

hazardex

EXHIBITION & CONFERENCE

2018

Runcorn, UK 28th Feb - 1st March

hazardexonthenet.net

EVENT GUIDE

Protecting Plant, Process and Personnel

Event sponsor



Awards sponsors



In association with



www.hazardexonthenet.net



Welcome to the Hazardex 2018 Conference & Exhibition

**Holiday Inn Hotel, Runcorn, Cheshire, UK
February 28 – March 1**

Following the success of the 2017 edition, in Runcorn for the fourth time, the 2018 Conference will be a unique event capturing and distilling decades of process safety experience from across Europe in two thought-provoking days of practical knowledge exchange.

The Conference brings together leaders and experts from around the world with one goal in mind: creating safer workplaces. Content is focused on the issues that affect your industry and delivered in high-energy sessions by leaders who have been there. Whether you're a senior executive, plant engineer, site-level safety manager or supervisor, the sessions offer you the tools you need to make work and industry safer.

The varied programme will give the latest insights from regulators, certification bodies, end-users, manufacturers, consultants, scientists, engineers and safety specialists involved in hazardous area operations, with a particular focus this year on cybersecurity.

The associated Exhibition features many of the most prominent companies that supply products and services to the sector, and delegates will have many opportunities between conference sessions to browse displays and engage with some of the top experts from companies whose efforts ensure process and occupational safety continues to improve across the industry.

Guests will also enjoy a drinks reception, fine dining and after-dinner entertainment, and the 2018 Hazardex 2018 Awards ceremony recognising safe practice in hazardous area operations. Most of all, the Conference & Exhibition will provide a valuable networking opportunity with top experts and industry peers from across the UK, Europe and across the world.

We would like to express our gratitude to event sponsor CSA Group, and to Awards Ceremony sponsors RS Components and C&P Engineering, and hope you have a fulfilling and useful event.

The Hazardex team

Opening and closing times

Wednesday February 28

Conference registration opens	8.00
Exhibition opens	9.00
Conference opens	9.20
Lunch	13.00
Conference closes	16.15
Exhibition closes	17.30
Drinks reception & dinner	18.30 till late

Thursday March 1

Conference registration opens	8.30
Exhibition opens	9.00
Lunch	13.00
Conference closes	15.35
Exhibition closes	15.35

Contents

In the supplement:

Conference timetable	S4 - S5
Conference presentations	S6 - S9
Hazardex 2018 floorplan	S11
Exhibitor profiles	S13 - S57

Event sponsored by:





HAZARDEX 2018 – PROTECTING PLANT, PROCESS & PERSONNEL

Running order subject to change.
Check www.hazardexonthenet.net for the latest updates

HAZARDEX CONFERENCE 2018 – DAY 1

8.00 – 9.20: Registration & coffee

Day 1 Morning - Stream 1 - Cybersecurity, IIoT & Industry 4.0

Main conference room (Access for delegates & exhibitors only)

Chairman: Lee Allford, Energy Institute

9.20 – 9.30: Chairman's introduction

9.30 – 10.10: **Sarabjit Purewal - Acting Head of Operations, HSE, & Tony B - ICS Tech Lead, NCSC**

Cybersecurity: Is the UK prepared to address the risks?

10.15 – 10.55: **Ian Curtis - Process Safety Systems Consultant, Siemens**

Digitalisation changes everything

10.55 – 11.30: Coffee & exhibition viewing

11.30 – 12.10: **Dr Alexander Horch - Head of Development, HIMA**

Safety & Security: The last line of defence is restored

12.15 – 12.55: **Thomas P. Ventulett - CEO, & Leigh Villegas - Marketing Director, Aegex Technologies**

Toward an IoT platform for hazardous locations

13.00 – 14.00: Lunch

Day 1 Afternoon - Stream 1 – Incident & Risk Management

Main conference room (Access for delegates & exhibitors only)

Chairman: Lee Allford, Energy Institute

14.00 – 14.40: **Zsuzsanna Gyenes – Deputy Director, IChemE Safety Centre (ISC).**

Lessons learned from major accidents in different industrial sectors

14.45 – 15.25: **Roger Stokes - Principal Engineer, BakerRisk**

When the lights go out

15.30 - 16.10: **Carolyn Nicholls - Consultant, RAS Ltd**

Risk tolerability targets; misconceived, misunderstood and misapplied

Day 1 Morning/Afternoon - Stream 2 – Safety Culture

Seminar room (Access open to all registered attendees)

Chairman: Ron Sinclair, Technical Manager, SGS Baseefa

11.30 – 12.10 **Dr Kevin Fitzgerald – Risk Management Dept. Manager, Lloyd's Register Energy**

Safety culture, climate and performance improvement

12.15 – 12.55: **Jamie Walker - Safety & Projects Director, UKPIA**

Mental health awareness in a safety critical environment

13.00 - 14.00: Lunch

Day 1 Afternoon - Stream 2 – IIoT & Industry 4.0

Seminar room (Access open to all registered attendees)

Chairman: Ron Sinclair, Technical Manager, SGS Baseefa

14.00 – 14.40: **Matt Jakuc - Cybersecurity Technical Lead, CSA Group**

The role of third-party testing in securing Industrial Internet of Things (IIoT) compliance

14.45 – 15.25: **Gido Van Tienhoven - CEO, Ex-Machinery**

IoT 4.0 and LoRa for maintenance purposes in hazardous areas

15.30 – 16.10: **Stefan Hack, Business Development Manager, R.STAHL**

Paperless safety lifecycle at the R.STAHL plant & engineering center

17.30: Exhibition closes

18.30: Dinner drinks reception

19.30: Evening event & awards dinner

22.30: After dinner networking



HAZARDEX 2018 – PROTECTING PLANT, PROCESS & PERSONNEL

Running order subject to change.
Check www.hazardexonthenet.net for the latest updates

HAZARDEX CONFERENCE 2017 - DAY 2

8.30 – 9.20: Registration & coffee

Day 2 Morning – Stream 1 – Functional Safety & Cybersecurity

Main conference room (Access for delegates & exhibitors only)

Chairman: Lee Allford, Energy Institute

9.20 – 9.30: Chairman's introduction

9.30 – 10.10: **Nic Butcher - ECI Specialist Inspector, HSE**

Functional safety management of installed SIS

10.15 – 10.55: **Tino Vande Capelle - Consultant, TVC, & Steve Smith - Consultant, ONRIX gcv**

No safety without security – No security without safety

10.55-11.30: Coffee & exhibition viewing

Day 2 Morning/Afternoon – Stream 1 – Certification & Regulation

Main conference room (Access for delegates & exhibitors only)

Chairman: Lee Allford, Energy Institute

11.30 – 12.10: **Hassan El Sayed - Functional Safety Business Manager, CSA Group**

Certification of robotics in an Ex environment - ATEX and functional safety requirements

12.15 - 12.55: **Ian Crellin - Marketing Manager, British Safety Industry Federation (BSIF)**

Recent changes in regulations governing PPE

13.00 - 14.00: Lunch

Day 2 Afternoon - Stream 1 – Practical challenges & solutions

Main conference room (Access for delegates & exhibitors only)

Chairman: Lee Allford, Energy Institute

14.00 – 14.40: **Frank Ward – Director & Project Engineer, Hennock International**

Addressing the challenges of dust explosion risks in grain storage

14.45 – 15.25: **Tim Jones - Senior Consultant, MMI Engineering**

Fire detector mapping – what metrics should we be using?.

15.25 - 15.35: Chairman's closing remarks

15.35: Conference & exhibition closes

Day 2 Morning - Stream 2 - Functional Safety & Safety Systems

Seminar room (Access open to all registered attendees)

Chairman: Ron Sinclair, Technical Manager, SGS Baseefa

9.30 – 10.10: **Chris Parr - Technical Authority for Functional Safety, Sella Controls**

Cybersecurity - What should Safety Instrumented System integrators be doing?

10.15 – 10.55: **Rob Turner - Advanced Solutions Consultant, Yokogawa**

When safety meets security - Combining the best of both worlds

10.55-11.30: Coffee & exhibition viewing

Day 2 Morning/Afternoon - Stream 2 – Practical challenges & solutions

Seminar room (Access open to all registered attendees)

Seminar room (Access open to all registered attendees)

Chairman: Ron Sinclair, Technical Manager, SGS Baseefa

11.30 – 12.10: **Tarmo Rintala - Technology Manager, Atexor Oy**

Are luminaires causing hidden risks in Ex Areas because of LEDs?

12.15 – 12.55: **Geof Mood - Technical Director, CCG Cable Terminations Ltd**

Coldflow in cables – some practical advice

13.00 - 14.00: Lunch

Day 2 Afternoon - Stream 2 – Practical challenges & solutions

Seminar room (Access open to all registered attendees)

Chairman: Ron Sinclair, Technical Manager, SGS Baseefa

14.00 – 14.40: **Mike O'Brien: Managing Director, Newson Gale.**

How to prevent the electrostatic charging of processing equipment in ATEX atmospheres

14.45 – 15.25: **Sarra Cheyne – British Standards Institution (BSI)**

How to improve performance, reduce risk and achieve sustainable growth in areas with explosive atmospheres

15.25 - 15.35: Chairman's closing remarks

15.35: Conference & Exhibition closes

DAY ONE – 28/2/2018

1. Cybersecurity: Is the UK prepared to address the risks?

Presenters: Sarabjit Purewal - Acting Head of Operations, Health and Safety Executive (HSE), & Tony B - ICS Tech Lead, National Cyber Security Centre (NCSC)

The keynote will cover the work that central Government is doing, including setting up to the National Cybersecurity Centre, its remit, what the landscape looks like and what we know about the energy and chemical industries sectors.

The new Network Information Security (NIS) directive will be transposed into UK law in late 2018, which will bring obligations for industries to manage risks to critical services and consequent penalties for non-compliance or loss of service. Although regulatory decisions will lie solely with the Competent Authorities, NCSC plays a leading role in advising industry and will share their approach to providing supporting guidance to the implementation of NIS.

HSE will share the outcomes from the field trials on the application of its operational guide, development of case studies, the strategic approach for regulating cybersecurity from 2018 onwards and the role industry can/is playing in addressing this topic.

The challenges, and risks looking ahead to the UK energy and chemical industries sector will be explored and what government is doing to assist.

2. Digitalisation changes everything

Presenter: Ian Curtis - Process Safety Systems Consultant, Siemens

A bold statement ... but you don't have to look too far to find examples of where digitalisation has proven to be disruptive.

Now digitalisation is being described as bringing about the next big industrial revolution (or Industry 4.0 as it is sometimes called) promising a quantum leap in terms of benefits to productivity, flexibility, quality... but what of safety? Surely digitalisation offers the scope for improvement in process safety?

The "digitalisation" topic is still somewhat fluid and fast moving and exactly what form it takes differs from one industry to another. Discrete manufacturing topics include collaboration between cyber physical systems; using the internet of things and the internet of services; digitalisation of the whole value chain to achieve increased flexibility and productivity.

For the process industries the emphasis is slightly different so digitalisation for process involves the integrated engineering and integrated operation of process plants across the whole plant life-cycle but also incorporates topics such as digital twins and Big Data.

Integrated engineering and operation offer scope for improving safety by reducing the scope for systematic errors throughout the lifecycle. The concept of the digital twin can significantly improve verification and validation along with training for operation and maintenance. A "digital twin" can be used to thoroughly test the automation layer including the SIS. Simulation is nothing new but the ability to auto-generate the simulation from a common data model helps avoid mistakes. Verification testing of the "digital twin" uses the same code as will eventually be running in the SIS. Of course the validation of the safety system will still need to be done "in the real world" when the SIS is hooked up to the physical equipment but effective verification and validation during pre-FAT can help reduce the time taken at FAT and SAT.

Increased digitalisation also facilitates ease of data collection and improves the ability to consolidate data across disparate systems into the Cloud to help avoid silos of data. Big Data has the potential to contribute to process safety in a number of areas:-

- Plant reliability and Asset Integrity
- Steady State Process Control
- Process Optimisation
- Accident Investigation
- Collating leading indicators for process safety
- Use of data from maintenance systems and incidents to promote process safety.

This paper seeks to give an overview of digitalisation in a process industry context focussing on the potential benefits for safety.

3. Safety & Security: The last line of defence is restored

Presenter: Dr Alexander Horch - Head of Research, Development and Product Management at HIMA

The advancing digitalization has an effect on almost all business processes, especially in the industrial sector. Machines communicate with people and increasingly also amongst themselves. What does this mean for security? Safety controllers have historically focused primarily on emergency shutdown requirements, not from the cyber-security perspective.

For effective Cyber-Security, it is not enough to upgrade an existing product by adding additional software functionality. Every solution for functional safety must be conceived and developed with cyber security in mind, right from the start. This applies equally to the firmware and the application software. Safety systems, which offer the fewest attack possibilities, represent the most effective defense against cyber attacks. Reduced controls on necessary security functions are protected against typical attacks on IT systems.

Safety-oriented systems are the last line of defence in a production facility. The implementation of effective cyber-security measures is particularly important. A crucial point is the minimization of human intervention, since humans are the most frequent cause of cyber risks. These include both targeted cyber attacks to disrupt production processes or steal industrial secrets, as well as incidents caused by carelessness. An effective protection concept includes, for example, special access protection, physical security or plausibility checks on changes. In addition, users need to take organizational measures, such as periodic testing of

internal networks through penetration tests or security training of their own employees. Because, when employee passwords become known, a hacker attack becomes child's play.

In addition, the intelligent use of existing data from the security network, for example for predictive maintenance or process optimization, now also allows operators to improve the efficiency of their systems by reducing downtime. The safety system is particularly suitable as a source of relevant information since a large amount of data is generated in safety control systems.

4. Toward an IoT Platform for Hazardous Locations: Examining the collaboration of humans and edge technologies in disaster scenarios for insight into Industrial IoT for extreme operations

Presenters: Thomas P. Ventulett - CEO, & Leigh M. Villegas - Marketing Director, Aegex Technologies

As more and more industrial organizations are adopting Internet of Things (IoT) strategies and beginning their digital transformation to Industry 4.0 or Smart Manufacturing, they face challenges in adopting technologies due to regulatory restrictions for highly combustible atmospheres such as exist in some of the world's largest and most critical industries - oil & gas, chemical, pharmaceutical, energy, utilities, food processing, defence and others. In ATEX/IECEx Zone 1 or UL Class I Division 1 hazardous areas worldwide, up to 15% of personnel do not have access to mobile devices unless they are certified "intrinsically safe," or incapable of causing a spark that could ignite a combustible environment. Thus, the human "sensor" in hazardous area operations, who could conceivably detect perceived anomalies or problems in the maintenance, workflow, process or function of these operations, is relegated to recording observations with pencil and paper and then entering data manually into ERP systems hours or days later. Such lack of real-time communication and data management results in inefficiency, increased costs and elevated safety and asset risk, causing potential down-time and even loss of life in extreme cases.

By deploying new IoT technologies that allow people to use technology inside Zone 1/Division 1 hazardous areas, humans can actively interact with machines in real time to dramatically improve productivity, safety and the bottom line in hazardous operations. A new style of IoT platform built especially for hazardous area operations, would need to include various and affordable types of sensors to cover vast spaces, real-time communications, cloud computing, machine learning, rights management, security, big data storage, analytics and user-friendly visualization, all functioning in highly explosive conditions.

This paper considers the possibilities for an IoT Platform for Hazardous Locations, based on hands-on research conducted by Aegex Technologies, Verizon, Nokia and multiple technology partners that tested various edge technologies with first responders in realistic disaster scenarios during Operation Convergent Response (#OCR2017). The event provided a unique opportunity to test IoT under extreme conditions, such as a staged chemical plant explosion, subway terrorism incident, neighborhood flood, cybersecurity attack, tornado disaster and hostage rescue. The results gave insight into the need for continued collaboration on IoT capabilities that can better manage not only emergency response, but everyday operations in hazardous industries.

5. Lessons learned from major accidents in different industrial sectors

Presenter: Zsuzsanna Gyenes - Deputy Director, IChemE Safety Centre (ISC)

Petrochemical and chemical industries store and process a large amount of dangerous substances in complex chemical establishments. For this reason, persistent care to controlling the processes and their related equipment is necessary at these sites to avoid a loss of containment that could lead to a serious accident. In reality, hundreds of chemical accidents are reported in the media around the world in average a year. Many of them have severe consequences, such as production disruption resulting in significant economic loss, temporary loss of public services, property damage, environmental damage and in the worst circumstances, injury and death. In many cases, lack of knowledge or procedures in place or lack of competence, even complacency led to the incident.

The paper studies accidents chosen from different industrial sectors and different topics, such as, incidents involving fertilizers, contract worker related cases, ageing of establishments or emergency response. These cases seem diverse but in reality, the lessons depicted show similarity and these findings demonstrate that learning from other industries or topics is indeed possible. Furthermore, the study highlights events where the lessons were not learnt even though similar cases had occurred already in the past.

The analysis of the cases selected covers lessons learned from the accidents and forms a summary on how to make industries to pay more attention to factors they had not considered as a potential element to contribute to a major event. Furthermore, how they can improve knowledge with looking at past accidents and learning from cases occurred in other industrial sectors. Finally, the study emphasises the importance of an effective safety management system in place regardless the type of industrial activity.

6. When the lights go out

Presenter: Roger Stokes - Principal Engineer, BakerRisk

Processing facilities require a reliable supply of electrical power. The consequences of a sudden power loss ranges from an inconvenience to a major incident with consequences including damage to equipment, failure of emergency systems, loss of containment, fires, explosions and environmental impact. Damage during restart can also be a major issue. The increasing reliance on automated systems for control, emergency shutdown and mitigation means that power supplies and back-up systems must be much more reliable than in the past.

There have been many incidents where loss of external power has been a key factor and there are opportunities to learn from these events when assessing the design criteria and maintenance requirements of supplies and back-up systems. Typical facilities that require a reliable supply of power include offshore

platforms, oil refineries, petrochemical, chemical, pharmaceutical, plastics, glass and nuclear industry facilities.

Power is not only required for process control and for driving the plant and machinery; it is also a crucial link in the chain for provision of services including steam, air, process water, cooling water, nitrogen, lubrication and emergency systems. There have been several instances where even a brief power loss has led to the cascade failure of services, which has then resulted in a major incident.

Causes of power supply failure include: Fires in substations and switch-houses, faults/ human error when working on switchgear, underground cable faults, excavations and other works damaging underground cables, vehicles striking overhead cables, lightning strikes and storm/ flood/ tsunami.

Typical protection from power loss include uninterruptible power supplies (UPS's), emergency power generators, services back-up (stand-by boilers, nitrogen back-up for air, gravity fed cooling water/ lubrication). These don't always work.

Procedures are written to include "load-shedding", manual activation of valves and critical safety systems. In a real situation, some of these may literally require working in the dark. There is a lot to do, few staff and little time to act.

Planning for power outage requires a thorough assessment of the scenarios that may occur, the possible consequences and the design and reliability of the measures that are in place. Novel ideas for low frequency/ high risk scenarios may need to be considered.

This presentation reviews some examples of incidents that have occurred to encourage operators to reconsider the potential impact of a sudden loss of power at their facility and how they would deal with such an event.

7. Risk tolerability targets; misconceived, misunderstood and misapplied

Presenter: Carolyn Nicholls – Principal Consultant, RAS Ltd

Following on from a quantification (or semi-quantification) of risk, the next step in any assessment is to compare the result to a set of risk tolerability criteria. Three regions of risk are usually defined, an unacceptable region and a broadly acceptable region bordering a region of tolerable risk. The tolerability of this middle region is dependent on those risks being As Low As Reasonably Practicable (ALARP). The 2001 HSE publication 'Reducing Risks, Protecting People - HSE's decision-making process' (R2P2) is widely used in industry to set these region boundaries. R2P2 clearly defines the tolerability boundaries for individual risk, and gives guidance regarding societal (or group) risk tolerability.

How these criteria have been applied across the industry varies dramatically, particularly in setting targets for Layer of Protection Analysis (LOPA). LOPA is often used to identify the need for, and define the required integrity of, a Safety Instrumented System (SIS). In this context, it is easy to see how setting the wrong targets for a risk assessment can result in serious consequences. For example, setting a risk target that is too lenient could result in a process that is not adequately protected, and setting a risk target that is too onerous could result in the requirement to needlessly install a high integrity safety system at a significant cost. To set appropriate risk targets, the intricacies between types of risk need to be well understood, and applied correctly for the given situation. Our experience is that this is often misunderstood and misapplied, people take simple rules and apply them in the wrong context.

This paper considers the differences between individual risk and societal (group) risk, and how these are often confused and misapplied. Differences between scenario risk and whole site risk, and how these should be considered in different ways depending on the type of risk and the type of study are then discussed. Risk targets are proposed which may be used in LOPA, including a demonstration of how these were developed and how they meet industry and regulatory standards. How these targets can be used and adapted into existing or new facilities, and how they may interact with existing corporate risk criteria and matrices is also considered.

8. Safety culture, climate and performance improvement

Presenter: Dr Kevin Fitzgerald – Risk Management Dept. Manager, Lloyd's Register Energy

The term 'safety culture' was first used in INSA's (1988) 'Summary Report on the Post-Accident Review Meeting on the Chernobyl Accident'. Safety culture has subsequently been defined as: "Consisting of shared values (what is important) and beliefs (how things work) that interact with an organisation's structure and control systems to produce behavioural norms (the way we do things around here)."

It has also been described as simply "how people behave when no-one is looking." Research over many years has demonstrated that incidents are almost always related to incorrect or inappropriate workforce behaviours, and it is the way that culture drives behaviour that is important to us. Within the process industries, incidents such as Longford (1998), Texas City (2005), Buncefield (2005) and Macondo (2010) have all served to highlight the importance of safety culture, along with other more specific human factors shortcomings.

The influence that an organisation's culture has on individual behaviour is generally acknowledged and many organisations worldwide have set themselves the goal of improving their safety culture so as to achieve lower incident rates. But what does safety culture really comprise, how do safety culture failings make themselves apparent, and how can we go about changing culture?

This presentation will:

1. Provide a brief introduction to the concept of safety culture and the characteristics of a positive safety culture.
2. Illustrate – through case studies – some consequences of safety culture failings.
3. Indicate how safety climate surveys can be used to help understand safety culture and how the output from these surveys can be used to prioritise issues for improvement.
4. Show some of the typical starting-points for safety culture improvement in organisations.

The presentation will draw on non-process sector experience (particularly Marine) to help illustrate the generic challenges that need to be managed in complex process safety environments.

9. Mental health awareness in a safety critical environment

Jamie Walker - Safety & Projects Director, UKPIA

The stigma around mental health has long been an issue. Fortunately, mental health awareness has recently been heightened as royalty and other public figures have publicly disclosed their own battles against the illness. HSE has already stated that stress and mental health pose a significant threat to the workplace. UKPIA is currently working with Competent Authority and other Trade Associations and organisations with the intention of providing a co-ordinated and structured approach to dealing with the issue.

In this question and answer session, UKPIA aims to increase the perception within the safety critical environment, looking at how mental health illness affects the patient, their families and equally as importantly, work colleagues and the organisations which they work for. The presentation is intended to provoke conversation within the workshop and provide people with the opportunity to discuss how the issue is currently being dealt with and how matters may be improved in the future.

Individuals who have, or are working with others who have, mental health issues and are engaged in process safety activities pose a risk if they are not managed correctly. The aim of the workshop is to provide a better understanding of possible warning signs and how to deal with sufferers who themselves may not be aware of their issues.

10. The role of third-party testing in securing Industrial Internet of Things (IIoT) compliance

Matt Jakuc – Cybersecurity Technical Lead, CSA Group

With some projections claiming a 300% increase in IIoT-ready devices in just the next 4 years (some 22.5 billion by 2021), and other forecasts suggesting that IIoT investment will make up as much as 40% of some organisations' capex budgets, the Internet of Things in the Industrial space is already well and truly here.

The major benefits of IIoT are well known – efficiency & reliability gains, coupled with the ability to record big data for remote analysis. Yet, the challenges and opportunities that IIoT brings in the quest for protecting lives requires an equal focus, particularly when you consider how IIoT will be incorporated into a Hazardous Location (explosive atmosphere). Here, there are a number of elements to consider, including continued hazardous location safety compliance, functional safety assurance and cybersecurity protocols.

The convergence of information technology (IT) operational technology (OT) networks, has tremendously increased the risk of cyberattacks that may affect safety, reliability and availability.

Modern control systems are no longer isolated but are part of a larger connected infrastructure that can offer significant cost savings but also cybersecurity concerns. Security risks associated with integrating, modifying or maintaining a controller in process can impact overall safety and security. This changes the risk profile that should be considered when designing and/or integrating components in the systems.

Often, little consideration is made to their security requirements due to cost constraints. Vendors, system integrators and asset owners face challenges in keeping their systems secure including technical expertise and privacy concerns. The integrators, asset owners and facility managers need cybersecurity assurance when selecting potential hardware and software-based solutions. These solutions should be specifically designed and formally evaluated to identify and prevent cybersecurity threats in industrial environments.

During this presentation we will uncover: Challenges & risks in IIoT – covering Hazardous Locations, Functional Safety and Cybersecurity; Steps to limit the likelihood of such incidents and their impact; Keys to third-party evaluation and testing and Steps to successful attestation and certification of connected devices.

11. IIoT 4.0 and LoRa for maintenance purposes in hazardous areas

Gido Van Tienhoven - CEO, Ex-Machinery

This paper focuses on the use of various sensors to monitor the technical state of various types of equipment by means of LoRa Wan technology. LoRa is short for Long Range. It explains how this technology can reduce maintenance costs thanks to preventive maintenance.

The results of a small study amongst end users about the opportunities for this technology will be presented. The result will show examples like monitoring the technical state of a pump by means of the vibration level. Other examples are temperatures of bearings, leakage detection, etc. Interaction with the people attending will be stimulated on this subject.

The paper will present LoRa as an international standard for wide area networks IIoT. It will discuss globally how it works and of what use it can be. Due to the low amount of RF energy involved it is technology that can be applied very well in hazardous areas without causing risks of ignition. Because LoRa technology requires low power it can be battery powered, so field installation can be done without wires.

LoRa technology is node-hub technology. As a result a few hundred sensors on a large plant can be easily connected to one hub. All the readings of the sensors can be seen on internet based systems. All communication via the internet is encrypted. Due to the design, partners involved in encryption the LoRa system has good performance on the aspect of cybersecurity.

The paper focuses mainly on the applications and opportunities of LoRa in the oil and gas industries and less on the IT-technology.

12. Paperless safety lifecycle at the R.STAHL Plant & Engineering Center

Stefan Hack - Business Development Manager, R.STAHL

Inspection plans and intervals vary deeply depending on the kind of equipment, the legal basis and the standards that are taken into account. Safety systems concerning process control engineering have to fulfil a certain safety integrity level (SIL) and are considered as safety integrated systems (SIS). The proof-test interval amounts into the calculation to reach a certain SIL according to IEC 61508. A typical interval would be only twelve month which leads to frequent inspections. The scope of the test itself depends on the equipment type. Fragmented IT-systems are another problem.

The Plant & Engineering Center offers a modern application that comes with a holistic approach to optimize periodic inspections and to relieve all people involved. Its three modules – PEC-EX, PEC-FS and PEC-SQ – provide paperless inspections for hazardous area equipment, for safety instrumented systems and for all other required inspections concerning operational safety and quality.

Instead of replacing the established CAE-, ERP and document management systems, PEC can be connected to them with automatically, bidirectional interfaces. This provides a high data quality, reduces data errors and saves a lot of time by offering the possibility to interact with all three systems through one application.

Within PEC-EX, inspection plans can be generated automatically. PEC-FS and PEC-SQ provide an inspection plan generator, which enables its users to work with individual inspection plans for each equipment that can contain standardized, reusable test blocks. An integrated Scheduler helps to keep track on deadlines. Inspection results can be evaluated to make sure standards can be met.

By offering an app for Android and Windows based tablets, PEC greatly reduces the amount of time spent on performing inspections. Protocols can be signed electronically and archived directly in PEC as well as being transferred to a document management systems.

PEC is currently in use at several plant operators in the Niederrhein area (Germany) and has already proven that it can help to save time, to be compliant to standards and to help in improving data inspection quality.

DAY TWO - 1/3/2018

13. Functional safety management of installed SIS

Nic Butcher - ECI Specialist Inspector, HSE

The requirements for functional safety management are set out in good practice BS EN 61511 but the lifecycle described is focussed on new SIS which may leave some conspicuous gaps in dutyholders' understanding of the requirements for their range of existing installed SIS, which might have been implemented to older standard or earlier versions of BS EN 61511.

The Health and Safety Executive has been working with the Chemicals and Downstream Operators Forum (CDOIF) to develop a set of pragmatic guidelines on how to manage installed SIS that describes the procedures and processes required including a process of periodic review and assessment.

14. No safety without security - No security without safety

Tino Vande Capelle, Consultant, TVC, & Steve Smith, Consultant, ONRIX gcv

This joint presentation by consultants Tino Vande Capelle and Stephen Smith will look at the history of functional safety and provide a practical approach to cybersecurity in industrial environments, with a common feature being the human factor as the weakest link.

What have we achieved after 20 years of Functional Safety standards in the process industry? Why does it remain so difficult to learn from mistakes others have made in our industry? Human nature does not like to admit or reveal knowledge of problems. So, for the past 30 years, certain standards have helped engineers apply good engineering practices, but the weakest link in the safety culture remains the human being. Standards such as, but not limited to, DIN 19250, ISA 84.00.01, IEC 61508 & 61511 have been put in place to force a safety culture in our industry in the hope of achieving a better world where people, environment and investment can be safe. Both the IEC61508 and IEC61511 are in their second edition as technology evaluates so does engineering culture. Tino's aim is to summarise and simplify some of the pitfalls that you may face in the future

Cybersecurity is often represented in the media through malware and hacking attacks. But little is written about the cause and effect of such attacks. Stephen will present pragmatic considerations concerning the problems and mitigation activities of cybersecurity; this inevitably centres on the human factor. Safety and quality activities in all industrial environments focus on the people and their actions; security is no different, it is much of the same in disguise. Unfortunately, the disguise is presented as being complex and forbidding. In closing, Stephen's aim is to shine some common sense on the subject and demystify the subject of industrial security.

15. Certification of robotics in an Ex environment- ATEX and Functional Safety requirements

Hassan El Sayed - Functional Safety Business Manager, CSA Group

It is the responsibility of manufacturers and design engineers to integrate protection concepts listed under EN/IEC 60079 series to demonstrate full compliance against the ATEX Directive when products are to be used in hazardous areas within EU member countries.

Compliance with the harmonized standards for potentially explosive atmospheres can be a challenging task, especially if the product cannot be fully certified to EN/IEC/ISO series due to excessive voltage range or if the application contains potential explosive source where the existing protection concepts cannot offer the safety measures required.

Product certification may require certain combinations of different protection concept techniques to provide the safety measures with respect to explosion risks and to meet a specific classification or category.

This paper discusses the certification requirement of a safety related controller located in safe area as a safety related device to control and manipulate the implemented safety functions built in a robot located in hazardous area, where the robot is partially certified to meet certain types of protection concepts to EN/IEC 60079- series.

The task requires risk assessment to the hazard sources in order to allocate a Safety Integrity Level (SIL). The assessment studies the requirement for a safety system validation where safety related software shall be developed to comply with the requirements defined for safety devices as described in article 1, 1(b) of the ATEX Directive 2014/34/EU.

These requirements are also shown in section 1.5 of Annex (II) of the Directive. In particular, the ATEX Directive recommends the use of IEC 61508, EN 50495 or any equivalent safety related standard for the safety-critical software development. The article also discusses the special protection concept (s) using IEC 60079-33 where safety achieved by functional safety and other protection concepts assessed to EN/IEC/ISO are coupled to deliver a fully certified product for use in hazardous location.

16. Recent changes in regulations governing PPE

Ian Crellin - Marketing Manager, British Safety Industry Federation (BSIF)

With the new PPE Regulation (EU) 2016/425 coming into force it is vital that both the commercial operators and users of Product understand the implications and that there is a consensus of understanding.

It is essential that the UK is able to achieve a smooth, effective and efficient transition to the new Regulation. Personal Protective Equipment plays a vital role in ensuring that occupational safety and

health is maintained. We are both in the midst of Brexit and in the middle of the timeline for the new Regulation becoming applicable and being applied exclusively from 2019.

BSIF's seminar will take delegates through a Step by Step process illustrating the actions that must be executed to ensure that products are able to be in compliance.

As those involved in the PPE market are aware the risks and therefore the products providing protection, are placed into risk categories (Categories I, II & III) and each category requires a range of compliance actions and differing levels of quality assurance once any necessary type testing and EU examination certificate has been granted. The presentation will walk the audience through the process in logical bite size steps.

17. Addressing the challenges of dust explosion risks in grain storage

Frank Ward - Director & Project Engineer, Hennock International

The storage of agricultural materials in large, predominantly sealed, vessels (silos) presents challenges in terms of the control of the risk of dust explosion and the protection of life, property and structures in the event of an explosion.

- A grain storage silo may contain numerous items of equipment all of which present potential sources of ignition.
- Dust is created as a normal part of the handling process, though the nature and levels of the dust may vary significantly over the time of loading/discharge and processing within the silo.
- Equipment is often operated by unskilled workers.
- Modification to equipment is not uncommon.
- The market for equipment is highly cost sensitive.

These, and other factors, are challenges faced by silo and equipment manufacturers

- How can the creation of the combustible dust be minimised?
- How can the potentially explosive mixtures of dust and air be controlled?
- What are the potential ignition sources and how can they be eliminated/controlled?
- What is the impact of an explosion in a full or semi-filled silo?
- What protective measures can be applied to a vessel of this size which meets the requirements of regulatory compliance and can be applied cost-effectively without affecting the primary purpose of the structure?

The paper will look at approaches which may be taken to address each of these questions.

- ATEX compliance of grain handling equipment
- Handling methods to minimise dust creation
- Use of aeration and ventilation to dilute air dust concentration to below MEL. How heavily can this be relied upon to provide total or partial control of the explosion risk? What levels of ventilation may be required to provide control, and how can this be provided in practice?
- Design of silo structures to provide dust explosion venting (frangible roof). This will consider the challenge of balancing the primary requirement of the silo roof, to withstand external loads (snow/wind/imposed loads) versus the need to be sufficiently weakened to adequately vent the explosion pressure. The additional challenges faced in provision of certification of such a large scale system under regulation as a protective device.
- Design of silo structures to withstand increased pressure during vented explosions. With explosion venting comes greater storage pressures. This will consider the balancing act that the designer must perform to provide light-weight, cost effective design with sufficient strength to withstand the additional pressures whilst controlling the engineering complexity of the roof structure to provide the required venting.

18. Fire detector mapping - what metrics should we be using?

Tim Jones - Senior Consultant, MMI Engineering

Fire and gas detector mapping using computational methods has become more and more common in hazardous industries in recent times. Despite the advances in the technology and methods associated with fire detector mapping, one of the most important aspects is how we deem a detection system adequate with respect to the coverage it provides.

At present, there is little guidance given by the UK HSE or other industry bodies on the definition of coverage and how it should be achieved. As a result, companies use their own internal standards and methodologies, which can vary significantly in efficacy. These company standards typically measure the performance of fire detector systems in terms of percentage coverage over a particular volume. This may seem a reasonable metric but it misses the most important factor, namely the size of the gaps that the detectors do not cover. It is the size of the gaps in your system that is going to dictate whether or not your system is able to detect a fire of a size that may lead to escalation. A fire area could have a very high percentage coverage but still have gaps where a significant fire could exist.

This paper aims to show the deficiencies in measuring detector coverage based on percentage coverage alone and presents the advantages of alternative methods, such as optimising your system to ensure that no fire above a certain size can go undetected e.g. 1m spherical fire. The work presented within this paper uses MMI's inhouse fire detection code, 'MMICast', that utilises ray casting techniques (see Figure 1) in a fully three-dimensional manner to account for obstructions that block a detector's line-of-sight.

19. Cybersecurity - What should Safety Instrumented System integrators be doing?

Chris Parr - Technical Authority for Functional Safety, Sella Controls

There is increasing momentum in the process industries to address cyber security risks associated with Industrial Automation and Control systems (IACS) and the publication of the UK Health and Safety Executive Operational guidance (OG-0086) on the subject matter is likely to see this focus increase.

Safety Instrumented Systems (SIS) are recognised as a primary protective layer for many Oil and Gas and Petrochemical facilities. Whilst the specification, design techniques and assessment of the integrity of these systems is well understood through industry guidance and standards such as BS EN 61508 and BS EN 61511, best practise for protecting these systems from security threats throughout their lifecycle is less clear. However, it does appear that IEC 62443 "Security for industrial automation and control systems" will become the de-factor guidance and is referenced in both BS EN 61511 and the HSE's operational guidance.

System Integrators play a key role in the design, modification and maintenance of Basic Plant Control Systems and Safety Instrumented Systems and in the majority of projects they provide turnkey solutions for the control and automation aspects of the project to the end users. This raises the question of how these system integrators handle security issues and if their practises and procedures sufficiently reduce security vulnerabilities in the design, operation and maintenance phases of the lifecycle.

IEC 62443 part 2-4 covers the security program requirements for IACS service providers. It gives specific requirements of what a system integrators management system should include to give confidence to asset owners that the integration and maintenance activities that they complete include appropriate security measures. The standard covers subjects such as staffing, solution hardening, network security, user security and patch management.

This presentation will introduce Part 2-4 of IEC 62443 and explain why compliance is good for both the system integrator and their clients. It will also draw on the presenter's own experience of applying the standard in a safety systems integrator environment and highlight the challenges and opportunities faced.

20. When safety meets security - Combining the best of both worlds

Rob Turner - Advanced Solutions Consultant, Yokogawa

The latest edition of IEC 61511-1 "Functional Safety - Safety Instrumented Systems for the Process Industry Sector" requires that the existing risk assessment process for a safety instrumented system should now include an assessment of cyber security vulnerabilities in addition. At first sight this might appear to be an additional burden for the process industries and an intrusion into the jurisdiction of IEC 62443 which already covers the security of these systems.

And yet these two standards might not be so far apart in their approach. This presentation explores:

- 1) The need for a tie between safety and security for industrial control systems, and safety instrumented systems in particular.
- 2) The areas of common ground between IEC 61511 (functional safety) and IEC 62443 (industrial cyber security).
- 3) How to potentially combine the best of both standards and achieve a control network that is safely secure, and securely safe.

21. Are luminaires causing hidden risks in Ex Areas because of LEDs?

Tarmo Rintala - Technology Manager, Atexor Oy

The potential risks of high-powered LED luminaires have been known for years. Those risks are growing as LEDs get more and more powerful. It is equally clear that the interpretation of the standards meant to ensure the safety of these luminaires has been anything but consistent.

In September 2016, at the IECEx meeting at Umhlanga, South Africa, The chairman of the Ex Technical Advisory Group (ExTAG), Professor Xu Jianping, presented the issues regarding LEDs and the possible ignition sources caused by powerful light.

The main message is clear: There are too many different interpretations of the standards, and this is resulting in compromises on safety.

The number of LED luminaires for applications where flammable vapors and particles are present is increasing rapidly. The risk if ignition may be significant if the optical radiation has not been accounted for in the design of the luminaires.

When selecting equipment for areas with possible risk of explosion, due care must be taken. All companies do not necessarily have experts qualified to understand the differences in the safety of products. Often the purchaser is just checking that the Ex certification exist, and not digging into the details of what that certification actually covers. The person responsible for selecting and accepting products must be able to trust the certification and other information of a product.

The problems with current practices are systemic, and they are leading us to a situation where Ex classified sites have an increasing number of LED luminaires which may not be safe to use at the site. Thanks to Professor Xu Jianping, the issue of optical radiation is properly out in the open. This is huge step, but still only the first step in actually ensuring the safety of high tech lighting systems.

22. Coldflow in cables - some practical advice

Geof Mood - Technical Director, CCG Cable Terminations Ltd

The subject of coldflow in cables is poorly understood and this has led to widespread confusion amongst designers, specifiers and installers particularly in the selection of suitable cable glands to use with affected cable in Ex applications. BS EN / IEC 60079-14 states that the installer should 'select cable glands to reduce the effects of coldflow characteristics of cable'. However it fails to define what is or is not cable with coldflow characteristics or how it is possible to reduce the effects of coldflow, and if possible how much reduction is needed. This has given some cable gland manufacturers the opportunity to make exaggerated claims for their products and to create an atmosphere of fear amongst specifiers and installers, having them believe that coldflow in cables is a risk in applications where it is not.

Lack of understanding of what coldflow is has also led to a number of installations being carried out with inappropriate cable glands leading to a need for costly refits in some cases. There is also the very real risk of installations being unsafe despite the installer following the guidance of BS EN / IEC 60079-14 and using the assurances of the cable gland manufacturer.

This paper will debunk a number of common myths. It provides some practical guidance about what coldflow really is and shows a simple and cheap test method to determine if cables are affected by it. It will also provide straightforward advice about how to eliminate the effects of coldflow and achieve a safe installation if the cable being used is at risk of coldflow. The advice is strictly in compliance with BS EN / IEC 60079-14 and will lead to safer, and in many cases also cheaper, installations.

23. How to prevent electrostatic charging of process equipment situated in ATEX atmospheres.

Mike O'Brien - Managing Director, Newson

This presentation will:

- Outline why static electricity is an ignition risk in the chemical industry.
- Provide case studies and analysis of incidents resulting from the ignition of flammable atmospheres due to discharges of static electricity.
- Describe what measures electrical equipment specifiers, production managers and QHSE managers can take to eliminate the ignition risks of static electricity.
- Correlate these measures with the guidance stipulated in IEC 60079-32-1: "Explosive atmospheres - Part 32-1: Electrostatic hazards - Guidance".
- Present novel ways of grounding multiple components at risk of electrostatic charge accumulation.

24. Making excellence a habit - How to improve performance, reduce risk and achieve sustainable growth in the areas of explosive atmospheres

Sarra Cheyney - British Standards Institution (BSI)

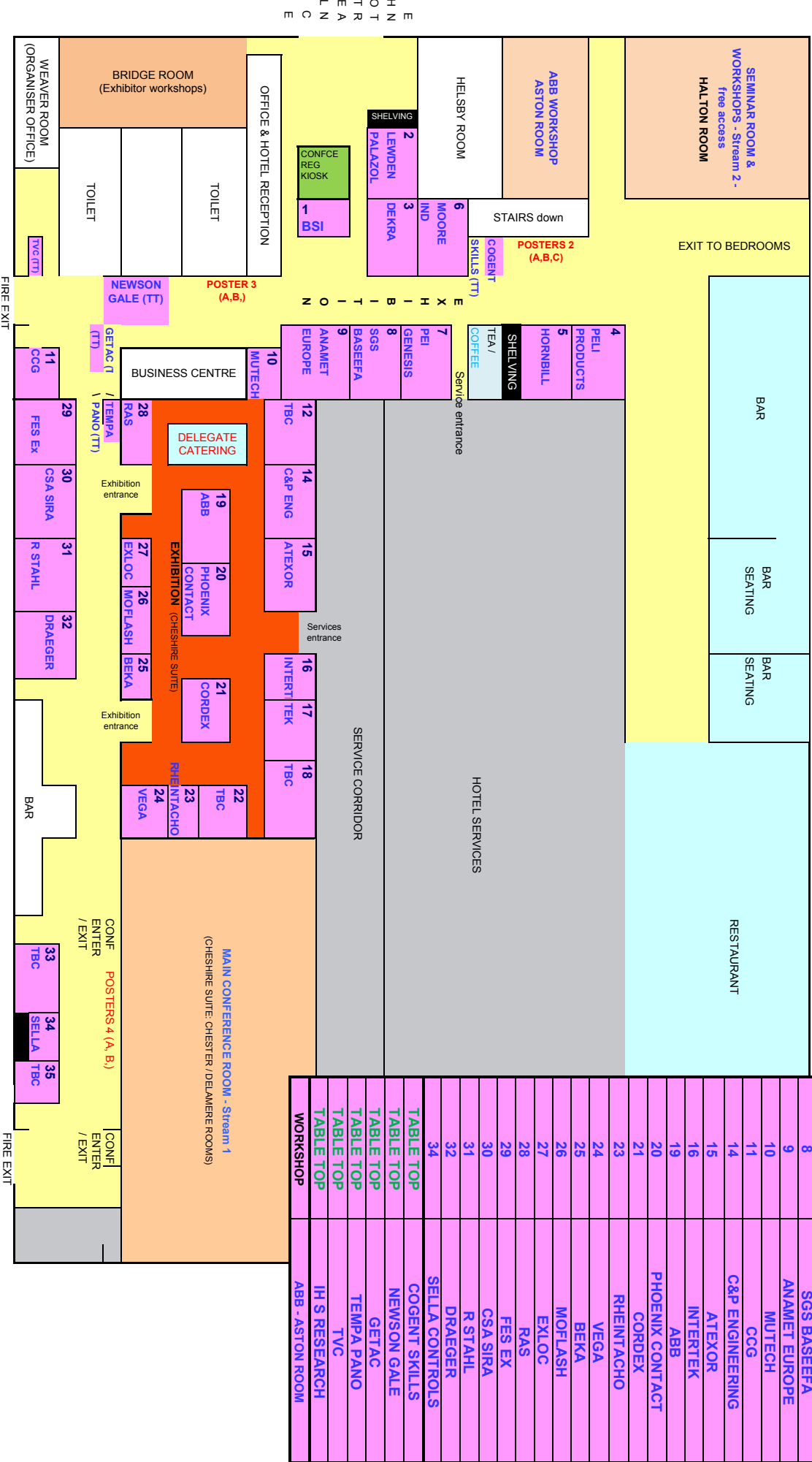
Risk management and assessment is necessary across many business processes, not just areas such as health and safety. Explosive atmospheres in the workplace can be caused by flammable gases, mists or vapours or by combustible dusts. Explosions can cause loss of life and serious injuries as well as significant damage. Guidance and standards can help avoid a potentially explosive scenario.

This presentation will show how a business can reassure shareholders, customers and employees that by managing risks it is being effectively managed and confirm its compliance with corporate governance requirements.



Floorplan and exhibitor list

Hazardex 2018 Conference & Exhibition – Holiday Inn, Runcorn, Cheshire – 28th - 1st March



STAND #	EXHIBITOR
1	BRITISH STANDARDS INST
2	LEWDEN PALAZOLLI
3	DEKRA INSIGHT
4	PELL PRODUCTS
5	HORNBILL ENGINEERING
6	MOORE INDUSTRIES
7	PEI GENESIS
8	SGS BASEEFA
9	ANAMET EUROPE
10	MUTECH
11	CCG
14	C&P ENGINEERING
15	ATEXOR
16	INTERTEK
19	ABB
20	PHOENIX CONTACT
21	CORDEX
23	RHEINTACHO
24	VEGA
25	BEKA
26	MOFLASH
27	EXLOC
28	RAS
29	FES EX
30	CSA SIRRA
31	R STAHL
32	DRAEGER
34	SELLA CONTROLS
34	COGENT SKILLS
34	NEWSON GALE
34	GETAC
34	TEMPA PANO
34	TVC
34	IH S RESEARCH
34	ABB - ASTON ROOM



Delegate Booking Form

Simply complete & return as soon as possible to events@imlgroup.co.uk
Places & hotel availability are allocated on a first come, first served basis.

Delegate 1: Job Title:

Delegate 2: Job Title:

Delegate 3: Job Title:

Delegate 4: Job Title:

Company:

Address:

.....

.....

Postcode: Contact Email:

Tel: Fax:

Please complete ALL of the following sections:

I wish to book place(s) on PACKAGE of the **HazardEx 2018 Conference**, as follows:

Delegate 1

I will attend on:

Day1 Day2 Both Days

Please book me accommodation on:

Wednesday 28th February ²

I would like to attend the inclusive Awards Gala Dinner ³

Delegate 2

I will attend on:

Day1 Day2 Both Days

Please book me accommodation on:

Wednesday 28th February ²

I would like to attend the inc. Awards Gala Dinner ³

Delegate 3

I will attend on:

Day1 Day2 Both Days

Please book me accommodation on:

Wednesday 28th February ²

I would like to attend the inc. Awards Gala Dinner ³

Delegate 4

I will attend on:

Day1 Day2 Both Days

Please book me accommodation on:

Wednesday 28th February ²

I would like to attend the inc. Awards Gala Dinner ³

² Inclusive for Package 'A' & 'B' delegates or at an additional £99.00+VAT for Package 'C' delegates.

³ Inclusive for Package 'A' & 'B' delegates or at an additional £90.00+VAT for Package 'C' delegates.

I wish to utilise the 2-for-1 deal available on package A only at £850+vat. It is agreed that we will still pay the full amount of £850+vat should only one delegate attend. Not applicable with any other package or offer and subject to availability. There is no discount for not utilising the 2-for-1 offer once booked. This is a limited time offer and will expire.

ANY accommodation required for Tuesday 27th February must be booked and paid for directly with the hotel and their terms will apply. We will NOT hold/book any rooms for that night. Please quote 'HAZARDEX' when you book rooms for the Tuesday night at the hotel by calling 01928 754808. Cancellations and amendments must be made directly to the relevant hotel for Tuesday 27th February or with the HazardEx Events team for Wednesday 28th February only.

PAYMENT: (Please tick the relevant box) all prices exclude VAT

Early-bird discount available for a limited time only, on package A delegates for just £600+vat, contact us by completing this form to confirm your discounted place!



**Package A: Full Conference Attendance & unlimited access to the exhibition area for both days
Accommodation for Wednesday 28th February
One Place at the Gala Dinner on Wednesday 28th February
All meals & warm refreshments for both days
Complimentary copy of the conference notes**

- 1 delegate @ £850 **Early-Bird discount £600**
- 2 delegates @ £1600
- 3 delegates @ £2340
- 4 delegates @ £3040

**Package B: One full Conference day on either day
Unlimited access to the exhibition area for both days
Accommodation for Wednesday 28th February
One place at the Gala Dinner on Wednesday 28th February
All meals & warm refreshments for the Conference day only
Complimentary copy of the conference notes**

- 1 delegate @ £595
- 2 delegates @ £1130
- 3 delegates @ £1695
- 4 delegates @ £2260

**Package C: Choose one conference day as well as unlimited access to the exhibition on both days.
Warm Beverages & lunch on your appointed day
Complimentary copy of the conference notes**

- Each delegate @ £445

Payment must be made prior to attendance via one of the following methods:

CHEQUE: Made payable to **IML Group plc.** Please send through to the address as shown, within 7 days of booking.

CREDIT CARD: Type of Card: VISA / Mastercard (*delete where applicable*)

Card Holder Name:

Card Number:

Expiry Date: CVC: Total Amount:

Please note a 3% charge will be added if paying by credit card

PURCHASE ORDER: P/O Number:

Signature: **Date:**

*On receipt of payment, you will receive confirmation of your place on the Conference within 7 days. Formal VAT receipts will be issued, only when payment has been received or a purchase order number has been assigned. Joining Instructions will be forwarded to you at least two weeks before the Conference. Cancellation charges apply.
The organisers reserve the right to change the programme.*

For Office Use Only:

Delegate No: Date: Amount:

Order #: Rep: HTJ0118RG Payment Received / Payment Due

**REGISTER TODAY BY COMPLETING AND RETURNING THIS FORM TO THE EVENTS TEAM ELECTRONICALLY
OR BY POSTING IT, WITH YOUR PAYMENT, TO THE ADDRESS AS SHOWN BELOW.**



Hazardex, IML Group plc, Blair House, High Street, Tonbridge, Kent TN9 1BQ UK
Tel: +44 (0)1732 359990 Fax: +44 (0)1732 770049 Email: events@imlgroup.co.uk
Website: www.hazardexonthenet.net