Achieving trusted and resilient mobility through proactive and reactive engineering will be necessary whilst also complying with all legal regulations, e.g. General Data Protection Regulation (GDPR).

A Defence in Depth strategy would be to: design with security in mind; control the production and test environment; control the perimeter; actively manage the software and firmware patch and Over-The-Air update mechanisms. Then test, test and test again to reveal any hardware or software bugs and malicious attacks, that is functional and structural monitoring of defects and degradations.

Standards

A British Standard already in force since 2018: PAS 1885:2018 covers the fundamental principles of automotive cyber security and is based upon a high-level set of guidelines developed by the UK Department for Transport in conjunction with the Centre for the Protection of National Infrastructure. It is aimed at all stakeholders within the automotive supply chain. More details can be found on the British Standards Institution (BSI) website https://www.bsigroup.com/en-GB/



There also exists ISO/IEC 15408 consisting of three parts. This international standard, however, is non-binding and can be implemented to test the security of IT systems in any sector. Although it can provide a baseline for an automotive cyber security system, it may fall short of being truly fit for the automotive security challenges. More details of this ISO can be found on the European Union Agency for Cybersecurity website.

Newly emerging cyber security standards are expected during 2021 consisting of the ISO 21434 from ISO and SAE as an international framework for compliance with the new United Nations Economic Commission for Europe Regulation WP.29/GRVA for CAVs (now accepted) which places new requirements on vehicle manufacturers and the supply chain. Another ISO/WD PAS 5112 is under development for product development audit and assessment monitoring and incident response.

UK Research information

Numerous UK projects include: Secure-CAV, MuCCA, Secure IoT, Project Meili, ResiCAV details of which can be discovered via internet searches. Coventry University and the University of Southampton are involved with Secure-CAV. There also exists the non-profit-making Automotive Security Research Group. https://asrg.io/

Q&A

Nick Oliver

Nick Oliver, Instrument & Control Technical Authority at Perenco, shares his thoughts on the past, present and future of engineering.

What was the root of your interest in Engineering?

From an early age I was immersed in machines and technology as my father was a mechanic and owned a small garage and an old fishing boat. Saturday mornings were spent scouring scrap yards for useful parts or more often just interesting things while evenings were spent working on cars. This taught me that machines are not just black boxes to be plugged together, but a collection parts that are interdependent; if one part is not performing or is stressed, it affects the whole. You have to understand what goes on inside a component to make best use of it.

What is your vision of Engineering in Britain for the next ten years?

My vision for the next ten years is that engineering will become diversified in more than just demographics. For engineering to thrive in the next ten years engineers, will have to break out of their niche. Without understanding how your own engineering efforts link into a wider environment, you won't find the efficiencies and improvements needed to compete on a world stage.

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

The government should make engineering as appealing a prospect as other professions. Schools should offer engineering not as an alternative career but as a first choice. Often the best and brightest are encouraged into medicine, the city or service industries but, if we lead with world class enthusiastic engineers, we can change this perception that engineering is, somehow, second class.

I moved from being a trades supervisor to an engineer later in life, and I was very lucky to be sponsored by my employer, Manx Electricity Authority. Mature students more often than not have commitments and responsibilities and taking two years out from work is difficult for most. Support for both young students and those entering the second part of their career could be supported by extending Education Maintenance Allowance and improving the repayment terms of student loans for those studying STEM subjects.

"Saturday mornings were spent scouring scrap yards for useful parts or more often just interesting things while evenings were spent working on cars. This taught me that machines are not just black boxes to be plugged together, but a collection parts that are interdependent; if one part is not performing or is stressed, it affects the whole."

Often the best engineers have a trade's background and encouraging them to progress from the tool room to the desk needs support. The support in the 21st century has to be in education and not just on the job; they need the academic discipline from a degree to give them the analytics they need to be a great engineer.

What do you do in your free time to relax?

In times gone by I raced motorbikes and still have a keen interest in club and roads racing. These days however, I have two young daughters (who I hope will become engineers) so risky pastimes are not on. Home maintenance and travel, when permissible, use up any spare days I have.

Given one wish what would that be?

Aside from an early conclusion to the Covid crisis, I'd wish that all managers, project managers, engineers and accountants would take into consideration the wider aims and goals of their company. We get tunnel vision and want to see our own goals achieved without thinking of the overall strategy. Managers want the least disruption even if longer term efficiencies might be realised by change. Project managers want to close out on time and on budget. Engineers want the latest, best solution often scrapping serviceable systems in the name of uniformity or unnecessary features. Accountants look to the balance sheet. If we all took a step back and consideredthe company's needs rather than more personal goals we might well make better decisions.

SAFETY STANDARDS FOR HOME HEALTHCARE DEVICES

ROJAN KARMACHARYA, FIELD APPLICATION ENGINEER, SL POWER ELECTRONICS

Health cost has been rising over the years and so has life expectancy.

Health care/medical providers have been looking at ways of providing better quality care at a reduced cost. One of the ways to do this is to provide treatment and monitoring at home. There is a growing need for affordable, reliable and convenient professional medical services at home. Most who benefit from this type of care are patients who would prefer to recuperate at home to save money, those who are disabled, or patients with complex treatment or chronic diseases that require use of medical equipment and/or medication monitoring. Regulatory agencies have identified that there are unique risks and implications that need to be considered with powered medical equipment. Standards specifically defining the requirements for the home healthcare environment were published in 2010. Requirements for medical electrical equipment and medical electrical systems must be incorporated into home environment use devices, along with other applicable standards in the IEC60601. The market for home health care devices and equipment is expected to grow exponentially as the delivery of health care shifts from a clinical environment to a home setting in the coming years.

Until as recently as 2010, many manufacturers of healthcare equipment intended for use in the home have been required to demonstrate compliance with the provisions of IEC 60601-1 "Medical Equipment, Part 1: General Requirements for Basic Safety and Essential Performance".

As originally developed, this standard was intended to apply to medical devices used in clinical settings by trained medical professionals. To obtain certification for their products, manufacturers of home healthcare equipment have been required to comply with the provisions of IEC 60601-1, and to demonstrate that their product design effectively mitigates the risks associated with use in the home by patients or caregivers.

IEC 60601-1-11 and Home Healthcare Equipment

In April 2010, the US Food and Drug Administration (FDA) and the Center for Devices and Radiological Health (CDRH) published documents to outline the Medical Device Home Use Initiative. Late in 2010, International Standard IEC 60601-

1-11 "Requirements for Medical Electrical Equipment and Medical Electrical Systems Used in Home Care Applications" was published. IEC 60601-1-11 is a collateral standard, meaning that it directly references provisions in IEC 60601-1, and is used in conjunction with IEC 60601-1 for the certification of home healthcare equipment. IEC 60601-1-11, deals specifically with the requirements applicable to medical devices intended for use in the home environment. Under its provisions, manufacturers must identify the specific product safety risks associated with the use of their equipment in uncontrolled environments by untrained users. To achieve certification, manufacturers must mitigate those risks through a combination of appropriate product design, user instructions and training, and maintenance protocols. While IEC 60601-1-11 is intended to cover most home healthcare equipment, it is important to note that some devices may still be subject to the requirements of other standards. For example, UL 1431 "Personal Hygiene and Health Care Appliances" covers household electric products for hygiene or other healthcare applications rated at 250 volts or less.

IEC60601-1-11 deals with general requirements, testing requirements, classification, identification, marking, documentation, protection against hazards, protection against strangulation/asphyxiation, and Electromagnetic Emissions.

Classification of Medical Equipment and Medical System

In addition to the requirements of the general standard, unless the Medical Equipment intended for the Home Healthcare Environment is permanently installed, it:

- shall be CLASS II (2 wire AC input – no ground connection at the input) or internally powered;
- shall not have a functional earth terminal; and
- if equipped with APPLIED PARTS, shall have either TYPE BF APPLIED PARTS or TYPE CF APPLIED PARTS.

Compliance is checked by inspection. In addition, the input voltage range is increased, requiring the medical device to operate from a lower input voltage, 80 % or 85 % of the nominal rated voltage depending on the type of medical application as well as increased immunity to electromagnetic disturbances from other devices in the environment.

Class II

There are considerable numbers of houses both in the US and Europe which were built before 1950 that do not have reliable earth ground wire. IEC 60601-1-11 requires that all medical devices for home use which are not permanently installed by licensed personnel have class II AC input. The safety from electrical shock in Class II power supply comes from the construction. Where additional insulation and spacings are needed, two layers of insulation or a single layer of reinforced insulation must be provided between the user and current carrying conductors.

Added protection

In addition to existing general medical standards, when performing the usability engineering process, the risks associated with usability in the home healthcare environment for operator profiles, including a lay operator, shall include consideration of at least:

- changes of controls
- unexpected movement
- potential for misconnection
- potential for improper operation, or unsafe use
- potential for confusion as to current operational mode
- change in the transfer of energy or substance
- exposure to environmental conditions specified in this standard
- exposure to biological materials
- small parts being inhaled or swallowed.

Power supply, interruption and interference

Essential performance criteria for IEC60601-1-11 are to be able to provide safety backup should there be power interruptions. In case of a power outage the medical equipment should be able to provide back up for life sustaining medical equipment to be operational until an alternative supply is deployed. Power supply features such as bidirectional communication and higher hold up time will be useful to integrate the backup power source in case of power loss.

An updated version IEC60601-1-11: 2015 was released in 2015 which superseded and replaced the old IEC60601-1-11: 2010. Some of the key requirements of IEC 60601-1-11 relate to the power supply being used for this equipment. A power supply that meets the home health care standards can be easily integrated into medical equipment for the home healthcare environment.

As the home healthcare medical equipment market expands due to an increase in home based medical needs, understanding the safety standards IEC 60601-1-11 healthcare is very important to quickly access this market.

AN INTRODUCTION

The Institute of Measurement and Control is committed to promoting the professional excellence and standing of engineers and technologists at all levels in the automation, instrumentation, control and related industries. Our aims are to serve the public by advancing the science and practice of measurement and control technologies and their various applications, to foster the exchange of views and the communication of knowledge and ideas in these activities, and to promote the professional development and qualification of our members.

In 2017 the Institute launched a new quarterly magazine which is a high quality journal with technical features related to measurement and control. This coffee table type magazine is circulated to the InstMC 3002 individual and 100 company members. It is also aimed at anyone interested in the various uses of measurement and control.

It is a positioning and marketing tool for the Institute as well as raising awareness to a wider audience of the use of measurement and control in the world today.

ADVERTISING RATES

Discounts can be given if 3 or more adverts are taken. POA.

Full Page	£1,375
Half Page	£825
IFC	£2,200
IBC	£2,200
OBC	£2,200

INSERTS

A4 & A5 Inserts	£825

Inserts are accepted into Precision magazine and must go to the entire UK circulation.

CIRCULATION BREAKDOWN:

2376 UK Engineers / 626 Overseas Engineers
100 Companion Company Members

PRECISION MAGAZINE

INSTMC SPECIAL INTEREST GROUPS

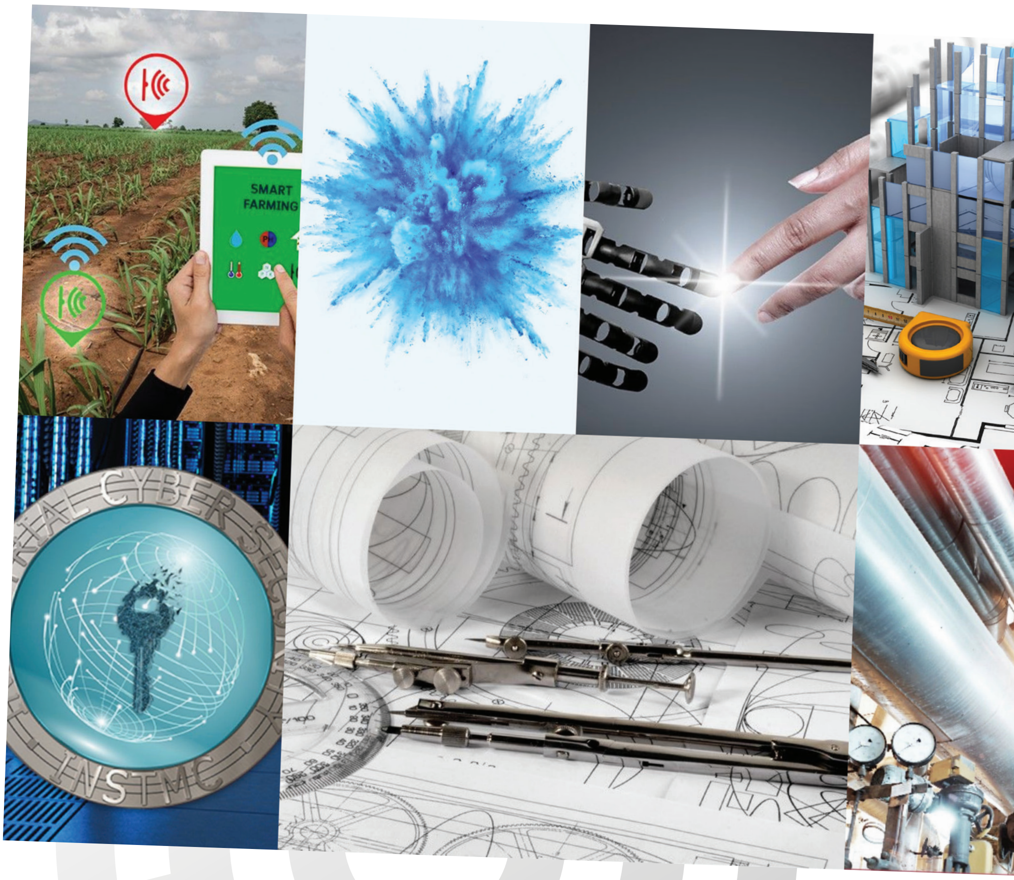
InstMC SIGs provide an opportunity for like-minded engineers to network, share ideas and expertise, collaborate and learn, and keep updated on industry news and developments.

We currently have 7 Special Interest Groups covering the following technical topics within the measurement and control fields: Cyber Security, Digital Transformation, Explosive Atmospheres, Flow Measurement, Functional Safety, Measurement and Standards. Driven by groups of volunteers who work, or have expertise, within the relevant topic area, SIGs promote the sharing and advancement of knowledge through a range of activities. These include producing white papers and briefing notes, as well as hosting and attending conferences, seminars and exhibitions.

How to Join

Members can join any SIG through the members only area of the InstMC website. Click 'MyInstMC' on the homepage and login to your account. Select 'Manage Personal Details' and under Special Interest Groups, click the 'Edit Special Interest Groups' button. Click 'Join' for any SIG you wish to become a member of.

If you are interested in finding out more about a particular Special Interest Group visit https://www.instmc.org/Special-Interest-Groups or email the relevant contact below.



Cyber Security Cevn Vibert
cevn@vibertsolutions.com

Digital Transformation
Maurice Wilkins
Maurice.Wilkins@instmc.org

Explosive Atmospheres
Harvey Dearden
Harvey.Dearden@instmc.org

Flow Measurement
Katrina Davidson
FlowMeasurementSIG@instmc.org

Functional Safety
Harvey Dearden
Harvey.Dearden@instmc.org

Measurement Andy Morris
measurementsig@instmc.org

Standards Maurice Wilkins
Maurice.Wilkins@instmc.org

LOCAL SECTION NEWS

LONDON

The London Local Section rounded off 2020 by successfully hosting a number of online technical presentations which were well attended by their local membership and guests.

Webinar: 'Taking Real Time Data Communication into Your Process - APL' presented by Pepperl+Fuchs 8th December 2020

The Industrial Internet of Things (IIOT) represents the possible future of industrial communication. Implementation, however, requires fast reliable communication from the field level to mobile, cloud-based applications. Field devices and sensors in process plants provide large amounts of data which is collected, processed and analyzed, however much of this valuable data remains unused. Ethernet-APL enables rapid and efficient communication of large data volumes at a rate of 10Mbit/s between field devices, process control systems and the cloud. The Ethernet has become the communication standard in factory and plant automation, in partnership with leading companies and associations. Foundations are being laid for future IOT applications in process industries through the Ethernet Advanced Physical Layer. Ethernet-APL fulfils all the central requirements for process plants such as two-wired systems with long cable lengths and interoperability, Ethernet technology can now be applicable in hazardous areas up to Zone 0/Class1, Div1. Four aspects are required to be precisely defined to create a completely open infrastructure which provides the interoperability that is expected from Ethernet: First IEEE 802.3cg defines data communication as 10BASE.T1L; Second, Ethernet -APL port profile specification defines power supply; Third, connections, cables and accessories such as surge protection: Fourth, the port profile will be published in an IEC Standard: Intrinsic Safety Explosion Protection. Ethernet-APL can be applied to any industrial Ethernet Protocol, such as EtherNet/IP, HART-IP, OPC UA and PROFINET making integration suitable for plant operations and allows plant asset management predictive maintenance, seamless transparent communication across all hierarchical levels.

Webinar: 'Cyber Security With a 20:20 Vision' presented by Emerson 10th November 2020

Cyber Security is the application of technologies', processes and controls to protect systems, networks, devices and data from cyber attacks. Process industry manufacturers and suppliers have accomplished incredible scientific and technological advancement in the products and services the industry provides. As the demands of industries have become more sophisticated so has the complexity of operations, making it necessary for control systems to be connected to business networks and therefore, indirectly to the internet, opening risks of cyber attacks. These require addressing and defending. An important factor in implementing a cyber security programme is to develop management systems to adopt a risk-based approach. Organisations regularly evaluate risk to their business and operations programs which affects strategic, compliance, operational, financial and reputational risks. A risk-based approach to cyber security is not to protect against all threats to your control system, but to identify potential vulnerabilities and make a strategic decision based on the likelihood and impact of each vulnerability. Emerson advised they support the adoption of IEC 62443 family of cyber security standards. The IEC 62443 standards define the requirements for how Distributed Control Systems should be developed, deployed and maintained to enhance the cyber security of the installed systems. In addition to the protection, which is integral with each system, end user's requirement to have an active role to ensure security 'best practices' are enforced in their control system. Cyber Security coverage starts with a complete assessment of the user's plant which determines key elements, company procedures and policies, back-up and recovery, incident response policy, tighten systems access, upgrades to more security, network segmentation, perimeter protection monitoring, remote access, management and network security monitoring. Almost all control systems are deployed with some type of remote connectivity and these must be kept safe and secure. Cyber attacks are the curse of the modern-day advanced industries and it becomes a major requirement to implement a comprehensive monitoring system to allow the capability to identify threats or issues at their earliest stages as well as leverage information for forensic purposes after an event.

Webinar: 'Rebellion Photonics – Intelligent Automation, Visual Monitoring Solutions' presented by Honeywell 13th October 2020

Honeywell's presentation demonstrated their intelligent automated visual monitoring solution which includes rapid verification of gas leaks and details the plume size and direction. Their system includes spectral imaging sensors together with analysing hyperspectral data to identify over 50 gas types. The systems camera captures gas leaks in the form of a visual cloud and the hyperspectral imaging technology captures both visible spectrum and infrared videos on the systems monitors. Honeywell advised their rebellion photonics software manages the analytics through its own user interface and displays real time video footage. The system provides monitoring indoors and outdoors 24/7 issuing gas leak alerts providing early warnings for the prevention of unnecessary safety issues.

Honeywell continued their presentation with 'Thermal Scanning for Fever Detection in access control systems', which is an innovated solution to effectively joining the fight against the threat of out of control viruses. The system assesses the core human body temperature using a combination of visual and infrared imaging technology and advanced algorithms to provide a non-invasive real time monitoring of people passing through an access point. This information is then analysed to reliably identify individuals who may exhibit a fever, alerting an operator to deploy a secondary evaluation method protecting occupants of the facility against infection. The system uses a thermal imaging camera measuring the individuals temperature pixel by pixel using temperature measurements algorithms to access core body temperature which is superimposed upon a visible image, fast and effective scans providing audible and visual alarms if any subject exhibits a temperature above the fever temperature threshold. In unprecedented coronavirus periods this system's wide range of applications can be used in transport, distribution centres, entertainment venues, manufacturing sites, educational establishments and many other venues in the fight against coronaviruses.

Barry O'Regan
Hon Secretary, London Section

IRELAND

New Ireland Local Section Formed

A new section has been formed to advance Measurement and Control in Ireland. Driven by the inaugural Chair of the Ireland section, Aidan O'Connell, the first section meeting was held virtually on the 22nd December 2020.

The desire to form a new section to serve members in Ireland originated from a number of InstMC members who wished to promote the aims and objectives of InstMC to the wider community, and to aid with the continuous development and sharing of knowledge to engineers, technicians, students, and laypersons.

Our first event, a presentation by Dr. Josh Reynolds entitled 'TeV Gamma Ray Astronomy - from Dustbins to Dark Matter' was held on Tuesday the 9th of February 2021. This was open to all members from every section.

New and existing members of the Institute of Measurement and Control are welcome to join the section by contacting us at ireland@instmc.org, or via our dedicated LinkedIn group, InstMC Ireland.

Frank Hallissey
Vice-Chair, Ireland Section

NORTH EAST

Test Equipment Donated to STEM Centre at Middlesbrough College

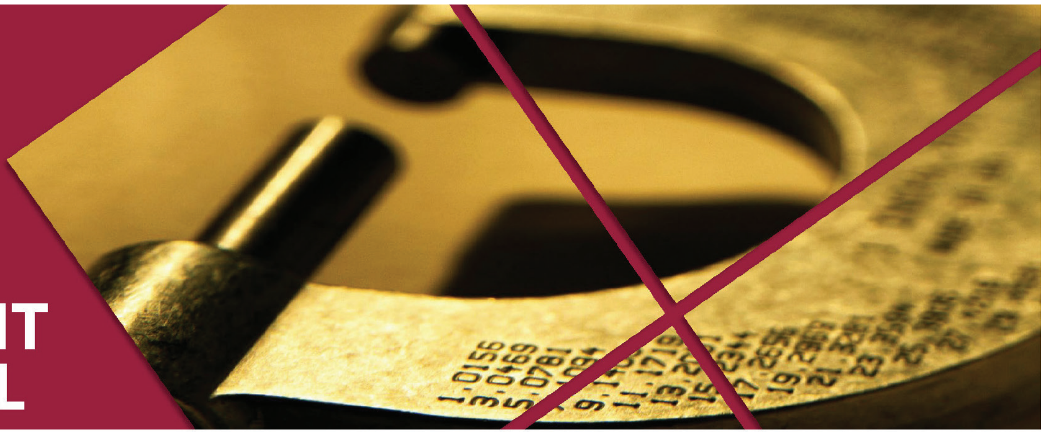
Omega Engineering Limited were recently seeking a good home for some surplus calibration equipment. Through their links with the InstMC North East Section Chairman, Richard Leng, a suitable home was soon found at Middlesbrough College.

With the help of Danny Curry, PSI and Damian Walker, Ashcroft UK (both members of the North East Local Section Committee), transportation was arranged and on 10th November Richard Leng and Damian handed the equipment over to the STEM centre at Middlesbrough College.

Many thanks to David Tipton, Vice President and Managing Director of Omega Engineering Ltd for kindly donating the equipment and to Damian Walker, InstMC North East, for providing the transport.

InstMC

THE INSTITUTE OF
MEASUREMENT
AND CONTROL



Professional Registration with the InstMC

WHY ?

Being professionally registered demonstrates to employers that you are committed to maintaining and enhancing the knowledge, skills and competence required to meet the engineering and technological needs and standards of today.
Your title will improve your CV and may lead to wider employment options, career progression and promotion.

HOW ?

To obtain professional registration individuals must be a member of a recognised Professional Engineering Institute such as the Institute of Measurement and Control.

Engineering Council

InstMC is licensed to award:

- Chartered Engineer (CEng)
- Incorporated Engineer (IEng)
- Engineering Technician (EngTech)

WHEN ?

Now! Whether you are looking to achieve the next level in your professional registration journey or are just starting out, the process is easy to complete online.

To find out more and start your application today, visit: https://www.instmc.org/Membership-Registration/Professional-Registration.

APPLY ONLINE

As an InstMC member apply through 'Engineering Council Registration' in the member's portal of the Institute's website. Complete the relevant form and supply the necessary supporting documentation. The membership team will assess your application then ask you to attend a professional review interview with our qualified assessors. If successful they will recommend to the InstMC Professional Registration Committee that you be added to the professional register.

Supporting Documents:

- A current CV
- An Organogram of your company
- Attested copies of your Degree/Diploma Certificates
- Attested copies of Academic Transcripts

WIRELESS GAS DETECTION AND MONITORING IN THE OIL, GAS AND OFFSHORE SECTORS

BY MEGAN HINE, DRÄGER MARINE & OFFSHORE,

Gas detection and monitoring has long-been a key consideration for businesses operating in the UK's oil, gas and offshore sectors.

Despite increasing attention by the Health and Safety Executive, which made reduction in the risk of offshore hydrocarbons a priority in its 2019/20 Business Plan, and by industry, there has arguably been relatively little innovation in the space. Until now, that is.

Wireless technology may have become ubiquitous in most people's lives for some time, but it's only relatively recently (the last six or so years) that it has become a viable option for gas detection and monitoring for the oil and gas sector. The reasons for this coming of age are, broadly, split into two key areas.

Firstly, industrial wireless technology has seen significant advances in recent years. Whilst the early adoption of wireless gas detection developed a poor reputation for patchy coverage and unreliable connections, data communications are now guaranteed; a crucial component for effective wireless monitoring systems which allows for detection of gas to be communicated reliably and in real-time using an ISA 100 industrial wireless system.

Secondly, there has been significant innovation in relation to device power consumption. Some of the advances in this area have been step-change reductions (in some cases by orders of magnitude), and this has been critical in offsetting more power-hungry functions which have otherwise advanced device functionality. The result is that battery life has improved considerably, with certain devices on the market guaranteeing up to two full years of battery life, compared to only a few months in the early days.

The cumulative impact of these and other minor innovations has been significant, and importantly, comes at a time when many legacy (wired) gas detection installations are now desperately in need of updating.

Two or three decades after the UK's first wired gas detection devices, both the technology and key drivers for monitoring have evolved. Environmental issues related to methane detection could soon rank alongside ongoing safety concerns around explosion risk etc, and standards around coverage and numbers of devices have also changed. Often, it is the inflexibility of hard-wired networks to respond to these sorts of changes, plus the vast costs involved in replacing cabling, that is now prompting operators to explore wireless alternatives. To prove the flexibility of wireless gas detection, it is now possible to rent a compliant fixed gas detection system for short-medium term coverage.

The ability to do away with the miles of cabling, which often has a life span of just 10-15 years, is a major advantage of wireless technology. Although the outlay for a wireless device may initially be higher, when the saving on cabling alone can be three times the cost of the wireless device, it's not a hard decision.

Flexibility is another key advantage – if for any reason a device is found to have been ineffectually-placed, or a new device is required, there is no need for new and potentially disruptive groundwork or cable re-routing.

One of the final – and perhaps most substantial – advantages of wireless technology is the fact that no site downtime is required. Wireless devices are intrinsically safe, so can be installed on live sites, offering a huge additional cost saving.

Challenges do remain; and arguably the key barrier to adoption is education and changing the poor perceptions around the technology, which still persist.

Despite these challenges however, the significant savings — reports of 60-80% overall savings are not uncommon — are contributing to an accelerating pace of adoption. As I write, the largest wireless gas detection network ever seen in the North Sea is being completed, and will employ 120 wireless devices across a remote seven square mile site. There is little doubt that this sort of project will become more commonplace as greater awareness develops and the full potential of the technology is realised.

STANDARDISATION OF GRAIN SIZE IN NEW ENGINEERING MATERIALS

BY KEN MINGARD, SENIOR RESEARCH SCIENTIST, NATIONAL PHYSICAL LABORATORY

The majority of engineering materials, whether metals or ceramics, are crystalline in structure and comprised of many grains of varying size and orientation.

The size of the grains is critical in influencing many materials' properties, whether structural or electromagnetic. For example, the yield strength of many metals follows a Hall-Petch type relationship, with strength proportional to the inverse square root of the mean grain size. The hardness and, in turn, the wear resistance of WC-Co cutting tools follows a similar relationship but often at the expense of toughness.

Grain size can be altered by changing production process conditions, so reproducible measurement of the grain size is important both for assessing process control and as a check that the final properties of (semi) finished components are likely to be to specification. Clearly grains are 3D in nature but the means of visualising and measuring the grain structure is almost always from polished 2D cross sections. These sections can reveal a wide range of sizes, seen in optical or scanning electron microscopes.

Well established standards exist (for example, ASTM E112 [1], ISO 13383-1 [2]) which define methods for calculating a mean size from measurements of the grain sections. These rely on identification of the boundaries between the grains, which is usually dependent on chemical etching attacking all the boundaries reasonably evenly and then on a manual operator judgement of what is a grain or grain boundary in the optical or electron images.

What is often not realised is that the mean grain size is actually the mean 3D size, related by stereology to the 2D average grain area or the average 1D intercept length of where a line crosses the grain boundaries. While this can be adapted for materials with non-equiaxed grain structures (e.g. elongated grains produced by extrusion or rolling) by measuring dimensions in orthogonal directions, in general a single mean value results which gives no indication of the distribution of sizes.

Electron backscatter diffraction (EBSD) is a rapidly growing technique which can eliminate the uncertainties of grain boundary etching and identification. Development of fast detectors in the past three years has meant that the grain structures over large areas of a polished section can be revealed and analysed in a similar time to that taken for etching, imaging and operator measurement of dimensions. EBSD is an electron microscopy technique which works by scanning the electron beam over a polished section in the same way that an image is acquired, but at each point a diffraction pattern is captured. If the possible phases present in the material are known, the orientation and phase at each point can be determined from the pattern and thus a digital map of orientation and phase can be produced. Grains can be defined as regions of similar orientation and thus sizes and phase information can be easily calculated with standard programs, giving details for every grain visible in the section. A typical example is shown in **Figure 1** of a recrystallised strain free Nickel superalloy.

The amount of information that can be obtained by EBSD extends well beyond grain dimensions. Micro texture can be measured to show if preferential orientations have developed (and hence potential anisotropy of properties) and local orientation changes in grains indicate if a material has been plastically deformed.

Although the EBSD method can be fully automated, this does not mean that accurate results will be obtained without care in sample preparation and use of the SEM and EBSD operating parameters appropriate to the material type and grain size. An international round robin [3] showed the errors that can result and has been used to inform one of the recent international standards [4] that covers the use of EBSD for grain size measurement. This standard covers the use of EBSD in reporting the full data distribution of sizes on materials processed by different routes measured in a cross section and how this may be related to the mean grain size. Another standard [5] focuses more on fully uniform strain free materials and how a mean grain size can be calculated using the same basic principles established in the standards for image based microscopy.

Underlying the previous discussions has been the general principle that uniform equiaxed grain structures are much easier to measure and compare through a mean grain size value. The increasing use of additively manufactured materials raises the issue of how to characterise and quantify the size of highly anisotropic grains with sizes ranging over two orders of magnitude.

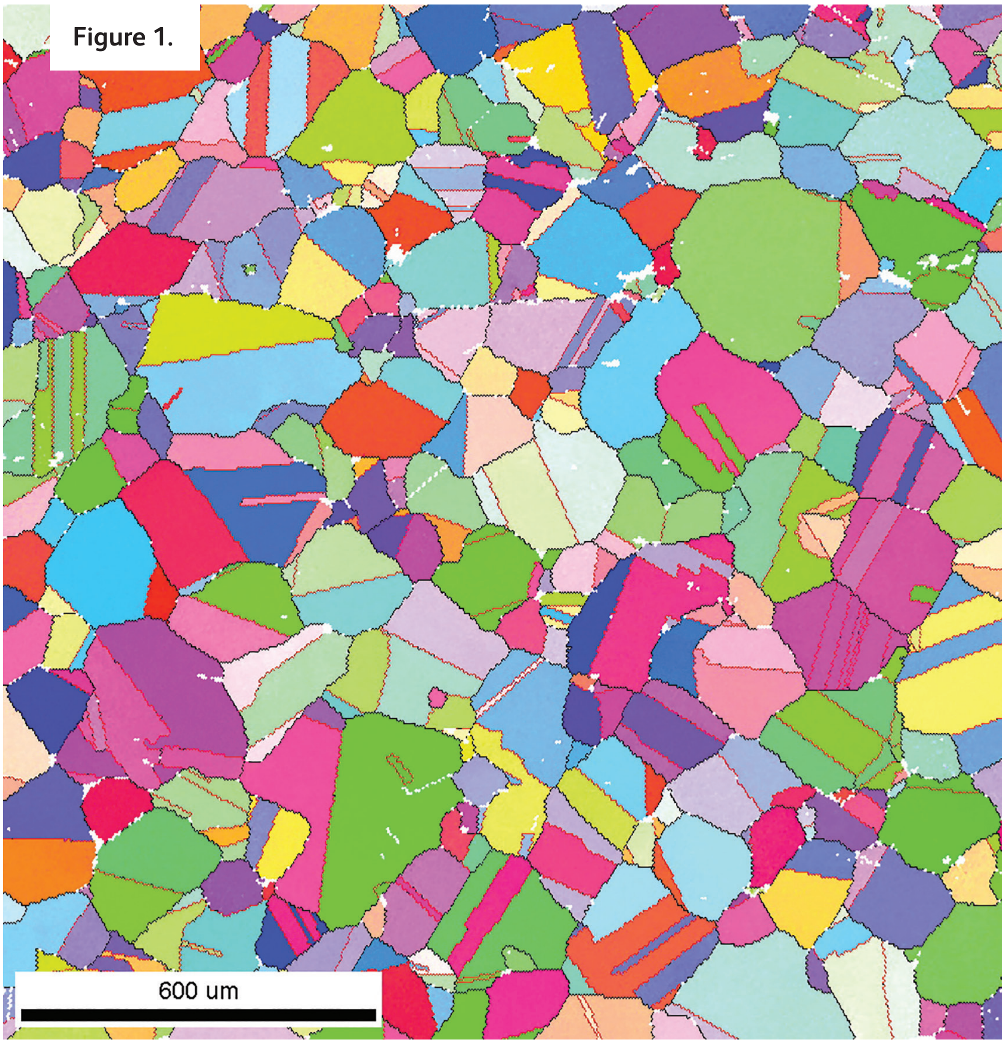
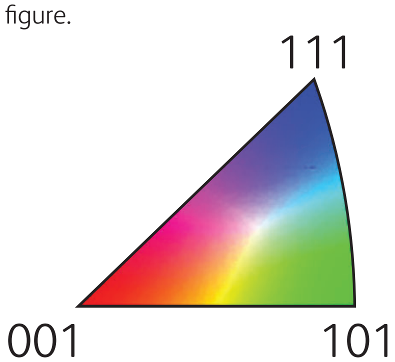


Figure 1. EBSD map to show the grain structure of a recrystallised Ni superalloy. Colours of grains show orientation given by the inverse pole figure.



Underlying the previous discussions has been the general principle that uniform equiaxed grain structures are much easier to measure and compare through a mean grain size value.

Figure 2.

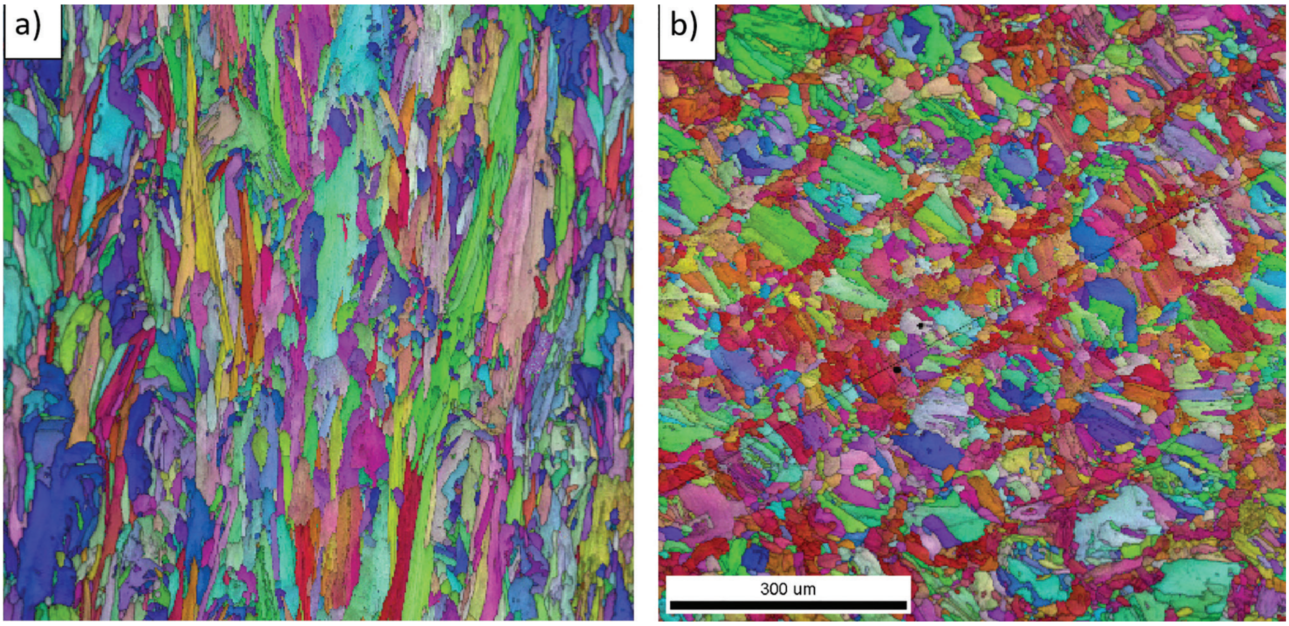


Figure 2. EBSD maps showing the grain structure of an additively manufactured Ni superalloy, a) parallel to the vertical direction of growth and b) perpendicular to the direction of growth.

Figure 2 shows an example of this in an additively manufactured Nickel superalloy. In the growth direction (Figure 2a) linear grain dimensions range from less than 10 µm to over 500 µm along the growth direction, and with dimensions orthogonal to this ranging from ≈10 to 50 µm have aspect ratios covering the entire range from 0.1 to 1. Perpendicular to the growth direction (Figure 2b) the grains are smaller with a maximum dimension of ≈ 100 µm, are more equiaxed and suggest a cellular like growth. Clearly, a single average grain size is insufficient to describe the structure. Measured dimensions can also be radically altered by the choice of definition of the minimum orientation change needed to define a grain boundary. In the example shown in Figure 1 the grains appear uniform in colour and boundaries are easy to define. In Figure 2a particularly, the grains show gradations in colours, indicating gradual changes in orientation and the definition of a grain boundary becomes more difficult.

Significant extra work is needed to determine how to define features that can be measured reproducibly on such additively manufactured microstructures, and establish which of these features are critical to determining the material properties. The wealth of information available from EBSD mapping will be essential to this process, but substantial effort will be required to define the international standards needed for reproducible microstructural characterisation.

1. ASTM E112, Standard Test Methods for Determining Average Grain Size
2. ISO 13383-1, Fine ceramics (advanced ceramics, advanced technical ceramics) — Microstructural characterization — Part 1: Determination of grain size and size distribution
3. Mingard K.P. Quested P.N. and Peck M.S., Determination of grain size by EBSD – Report on a round robin measurement of equiaxed Titanium, National Physical Laboratory, 2012, Report MAT56, ISSN 1754-2979
4. ISO 13067:2020, Microbeam analysis- Electron backscatter diffraction- Measurement of average grain size
5. ASTM E2627-13, Determining Average Grain Size Using (EBSD) in Fully Recrystallized Polycrystalline Materials

"Significant extra work is needed to determine how to define features that can be measured reproducibly on such additively manufactured microstructures, and establish which of these features are critical to determining the material properties."

COMPANION COMPANY SCHEME (CCS) SHOWCASE

The InstMC Companion Company Scheme has been running since 1992, enabling companies to raise their profile amongst our membership of 3,000 professional engineers in the measurement, automation and control sectors.

There are opportunities to network with other businesses, InstMC accredited universities and with individual members, at local and regional level, through Local Sections and Special Interest Groups. We currently have 75 CCS members and are pleased to introduce some of them to you here.

DPS Group

DPS Group is one of the UK's only integrated Electrical, Instrumental & Control and Compliance providers. We solve complicated manufacturing challenges for some of the world's best-known brands, through the intelligent use of technology.

Our team is trusted to work across multiple sectors including Food & Beverage, Water, Bio-energy, Pharma, Paper, Power, Oil & Gas and Petrochemical. We create valuable, long-term partnerships, by finding solutions that enable increased efficiency and productivity, all whilst meeting the highest safety standards.

And in everything we do, we seek to minimise our environmental impact by complying fully with the requirements of the highly regulated industries we operate in, conducting our business professionally and ethically.

Tel: +44 (0) 1592 772577
Website: www.dp-sgroup.co.uk

KROHNE

KROHNE is a leading manufacturer of products, services and solutions for the process industry covering flow, level, pressure, temperature and analytics. Our products are used in oil & gas, chemical & petrochemical, pharmaceutical, food & beverage, water & wastewater, power, mining & minerals, marine and many other markets.

Founded in 1921, KROHNE has steadily grown into a global enterprise and today employs more than 4,000 people with total sales in excess of €600 million. Headquartered in Duisburg, Germany, we operate 16 production facilities in 12 countries supplying 44 KROHNE-owned companies and joint ventures and 55 exclusive representatives.

KROHNE Ltd is the group's global Centre of Excellence for Coriolis mass flowmeter technology. Its manufacturing plant in Wellingborough, United Kingdom, is home to the award winning OPTIMASS range of Coriolis mass flowmeters. We also provides a full range of engineering and sales services for the complete KROHNE product range.

Tel: +44 (0) 1933 408 500
Website: www.krohne.com

Sella Controls Ltd

As an independent systems integrator, SELLA CONTROLS have developed a strong reputation of proven innovative system design expertise and engineering specialist for the supply of Safety Instrumented Systems and Control Systems across various industry sectors. Through our partnerships with key product partners and our unrivalled in-house engineering capabilities, the company offers the complete best in class project capability. Utilising the latest programmable, hard-wired safety-critical integrated control and automation technologies, in the Oil & Gas, Nuclear, Renewable Energy and Process industries, providing the following systems and services: System integration; Concept design development; Integrated safety and control systems; HIPPS, ESD, F&G, BMS, SIS, IPS; Product development; IEC62443 Cyber security assessment & protection; Safety assurance; Cyber and Safety Training; Lifecycle technical support; CASS certified procedures.

Our history and pedigree make Sella Controls the logical choice for all your Control & Safety System needs.

Tel: +44 (0)161 429 4500
Website: www.sellacontrols.com

Silchester Control Systems

Silchester Control Systems Ltd (SCS), based for over 30 years near Alton in Hampshire, UK, works nationally and internationally to support a wide range of industrial clients. SCS is a specialist systems integrator in consultancy, design, procurement, installation and commissioning for both new and upgraded industrial electrical and process control systems. We have developed a long-term reputation in industry for quality, reliability and dependability.

SCS works also in maintenance support, in training and bespoke operations, in electrical and control system project management and for the development of maintenance manuals. Support for industrial IT systems and network design and installation for many process industries also requires expertise in the visualisation and data collection for MES systems and in pharmaceutical validation to the latest GAMP standards.

Tel: +44 (0) 1420 561 902
Website: www.silchester.co.uk

ARE ALARMS CREDITWORTHY?

BY NICK OLIVER
CENG MINSTMC

When we think of safety systems, alarms are often taken for granted as being readily available, but are they?

Layer of Protection Analysis (LOPA) is a methodology used in the process industries for simplified, rule-based risk analysis. In this type of analysis, there is a natural design to credit every mitigation layer possible. This is not limited to just the capital cost, but includes the lifetime ownership costs of proof testing and FSA stage 4 assessments. LOPA teams are frequently asked to take credit for alarms, often without analysis, or even to strike out a loop if not SIF is required, so as to reduce the safety integrity level (SIL) category. Project managers often see alarms as a lower cost means of implementing safety compared to other inherently safer methods.

When I, as a LOPA Chair, am asked to take credit for an alarm in a LOPA, I like to give the following nine tests;

1. There has to be a clear separation of the function of the alarm from the SIF and the initiating cause.
2. There has to be sufficient time from the annunciation of the alarm for the operator to avert the operation of the SIF.
3. There has to be a clear response to take upon the alarm.
4. The alarm set point must be at a level where it will be activated before it is swamped in an alarm flood. It must also not activate routinely. This can be a tricky balance.
5. It should always be prioritised in the highest level for the plant Distributed Control System.
6. There has to be clear relationship from the alarm to the SIF.
7. The alarms system should be in a good state of performance.
8. The operator should be well trained and aware of the actions they should take.
9. The alarm should be periodically tested.

During the LOPA some of the criteria above can be confirmed or the existing site policies may demonstrate compliance although this should not be taken for granted. If these are not known actions, they can be raised against the LOPA for closure later.

Questions such as whether the alarm is generated within the Basic Process Control System (BPCS) rather than the Emergency Shutdown System (ESD) can be asked. If, however, failure of the BPCS is the initiating cause of the event then no credit can be taken if the BPCS also delivers the alarm. Additionally, where the operator responding to the alarm is a human factor initiating cause of the incident, then it is questionable whether an alarm should be credited. My view is that, unless the time to consequence for the alarm is sufficiently long to cross a shift hand over and thus alert another operator evidence of good shift handover would also have to be demonstrated. There is very little excuse for not resolving basic questions such as

Activities like calculating time to event, operator response time and assessing if there is a clear action the operator can take to avert the operation of the SIF can be very time consuming and are normally recorded as actions to be done outside of the LOPA. A good LOPA chair, however, should be able to weed out the more fatuous calls to add an independent protective layer (IPL) where the event will clearly come very shortly after a loss of control or another initiating condition.

The operator response should be clear, unambiguous and detailed enough to be followed under stress conditions. It should be included as part of a wider plant alarm response manual (ARM). This ARM in more modern HMI systems can be imbedded in the alarm banner as background text available from a mouse click or hover. In older systems where this is not possible the HSE have in my experience accepted an Excel based lookup tool on a screen next to the control system.

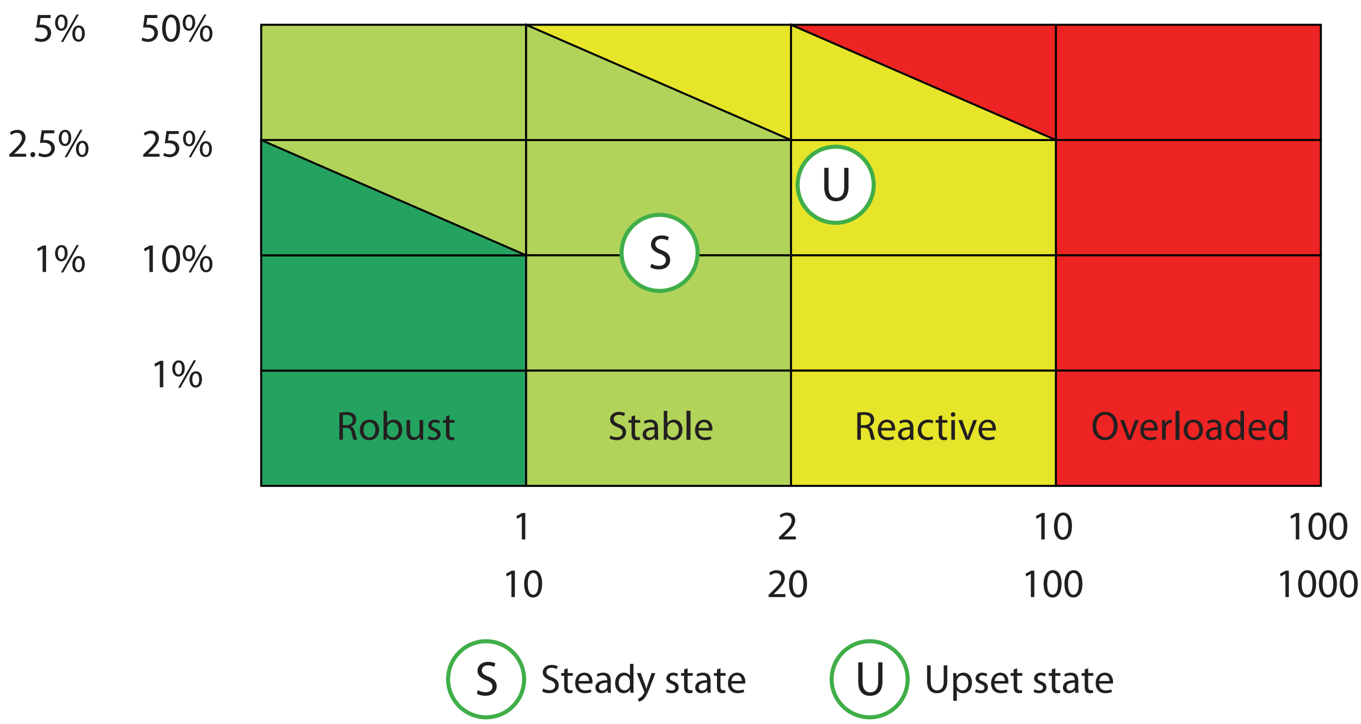
If an ARM is confirmed to be available on the site, then the LOPA Chair should determine if the action is simple to take and unambiguous. Where there are multiple initiating causes, each with separate actions, it is difficult to say the operator would respond correctly or if the action has its own risks, for example blowing down a high pressure gas plant. In these cases, a LOPA Chair should weed out the less credible requests for an IPL based on this criterion.

The alarm set point should give the operator sufficient time to respond before the SIF is demanded. If the operator has to take steps to reduce pressure or temperature build up in a vessel then this may take many minutes or possibly hours before their corrective action takes effect. The time necessary to determine a root cause and possibly the time to walk to the plant or call another operator to do so should also be included.

The set point should not be at a level where it is used as a prompt to take action. If this is a requirement, then an alert or similar should be configured to activate first. The alarm's occurrence should be outside of the norm, and any activation of a highly managed alarm (HMA) should be noted and logged even if steady state is resumed following its activation. There should also be an assessment if its activation would be during "under stress" conditions for the control room operator. The review of all of these criteria should be included in the LOPA, or latest in FSA stage 2. However, in some circumstances only time would tell where alarms are used as a credit in the LOPA, an early stage 4 FSA would be advisable.

> The operator response should be clear, unambiguous and detailed enough to be followed under stress conditions.

Figure 1. Alarm System Performance Graph



Prioritisation of an HMA at the highest level would be normally set out in the ARM. The requirements for written policies and procedures are laid out in EEMUA 191 rev 3, and these policies should describe a method of indicating HMAs as being distinct from other alarms. Ensuring that the alarm system performance is maintained by allowing HMAs to be actioned by the control room operator in a timely manner without them being swamped by alarms of less priority is a challenge for any process environment.

EEMUA 191 rev 3 describes performance zones as robust, stable, reactive and overload. These are plotted on a graph with axis scaled in % of time and alarms per minute. There are two sets of scales to represent both the steady state environment and the upset environment. This allows the loading on the operator during alarm flood as well as over the entire shift to be assessed. The number of alarms assessed over these time frames should be all the alarms the operator has to respond to. Therefore if the operator has a process control system, a separate ESD system and a fire and gas monitoring system along with standalone package PCs to monitor, all the accumulated alarms must be included to assess loading. If these are brought together on a dedicated alarms terminal this may also be able produce the KPI charts expected in EEMUA 191 rev 3.

There are many other KPI criteria for alarms such as distribution of priority and % of time in flood. However, for the purpose of taking credit for alarms in a LOPA, if we concentrate on the alarm system performance graph (Figure 1), it sets a clear bar of acceptability. Can the plant in question maintain its alarm KPI performance in the robust or stable region, both for steady state conditions and upset conditions. Guidance for this can be found in EEMUA191 rev 3 section 6.5.2.

The LOPA Chair should ask if the plant can show a constant history of keeping to this KPI. A minimum of six months in robust or stable would be a reasonable expectation. They should also ask what policy the company has to assess SIF validity if the system falls out of this performance.

Criteria 8 and 9 look at the operations and maintenance phase of the alarm system, comparable to the safety lifecycle. Before taking credit for the alarm in the LOPA it should be confirmed that the company has appropriate policies and procedures for operator training and maintenance of all alarms not just the HMA alarms. If the alarms system performance is impaired due to lack of maintenance then it affects the ability of the operator to respond to the HMA regardless if this is maintained in isolation. EEMUA191 rev 3 states all alarms should be tested routinely.

The nine criteria set a high bar before alarms can be credited in a LOPA, indeed if the site does not presently take credit for alarms then extreme caution should be used before doing so. To bring a site up to an acceptable standard of alarms systems performance is costly, and to maintain it is onerous, though it is probably necessary for reasons other than crediting alarms in a LOPA, as the HSE has stepped up its scrutiny of alarm handling in recent years.

It has to be said that nothing comes for free, so a convenient 1 order of magnitude credit in the LOPA for an alarm may come at a high price to maintain and improve the standards of a site wide alarms system. In the long term, passive means of mitigating the risks such as pressure safety valves or bunds may prove cheaper than using alarms, and removing people from exposure by automating a plant is often the cheapest and most effective mitigation measure.

"If the alarms system performance is impaired due to lack of maintenance then it affects the ability of the operator to respond to the HMA regardless if this is maintained in isolation."

SPOTLIGHT ON STAFF:

Q&A with InstMC Staff Member Caroline Trabasas, Membership & Administration Officer

How long have you been with InstMC?

I joined in September 2020 so six months, and the newest member of the team.

What is your background?

I read Philosophy and Politics at Newcastle University. Since graduating, I have worked in both fundraising regulation and property law regulation. I have also worked for various charities from those that serve on the frontline to those involved in influencing policy. I have a keen interest in governance and have had experience at board and committee level.

> "I have a keen interest in governance and have had experience at board and committee level."

What is your role at InstMC?

My role is varied between membership, accreditation, professional registration and providing administrative support within those domains.

Can you describe a typical day in the office?

There is no typical day however, it can range from dealing with standard membership enquiries, reviewing, crosschecking and processing membership applications. Updating our database, revising policies and procedures to reflect new standards, organising academic accreditation visits, coordinating the running of CPD renewal, liaising with the Accreditation Committee, issuing committee papers and writing minutes.

What do you bring to the team?

I am quite methodical and process driven, and I enjoy overseeing end-to-end processes. As I have only been with the Institute for a short while, I hope to be involved in projects that look at our processes – I believe there's always room for improvement.

What do you like best about working for the InstMC?

Well… I have joined the InstMC virtually, so I have not yet met any of my colleagues in person! Despite the pandemic keeping us apart, the team have made me feel very welcome and have been super helpful in inducting me online. I wait in anticipation of when we can all be together and hopefully will also be able to enjoy and devour the "office cakes" that they are all so fond of.

What do you do to unwind, once your working day is over?

Once my working day is over, I usually have to begin other work. I dedicate a lot of time to my voluntary engagements as a trustee of a small charity and a governor for a federation of schools in East London. But when I do get the chance to relax, I like to keep active by taking part in zumba and boxing, both of which I do in my local community.

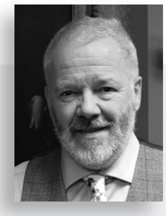
Can you tell us a fun fact about yourself?

I went to a performing arts school and performed on the opening night of the Millennium Dome. I also reviewed children's films on the Richard and Judy show and I used to play in a steel band!

OUR CORE TEAM

OFFICERS

President
Martin Belshaw



Honorary Secretary
Billy Milligan

Honorary Treasurer
Ian Craig

Engineering Director
Dr Maurice Wilkins

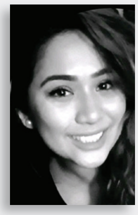
Chief Executive
Steff Smith
+44 (0)20 7387 4949
steff.smith@instmc.org

Business Executive
Sydney Reed
+44 (0)20 7387 4949
sydney.reed@instmc.org

Marketing Executive
Ernest Kyei
+44 (0)20 7387 4949 Ext 4
ernest.kyei@instmc.org

Director of Membership & Registration
Leila Atherton
+44 (0)20 7387 4949 Ext 3
membership@instmc.org

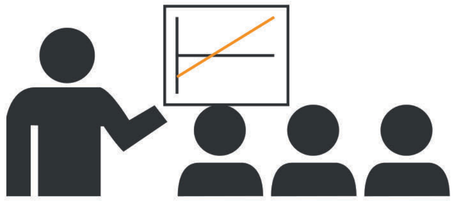
Membership & Administration Officer
Caroline Trabasas
+44 (0) 20 7387 4949
caroline.trabasas@instmc.org



Marketing & Events Officer
Jane Seery
+44 (0) 20 7387 4949
jane.seery@instmc.org

Live Online

Classroom



TUV Certified 61511 Functional Safety Training

Method Functional Safety delivers TUV SUD Certified Functional Safety Training as both Classroom and Live Online formats

For more information go to www.methodfs.com/61511

Contact us on:

w: www.methodfs.com
e: support@methodfs.com
p: +44 (0)1462 713313

=Method
Functional Safety