Hazards forum

The Hazards Forum Newsletter

Issue No. 89
Winter 2015

Web version

Hazards Forum Newsletter

Issue No. 89 - Winter 2015

Contents

Edited by Dr. Neil Carhart

Views expressed are those of the authors, not necessarily of the Hazards Forum

Further information regarding the articles in this issue is available from
Tim Fuller on 020 7665 2230, in the Hazards Forum Secretariat Office
E-mail: admin@hazardsforum.org.uk

Hazards Forum website: www.hazardsforum.org.uk
Hazards Forum Executive Secretary: *Brian Neale*

December 2015

The Health and Safety Laboratory and the Health and Safety Executive: Recent Developments

Professor Andrew Curran BSc PhD FRSB FCMI Hon FFOM
Chief Scientific Adviser Director of Research,
Science Directorate,
Health and Safety Executive

Richard Lewis BA MBA MLS MCLIP
Head, Chief Scientific Adviser's Office,
Science Directorate,
Health and Safety Executive

For twenty years until April 2015, the Health and Safety Laboratory (HSL) operated as an agency of the Health and Safety Executive (HSE). During that time, HSL developed a distinctive and distinguished role in occupational health and safety in Britain and internationally.

HSL supported HSE in providing scientific and technical support and insight into accident investigations, and provided much of the evidence from applied research that HSE needed to develop policy, regulation, guidance and other interventions.

HSL was encouraged by HSE to work for external customers as well over the same period, developing commercial capabilities and generating additional income. This activity helped HSL maintain and develop its unique offering during a time of reducing public funding.

The Triennial Review of HSE, chaired by Martin Temple, reported in January 2014. It concluded that while an organisation like HSE remained the best model for delivering the statutory functions established by Parliament, there were a number of areas where HSE could improve delivery and could explore options for further commercialisation or delivery through and in partnership with others. Subsequent work concluded that a change in HSL's status, to integrate it with the rest of HSE, would provide one of the means through which HSE would play its enhanced role in the health and safety system in Britain and internationally.

Richard Judge, HSE's new Chief Executive, decided to create a Science Directorate, by bringing together the capabilities in HSE's Corporate Science, Engineering and Analysis Directorate (CSEAD) and HSL, from 1st April 2015. CSEAD was the home to HSE's members of the analytical professions which operate within Government –statisticians, economists and social researchers. They too have a proud record: for example, last year and for the life of the last parliament, HSE came top of all government departments for impact assessments whose analytical quality was rated as 'fit for purpose' by the independent Regulatory Policy Committee.

The new Science Directorate is seen as vital to and wholly in harmony with HSE's plans. Revitalised science lies at the heart of HSE's evidence-based approach to policy making and risk management and having this capability 'in-house' gives HSE some significant advantages as a modern regulator.

By bringing together HSL's scientists, engineers and technical staff with HSE's economists, statisticians, social researchers, doctors and science policy staff, the Science Directorate continues to support HSE's work and to offer enhanced commercial work in Britain and internationally. The new directorate also improves professional development options for people whilst gaining more value from sharing the different skills, networks and relationships that people previously had.

Work to integrate HSL into HSE is progressing – and is progressing well. The key strength of Science Directorate is that both parts shared a common vision: *using science to enable a better working world* and *ensuring that HSE's work is underpinned by sound evidence, accessible expertise and effective engagement.* While there is some way to go on issues like systems, and culture,

one thing is clear; there is a positive feel among the staff about this integration.

HSE's new Chief Scientific Adviser is Prof Andrew Curran – who is also HSE's observer on the Hazards Forum Executive Committee. He is also HSE's Director of Research and the Head of the Science and Engineering Professions across HSE.

Creating the Science Directorate will help HSE develop more forward looking and long-term approaches to planning, including identifying priorities, investing in understanding the problems and developing effective science and devising regulatory solutions.

Removing the customer-contractor relations between HSE and HSL, and replacing them with slimmer procedures for commissioning and completing work for HSE, has released capacity for initiating new programmes of shared research, conducting more futures work, completing a Science Strategy and HSE's Science Report.

The HSE Board is taking greater interest in its science. It is appointing a Science and Engineering Assurance Committee whose members will be independent of HSE – leading academics, professionals or practitioners in an area related to health and safety.

HSE is re-establishing the roles of Chief Analyst and Chief Medical Adviser to improve HSE's expert representation in Whitehall and in other national and international fora, and to represent analysis and evidence better at high-level discussions in HSE.

The long-standing commercial culture in HSL is being extended throughout HSE. The commercial work is ultimately focussed on working for the public good and offers a range of interventions which will help both the new Science Directorate and the wider HSE thrive. These are some of the commercial and international activities that have benefitted from bringing HSE and HSL closer together:

- The recently formed International Team is following up on a series of senior level visits to the UK. One example is to deliver a contract secured with the Mexican Government related to offshore safety.
- So far, over 50 ideas from HSE staff have been evaluated such as specialist training linked to new construction regulations.
- A Land Use Planning Web App was successfully launched in 2015. Multi-disciplinary teams from HID and Science Directorate are attending relevant construction events to deliver live demos and talk directly to developers and planners.
- The reputation of HSE's data analytics capabilities continues to grow across government. Our expertise in mining large volumes of data, extracting useful information and then presenting this in a user friendly way is attracting a lot of interest.
- HSE's annual statistics this year were disseminated using innovative media such as YouTube and twitter and were turned into an infographic poster which is for sale. The owner of a small business commented, *"Congratulations on the new poster. It really does concentrate the mind and assists H&S professionals to put the message across in a way people can understand. Great job, more of this style please."*

By creating the Science Directorate, HSL is being integrated into HSE, creating a unique resource available globally for investigating, researching and creating evidence based interventions to manage risks to health and safety at work.

For more information go to - http://www.hse.gov.uk/research/ and http://www.hsl.gov.uk/

Contacts:

Andrew Curran - Andrew.curran@hsl.gsi.gov.uk

Richard Lewis - richard.lewis@hse.gsi.gov.uk

European Safety and Reliability Conference ESREL 2016

Jacqueline Christodoulou
CEO, Safety and Reliability Society

The Safety and Reliability Society is pleased to announce that it will co-organise the **European Safety and Reliability Conference ESREL 2016** jointly with University of Strathclyde and ESRA.

The conference will be held on **26-29th September, 2016** in the Conference Centre of the new **Technology and Innovation Centre (TIC)** in the heart of **Glasgow**.

It aims to bring together industrial and academic experts in safety and reliability, focusing particularly around core areas of expertise and industrial needs, in energy (oil and gas, renewables, nuclear), aerospace, and defence in particular. The Programme Committee will be led by Lesley Walls (Strathclyde), while the meeting will have three co-chairs – Terje Aven (ESRA), Richard Denning (SaRS) and Tim Bedford (Strathclyde).

Jacqueline Christodoulou, Safety and Reliability Society's Chief Executive Officer said, 'This as a major opportunity for everyone involved in safety and reliability to come together at an international conference where cutting edge research meets industry innovation. The last ESREL conference held in the UK in 2000 forged partnerships on all levels that have lasted – we hope that ESREL 2016 will provide an opportunity for industry, academia and professional institutes to meet and network to the benefit of all.'

For academics and industry practitioners who wish to submit an abstract, key dates for abstract submissions are as follows:

- Abstract submission 1st February 2016
- Paper submission 4th April 2016
- Paper notification 30th April 2016
- Final paper submission 23rd May 2016

This year the conference chairs seek submissions from industry as well as academia to fulfil the theme of 'Cutting Edge Research meets Industry Innovation'. To facilitate this there will be an opportunity to submit abstract and presentation only and flexible attendance options as well as academic papers. If you have any questions about the program please contact the organisers who can clarify.

Glasgow's unique location provides not only the ideal industrial context for an ESREL conference, but also close proximity to the Scottish Highlands and Islands, golf courses, whisky distilleries and much more. Glasgow is a city of industrial heritage and invention. Importantly for ESREL, it is a modern city of innovation and higher education, with 3 universities and a number of industrial innovation centres, and it is a friendly and open city with a long tradition of welcoming visitors.

This will be first time since 2000 that ESREL has taken place in the UK, where it was last jointly organised by the Safety and Reliability Society in Edinburgh attracting more than 700 delegates to multiple streams over three days.

If your organisation is interested in early details about sponsorship or exhibition opportunities at the ESREL 2016, Glasgow UK or wishes to register interest, please contact the Safety and Reliability Society by email at Esrel@in-conference.org.uk or call +44 (0) 131 336 4203.

More information on submission dates and formats at www.esrel2016.org

Managing Risk, Quality and the Environment in the Global Arena

Neil Carhart

On **Tuesday 22nd September 2015** the Hazards Forum hosted an **evening event** at the Institution of Mechanical Engineers, 1 Birdcage Walk, Westminster, London.
Higher expectations for organisations mean that the bar is always being raised whilst increasing globalisation introduces much greater complexity. Maintaining high-level management systems is considered crucial including awareness of the potential for cyber-attack. Effective standards help to give a framework for consistency of approach for both large and small organisations. ISO has now introduced a common structure and text for its management systems standards. Risk based thinking and the optimum use of information is now central with, for example, a shift from an explicit need for traditional documents such as a quality manual to a broader requirement for 'documented information'.

This timely event was held to coincide with the publication in the UK of the new international standard that sets out the requirements for quality, ISO 9001. By revising ISO 9001 to this structure (often referred to as the HLS or Annex SL), organisations should find it easier to cross reference and align with the other management systems standards they might use. The new structure uses risk-based thinking throughout rather than putting risk into a separate clause. Organisations need to be resilient in many ways and recent experiences suggest that cyber-attack is a significant risk that should be considered also and thus formed an integral part of this event.
The event began with a few brief words from **Hazards Forum Chairman** Rear Admiral (retd) **Paul Thomas CB**. He thanked the Institution of Mechanical Engineers for co-sponsoring the event before introducing the chair for the evening, **Ian Joesbury**, Chair of the IMechE Management Group.

The first talk, '*Risk in quality management and the key changes and themes within the new ISO 9001'* was delivered by **Hilary Roberts**. Hilary is Global Portfolio Manager at BSI. In her talk she gave an overview of the key changes and themes within the new ISO 9001, explaining why it has changed, with a key focus on risk and opportunity. Hilary described what the standard looks like and discussed why ISO 9001 is relevant to professionals with an interest in hazards and risk management.

The second talk was given by **Professor Edward Humphreys** into the risks that confront business, government and citizens when they engage in use of 'cyber space'. Protecting business and citizen information from a range of risks as it is transported through and processed in 'cyber space' is important. Cyber security is not enough, we also need 'Cyber Resilience' - we need the adaptive capacity in our business systems to respond to the disruptive risks that plague us in 'cyber space'. Managing the risks in 'cyber space' requires a combination of information security, assurance and operational resilience. Prof Humphreys' talk outlined a strategy for achieving this.

The final talk of the evening, *'ISO 9001:2015 – What's it all about then?*' was delivered by **Paul Munday**, Business Development Manager – Training Solutions at Lloyd's Register. Paul called upon LRQA's experience in training organisations to work to the current ISO 9001. He considered how the new standard may be accommodated by an organisation that already has ISO 9001 certification.

Hilary Roberts began by asking the audience how many of them worked within an organisation that was already certified to ISO 9001, discovering it was quite a large majority. This underlines the relevance of the update to a wide range of practitioners. There are in fact over 1.1 million businesses around the world that are certified to the ISO 9001 standard.

BSI, established in 1901, is the UK's national standards body: the creator and writer of many of the leading standards. While BSI leads on British Standards, they are also involved in international, ISO, standards. BSI also helps organisations to write their own internal, private standards. They are involved in the revision of many of the key management system standards, such as ISO 14001 which deals with environmental management, and OHAS 18001, the health and safety standard. BSI operates global from offices in over 70 countries, with customer diverse in size and sector. Hilary described her position within the organisation as part of system certification group. While the groups work closely with those authoring the standards, they are more closely focused on how organisations implement those standards and what it means to be certified.

ISO 9001 last saw significantly change in the year 2000. There was an amendment in 2008, but this was considered to be a minor change, albeit resulting in a change to organisations certified to the standard. Hilary continued by exploring the motivation for the current major revision. ISO, the International Organization for Standardization, based in Switzerland, initiated the review based on a need to maintain relevance with the ways in which modern organisations operate. It is usual for major standards, such as ISO 9001, to see a review cycle of roughly ten years.

ISO publish over 20,000 standards. The committees of experts which prepare those standards are made up of representatives from over 100 nations. The development of the standards is done by consensus within the committees. The experts will bring insights and feedback from many different industries and different sized organisations, but crucially, also from the perspective of different countries. This aims to reflect they key ways in which the global context changes; and this is one of the reasons why ISO 9001 has been reviewed and amended in the way that it has.

There are several challenges arising since the millennium that mean that that the way in which the standard is structured, and the approach to its content needs to be adapted. For example, some of these challenges concern the way in which globalisation has manifested itself in the way business operate. Most citizens now think nothing of dealing with organisations in different countries and time zones. This obviously has knock-on effects into things such as price-sensitivity and the way in which the market an organisation works within fluctuates. There is much more global competition than there was a decade ago. The standards need to reflect these kinds of changes.

As a result of the 2008 recession many companies have had to restructure and implement cost saving measures. Many companies have become leaner and more agile as a result. Efficiency is now more important than ever, and driving costs down is a key part of that. The standard has been revised to enable organisations to use it to help them to achieve this, to operate in a more effective and efficient way. Organisations at all scales are more risk conscious than ever, and are increasingly concerned with their corporate reputation.

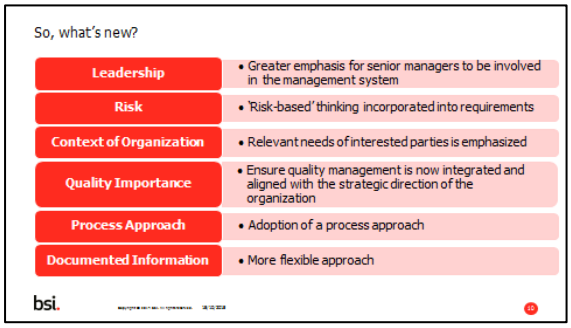
Throughout this the heart of ISO 9001 has remained consistent: making sure that quality is delivered with the customer at the forefront of thinking.

Hilary then introduced the new high-level structure for ISO 9001, Annex SL. This is one of the key changes to the format of the standard, and is common to many of the management systems standards. As more businesses have adopted different management systems standards, it has become increasingly challenging for them

to integrate and embed new standards. The management system standards come in many different shapes and sizes, with different structures and terminology. In 2012 ISO produced what is in effect a standard for standards. This provides guidance and a template to help standard writers develop management system standards in a consistent way. In ensures that all management system standards will have the same look and feel. Annex SL introduces common text and number schemes as well as common definitions. Within this structure is some degree of flexibility to account for specific contexts. This new framework allows for different management system standards to be co-managed efficiently and effectively.

Many organisations implementing ISO 14001 also implement ISO 9001, so a common approach can be very valuable for compatibility. Each standard now has ten common clause titles. This reduces conflicts, duplications and misunderstandings which improves the ease with which the multiple standards can be integrated.

There are six key areas of change within the standard that will likely have a significant impact.



There is now a greater emphasis on leadership. It has been observed that standards perform better when they align with the business strategies, therefore top level management involvement in their implementation is key. There is also an increase focus on risk-based thinking throughout the standard. Thirdly, the context of the organisation now receives greater emphasis. This can be key to embedding management systems as business improvement tools. The importance of quality is also emphasised in the standard along with the process approach (as opposed to procedures) which seeks to ensure processes are aligned to deliver desired outcomes. Finally, 'documents' and 'records' are replaced with 'Documented Information' to more flexibly meet the needs of modern organisations.

Returning to Leadership, while previous standards have assumed a dedication from the leadership to quality management systems, the new standard requires this to be more explicitly demonstrated. It sees a shift from management to management and leadership. This can help to avoid scenarios where ISO 9001 certification is obtained simply as a contractual obligation or tick-box exercise. Top management now have to make sure that the requirements of the management system are integrated into the organisation's processes and the policy and objectives are compatible with the strategic direction of the organization. This includes communicating the importance of an effective management system to all elements of the organisation from accounting to the factory floor. This includes supporting others to demonstrate its application within their specific area of responsibility. Top level management are now required to take accountability of the effectiveness of the management system and its delivery of the intended outcomes. This increased emphasis on the importance of the role of the leadership is common to many of revised standards.

Risk, or rather risk based thinking, has similarly always been implicit in ISO 9001. As with leadership, this revision makes it explicit and builds it into the whole management system. It makes proactive planning part of the strategic approach, helps identify new opportunities, and prevent or reduce undesired effects. Risk is now mentioned in clauses 4 to 10 of the standard. For example, clause 4 requires an organisation to determine the risks which can affect its ability to meet the system objectives.

ISO 31000 – Risk Management provides further specific guidance on the issue of risk. It views risk as the effect of uncertainty on objectives. The effect is any deviation from the expected and therefore can be positive or negative. The 2015 revision of ISO 9001 establishes a systematic approach to risk management rather than treating it as a single component of a quality management system. Risk based thinking, in terms of the management system, means considering qualitatively, and depending on the organisation's context, quantitatively.

Clause 4 of the standard deals specifically with the context of the organisation, and how it can grasp opportunities to move forward. Under Annex SL, all new standards which follow this structure will contain fourth clause dealing with the context of the organisation. This aims to ensure internal and external issues are considered. It seeks to identify 'interested parties' and ensures their needs are taken into account. It looks at the strategic direction of the business and what it is trying to achieve. It looks to apply risk based thinking to this.

Clause 4 ensures that the quality management system is designed and adapted for the specific organisation by providing an understanding of what it does, who for and how. The outputs of this element are used throughout the rest of the management system, so it is a very important change.

Another key theme is quality importance, which might sound like stating the obvious for the key quality management standard, but again and again though the standard this is focused on understanding that the customer wants, and what the customer will want. This means weighing up risks and opportunities. The revision aims to bring quality management and continual improvement into the heart of an organisation, aligned with the strategic direction of the organisation. The standard gives you a framework to keep assessing and ensuring that the organisation maintains the quality of the product or service it is delivering.

The next key theme is the 'process approach'. Hilary described this as looking at what happens within the business end-to-end and where it is going. It is not about drilling down into individual procedures, but rather how is the end goal achieved, and how do the departments within the organisation work together to achieve that. It is more about how the processes and procedures work together, than their individual detail. The benefits of the processes approach should be lower costs, shorter cycle times and more effective resourcing of people and materials. It can help gain trust from customers and stakeholders about the consistency of the performance of the organisation.

A final key to new area of focus is the need for 'Documented Information'. The team that created the standard recognised that not everything that makes an organisation 'good' is in a procedures manual. This doesn't mean organisations have to get rid of their quality manual if it is of benefit to them. New technologies mean very different forms of documentation may be possible or more suitable for specific purposes. It is longer about a physical ring binder of knowledge. 'Documented Information' refers to the broader suite of media. Anything that can be demonstrated to have a benefit on quality is acceptable within that suite.

Hilary summarised her talk by re-emphasising how the revised ISO 9001 places quality at the heart of the business more than it has ever done before. Risk based thinking and identifying opportunities has become more consistent throughout ever section of the standard. It is much more integrated, and its new structure means it can be more easily integrated with other standards. Finally the increased emphasis on leadership helps to drive all of this to the core of the organisation.

Professor Edward Humphreys began the second presentation of the evening,

'*Cyber (Risk, Security and Resilience)*' by posing the question: Is cyber security enough? It is something we hear about all the time in the press, but should we really be looking at cyber resilience, something raised recently by the Word Economic Forum.

The term 'cyber' is used all the time, perhaps too often without reflection on what it really means. An early modern interpretation was given by the influential author William Gibson, who coined the term 'cyberspace' in the 1980s, defining it as: "A consensual hallucination experienced daily by billions of legitimate operators, in every nation ...". Again in the 2000s he reflected on whether it was just a buzzword.

So what does cyber security actually mean? Only 10-15 years ago conferences were called IT security or information security events, today our conferences are called cyber security conferences? Is there any difference? Is the intent and content the same or different? Is there an internationally agreed definition for 'cyber security' that the world's experts and security community have arrived at by a process of consensus? Is it a useful term to use or is it just a buzzword?

The word 'cyber' finds its origins in Ancient Greek. Many ancient writers used the term to mean leading, steering, and governing. As Professor Humphreys explained, Plato, in *The Republic*, uses the term in relation to steering and governing the "ship" of nation state. There is something appealing in this broader definition and usage that goes beyond the idea of 'cyber' being synonymous and interchangeable with IT networks and systems.

Based on this original meaning perhaps one of the greatest cyber-attacks of all time was in 480 BC, the Battle of Salamis. The Persian Empire was threatening Ancient Greece, resulting in a naval battle around the island of Salamis, which is situated near the port of Athens. The Greek navy won the battle through intelligent cyber strategy and risk management policy and what could be described as effective cyber leadership and governance.

Professor Humphreys used this original notion of 'cyber' to propose that the cyber problem was one of governance, leadership and management in dealing with the risks and opportunities in today's digital world. Managing cyber risks goes far beyond risks in the IT sense, but risks involving managing people, processes, information and physical objects. Furthermore, it is about governance and everything this entails in terms of leadership commitment, policy, strategy, etc. A third aspect of the cyber problem is its relation to resilience: managing the capacity to adapt. In the Battle of Salamis the Greek navy were able to regroup, adapt and respond to the challenges they faced.

The use of the Internet has grown. Many years ago it was only used to connect things like PCs and mainframes. We have been through a period of increasing mobile and societal connectivity leading to more things being added to the Internet, such as mobile devices and social media. This has continued apace, but increasingly, the things being connected to the Internet are not limited to computers or computer-like devices. We are now seeing smaller and smarter things connected to the Internet – the age of the Internet-of-Things. These smart things are becoming the basis of smart infrastructure, cities, buildings, utility systems, connect to, and rely on, the Internet. Looking at the future, the conversation is moving more and more towards the discussion of "smart" things and the connectivity of these things to provide lots of business and societal opportunities in sectors such as healthcare, environment, energy and transport. This expands the 'cyber' concept to include cyber physical things. Along with the large scale smart infrastructure, encompassing the smaller scale Internet-of-Things, there are other technologies such a Big Data, sensor networks and the 'cloud' that together bring a variety of cyber opportunities and

benefits to business and society.

These all present opportunities to do business in new smarter ways and play in the ways we want to play. They can make our world smarter: our buildings, environment and transport systems. All of these opportunities also come with risks and impacts. In the 'cyber' world of the biggest cyber risk is people: how the users behave and act in cyberspace but also risk related to information, operational, system and reputational risks. Businesses can lose their reputation overnight if their systems are compromised or are seen to be vulnerable.

The standard ISO 31000 defines risk in terms of the effect of uncertainty on objectives. This definition can be thought of as the combination of the impact of a cyber-attack and the likelihood of that cyber-attack occurring. In the security and privacy domain there are many things that could cause a cyber related event to happen such as people hacking into systems, processes going wrong, systems failing or external environmental hazards. When a cyber-attack will happen and how likely it is to happen we generally do not know. We need to estimate when it will happen, along with identifying the potential impacts. Damage, losses and harm to information, systems, resources, physical assets and reputation, theft and fraud these are some of the impacts of the cyber-attack being successful.

If a cyber-attack is happening or is about to happen, the focus must shift onto how the organisation can respond and recover, and how organisations should adapt to survive cyber-attacks. Professor Humphreys referenced Charles Darwin on this subject – 'it is not the strongest of the species that survives, nor the most intelligent, rather it is the one that is most adaptable to change'. Change is inevitable. We must accept that systems and processes need to be able to respond and adapt to this change.

ISO 22300 defines resilience as the adaptive capacity of an organisation in a complex and changing environment. This is all related to disruptive risk and the ability of an organisation to manage it. Cyber resilience is the adaptive capacity of an organisation to return back to normal operational state after a major disruptive risk caused by a cyber-attack. How can an organisation anticipate the disruption and adapt to events? The cyber attacks may be simple but still catastrophic. How can an organisation address the combined issues of security, preparedness, risk and survivability? How can an organisation maintain its functions and structure when faced with internal or external changes or threats? All of these things are important in looking at what cyber resilience actually means and how an organisation can actually deal with it.

The World Economic Forum defines *cyber resilience* as the ability of systems and organisations to withstand cyber events, measured by the combination of mean time to failure and mean time to recovery.

Having established the concept of cyber resilience, Professor Humphreys then turned to look at supply-chain resilience as an example. A manufacturer may have various supply chains, overseas and domestic. Supply chains are now using IT based supply chain and logistics management systems. There may be risks of disruption at any part of that supply chain. There is a question as to how we build cyber resilience to counter cyber-risks in regard to supply chains. There are many examples of supply chain disruptive risks around the globe. Following the serious floods experienced by Thailand in 2011-2012 many companies in the automotive, electronics and hi-tech sectors suffered serious impacts, involving supply chain problems and disruptions. This is just one example of where cyber risk: physical, management and technical risks - point to the need for cyber resilience.

There are many standards that can be used together in order to build organisational and cyber resilience. ISO 31000 deals with risk management, while others deal with business information security management, continuity, operational resilience and emergency management. ISO/IEC 27001 is a management system standard that deals with information security. It embraces all of the necessary elements to implement an effective, adequate and suitable information security risk management process. It allows organisations to govern (as per the original meaning of cyber) their information security risks. As all management standards do, it also enables organisations to adapt to change through continued improvement.

It is all very well defending against possible attacks, but there also needs to be consideration of how to respond and return from disrupted systems and services in the shortest possible times. Some things will inevitably go wrong, and when they do, thoughts will turn to response and recovery. The easiest option may be to do nothing and let the service naturally return to pre-disruption levels if it can. This could be disastrous for any company. There has to be some thought to how the period of disruption can be reduced with the minimum of impact. Fortunately, there are standards and specifications, which outline how to achieve this and build in resilience. For example, building cyber resilient systems can be assisted by integrating and implementing together a number of standards: ISO/IEC 27001), with Information Security Incident Management (ISO/IEC 27035), Business Continuity Management System (ISO 22301) and ICT Readiness for Business Continuity (ISO/IEC 27031) among many others.

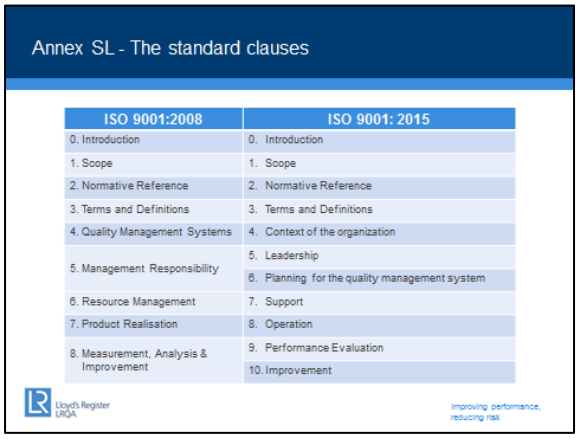
Professor Humphreys summed up his talk by arguing that 'cyber' is all about governance and management of cyberspace and cyber risk. Attacks will happen at some point in time, so cyber resilience is critical. The world is growing more and more towards smarter Internet connectivity and smarter cyber risks and opportunities: smart things, technology and future smart infrastructures all connected across the Internet. Cyber resilience is about adaptation to change and the ability respond and to recover from disruptive risks. Survivability is all about adaptation to these changes. The future cyber business agenda is about executive leadership, governance, responsibility and accountability. The cyber agenda requires multi-stakeholder initiatives, partnerships and information sharing. An integrated approach to risk management should also be part of the future cyber business agenda.

The final talk was given by **Paul Munday** from Lloyds Register Quality Assurance who began by reflecting on Hilary Robert's earlier talk, and how he aimed to build on this by discussing some further practical ways in which ISO 9001:2015 could be implemented.

Within any ISO standard there is a degree of interpretation. It is about each organisation applying it in a way that works for them, and a way in which they can achieve ownership of the applied process. While the standards are drawn from best practice, each company applying it will best understand their own context and unique qualities. While outside guidance can be advantageous, it requires the knowledge from within the organisation.

Under Annex SL clauses 0 to 3 remain the same, but the others have seen some changes. This is now the common terminology and framework that will

eventually be seen across all ISO standards.



Paul focused his talk on Clause 5, Leadership. This does not necessarily mean that the organisation's CEO becomes responsible for the Management System. In some smaller companies, this might well be the case, but this is not what is meant by Leadership in this context. Many people ask whether leadership here refers to the leaders of business functions or departments. The management representative is still needed. The person who sits at the top is responsible and accountable, but the day to day running is still linked in to the person running the Quality Management System, the Environmental Management System and so on. These people are still required, but there is more pervasive emphasis in the standard on the leaders taking ownership. This new emphasis requires consideration of how the management system actually aligns with the business objectives, and the context of the organisation. This is a challenge moving forward. If it is possible to get alignment with the business objectives then it will overcome the problem of quality being seen as an add-on and not a fundamental, embedded element. Ultimately a more joined up approach will lead to better products and services and happier customers.

Clause 6 deals with planning, and the management of risk and change. As discussed by the previous speaker, risk is used in many different ways. Risk in the IT community may be interpreted differently to health and safety risk. Risk, in the context of ISO 9001, means looking at the opportunities within an organisation. This can include getting a better understanding of customers, better planning and better preparation. As discussed earlier, risk based thinking, something which is often done automatically or sub-consciously is built into the whole management system by ISO 9001:2015. Whereas it may have been implicit before, it has been made explicit.

The standards are international, but the cultural approach to risk and other operations vary across the globe. It is not necessarily right or wrong; it is about understanding the political, social and economic context of the organisation. The system can help to understand these contexts and better manage the risks of doing business across the different socio-political environments. This might mean looking at an organisation's international offices, or global supply chains. Simple models and tools related to the implementation of the standards can help harmonise thinking internationally. The simpler the management system, the more likely it is to be understood and to be effective. The simpler the management system, the easier it is for people across all levels of the business to understand how it is relevant to them, and not just something operationalised by a particular group within the organisation.

From the leadership and planning perspective, how do you take the necessary messages across the business so that everybody knows what quality means to them? They may all have different perspectives. Communication is key to achieving this. This also emphasises the importance of keeping the quality manual. It can help with this communication.

Taking a process approach means cutting across organisational silos. Embedding a risk based approach can help overcome any issues this may present.

Customer focus is central, regardless of what part of the business you work within.

ISO 9001:2015 supports this by ensuring quality cuts through the quality management system.

While there are changes to the standards, many companies are already doing the things the standards require of them. While changes can cause concern, in practice they may not be onerous. It is a case of aligning current operations with the standards. ISO 9001: 2015 presents an opportunity to revisit the systems and refresh them. For many, the tools and process they already use will be relevant to the application of ISO 9001:2015.

Paul concluded is talk by revisiting the significance of the key changes to ISO 9001, and how these manifest as practical implications for an organisation. It is very much dependent on:

- An organisation's contextual circumstances
- The maturity of the existing QMS
- The level of involvement from top management
- The approach to risk management
- The use of a process based approach.

The chair thanked the speakers before opening the floor to **questions from the audience**. The first question highlighted how many of the changes seemed to relate to doing things in a more holistic way. Many within the major hazards industry see the real goal as not seeing safety and quality as being separate types of risk. Excellence can be supported by binding it within a culture of excellence. The question then is: how much more difficult is it going to be to assess for ISO 9001 certification against the softer issues, such as leadership, and more holistic approach that is coming through in the revision?

Paul Munday responded by reflecting on the conversations he had had with those transitioning to ISO 9001:2015, and with those responsible for awarding certification. These areas of increased interest have to be examined and assessed through the KPIs and measures. The auditors will examine these KPIs and bring them to the attention of the leadership team if they feel there are issues with quality or they are not providing appropriate indication of performance against these softer issues.

The second question related to standards on resilience, in particular BS 65000. This looks at resilience at a strategic and operational level, and calls for coherence between different areas and risk disciplines. The audience member asked the panel how they see the standards and changes discussed in the presentations as helping or hindering the achievement of coherence.

Hilary Roberts acknowledged that this will increasingly come to the forefront of increasing organisational resilience. It is something that is very high on the agenda within the standards community and will be taken account of moving forward.

Professor Humphreys highlighted the ISO standards which also deal with security and resilience. The British Standards provide inputs into the ISO technical group responsible for the ISO standards relating to resilience, helping to achieve coherence and best practice. There are many other standards being developed in this area at the ISO level, and coherence is an area of focus.

Paul added that each organisation can build on the standards to ensure they work in their specific context. If the British Standard is used by ISO then it will be brought in line with the Annex SL format, but an organisation could tailor the exiting BS standard in this way for coherence with the ISO standards should they wish.

The third question asked how ISO or LRQA evaluate the benefit of introducing new standards. Clearly there is a cost associated with changing and implementing the standards. How are the benefits assessed and how is the learning from the process captured to improve the next change?

Hilary replied that the benefits will be assessed based on the performance of a certified organisation rather than in more general terms to the standard itself. Monitoring the benefits experienced by a certified organisation as a result of implementing the standards can be difficult. It is not always possible to arrive at a quantitative assessment, particularly in the short term. The standards can take some time to embed in the organisation. It is possible to observe what organisations expect to get from applying the standard at the start of their journey. They may identify a particular suite of KPIs they expect to see change as a result. One or two years later these can be measured to get some indication as to whether there have been positive changes in line with expectations.

Professor Humphreys added that there needs to be a reasonable justification for revising a standard. This process involves getting feedback on the existing standard. A justification study is needed for entirely new management standards. In both cases feedback is taken very seriously. Public consultations are often undertaken which enables anybody to respond and provide feedback with regards to the standard and the implementation processes. The review and renewal process can take several years.

Ian Joesbury brought the event to a close by reflecting on the excellence of the three presentations. He highlighted five words which he had identified through the talks and discussions as being of key importance. The first is '*commonality*', not just within a company, but to improve transactions of all sorts between companies. The use of common terminology and standards between organisations in a supply chain will help remove a lot of waste. The second is '*process driven*'. Functional boundaries present a big risk of disruption of organisations. Focusing only on process within a function have stopped organisations delivering efficiently. A further key point is '*risk management*' which is now at the forefront of business operations. Embedding it in quality management is fundamental. All of the speakers talked about '*leadership*' and the dangers of not having the effective leadership from the top. It is about setting the tone for the whole organisation. The final key point is to remain '*customer orientated*'.

Ian concluded by thanking each of the speakers, the audience for their participation and those from the Hazards Forum who helped to organise the event.

The Hazards Forum Chairman Paul Thomas closed the event by thanking Ian and the events sponsors, before inviting all those in attendance to continue their discussions over refreshments.

.

Parliamentary and Scientific Committee

The latest issues of "Science in Parliament", the journal of the Parliamentary and Scientific Committee of which the Hazards Forum is a member, has among its contents the following articles. Any member who would like any further information on any of the articles below should visit the PSC website www.ScienceInParliament.org.uk

INNOVATION HUBS	Professor Sa'ad Medhat
INCENTIVE PRIZES AND THE ADVANCEMENT OF SCIENCE AND TECHNOLOGY	Paul Ridout
ECOLOGY MATTERS	Ben Connor
150 YEARS OF THE STATE VETERINARY SERVICE	Dr Alison Wilson

FOOD AND THE FUTURE	Veronica Vaccari
THE UNIVERSITY OF NOTTINGHAM INSTITUTE FOR AEROSPACE TECHNOLOGY	Professor Herve Morvan
THE FUTURE OF ROAD TRANSPORT	Address to the P&SC by Lord Borwick, Rob Wallis and Steve Yianni
THE BIG DATA OPPORTUNITY	Hetan Shah
BIG DATA IN NEUROSCIENCE	Professor Mark Stokes and Nicholas Myers
THE COLD TIME BOMB	Professor Martin Freer and Professor Toby Peters
GALLIUM NITRIDE FOR SAVING LIVES, ENERGY, CARBON EMISSIONS AND MONEY!	Address to the P&SC by Professor Sir Colin Humphreys
NANOTECHNOLOGY	Address to the P&SC by Professor Andrew Fisher, Professor Milo Shaffer and Professor Alex Orlov
COMBATING ANTIMICROBIAL RESISTANCE	Dr Lindsay R Chura, Elizabeth Hogben and Stefania Di Mauro-Nava

The Hazards Forum Executive Committee

The Hazards Forum Executive Committee is responsible for the management, finances, policies and overall direction of operation of the Forum. The members of the current Executive Committee, showing professional qualifications and honours, are:

Chairman: **Rear Admiral (retd) Paul Thomas** CB FREng FCGI CEng FIMechE HonFNucI HonFSaRS

Mr Brian Wimpenny CEng FIMechE

Mr Dave Fargie CEng FIChemE

Dr Luise Vassie FInstP CFIOSH

Mr John Armstong CEng FIMechE

Mr Ian Wright CEng MICE MIStructE FCIArb QDR Barrister at Law

Dr Owen Keyes-Evans MFPHM MFOM FRSA

Mr Andrew Buchan CChem MRSC FSarS MIFirE

Prof William Bardo FREng HonFInstMC FIET FInstP FPhysSoc **(RAEng Observer)**

Lord Julian Hunt FRS HonFICE FIMA FRMetSoc **(Royal Society Observer)**

Prof Andrew Curran FSB FCMI Hon FFOM **(HSE Observer)**

Dr Mark McBride-Wright CEng MIChemE **(Observer)**

Secretary: **Mr Brian Neale** CEng FICE FIStructE HonFIDE

More information about the structure and mission of the Hazards Forum can be found on the Forum's website: www.hazardsforum.org.uk

The website also contains a great deal of useful information on the benefits of becoming a member of the Hazards Forum along with details on how to become a member, interesting articles, a calendar of events and previous issues of the Hazards Forum Newsletter.

From the Secretary…

Members are asked to note that the **2016 AGM** is scheduled for Tuesday 22nd March and to attend if possible, when they will be made most welcome. The AGM is to begin at 16.30 and to be held at the usual venue of One Great George Street, Westminster. A formal notice will be sent to members early in 2016. An evening event will follow as usual. As advance notice, the **next Evening Event** after 22nd March is being planned for 14th June.

Brian Neale

Calendar of Events

Please check the Events section of the Hazards Forum website for more information at **www.hazardsforum.org.uk** and to see any updates in the calendar. These may include additional events or perhaps amendments to the Events shown below. Attendance at Hf events is by invitation, as usual.

Date	Event	Venue	Contact/further information
December 2015			
9th- 10th	ICE Event: The Civil Engineering Triennial Summit 2015	Institution of Civil Engineers, One Great George Street, Westminster, London, SW1P 3AA	https://www.ice.org.uk/events/
10th	SaRS Event: Human Error	Birchwood Golf Club, Warrington WA3 7PB	http://www.sars.org.uk/branches/the-north-west-branch/
January 2016			
19th	SaRS Event: Standardisation for the Safety and Reliability Sub Sea Gliders	BMT RCL, Hampshire, PO15 5SU	http://www.sars.org.uk/branches/solent-branch/
20th	ICE Event: Alternative Disruption Resolution	Institution of Civil Engineers, One Great George Street, Westminster, London, SW1P 3AA	https://www.ice.org.uk/events/
26th	SaRS Event: The Human Factors of Violations in Systems Safety	BAWA Leisure Centre, Bristol BS34 7RG	http://www.sars.org.uk/branches/western-branch/
28th	IET Event: My wireless network is secure, right? Right?!	Bargeman's Rest, Little London Quay, Newport, Isle of Wight, PO30 5BS	http://www.theiet.org/events/local/225028.cfm?nxtId=230203
February			
3rd- 4th	IET Event: Cyber Security for Industrial Control Systems	IET London 2 Savoy Place, London WC2R 0BL	http://conferences.theiet.org/cyber-ics/index.cfm?nxtId=225125
9th	SaRS Event: The Queen Elizabeth Aircraft Carrie – An Electric Ship	BMT RCL, Hampshire, PO15 5SU	http://www.sars.org.uk/branches/solent-branch/
23rd	SaRS Event: Safety/Risk and Climbing Mountains	BAWA Leisure Centre, Bristol BS34 7RG	http://www.sars.org.uk/branches/western-branch/
24th	IET Event: Cyber Security for Urban Transport	IET London 2 Savoy Place, London WC2R 0BL	http://conferences.theiet.org/secure-transport/index.cfm?origin=events-carousel
March			
1st	IET Event: Functional Safety Made Easy	Shrewsbury College of Arts & Technology, London Road, Shrewsbury, Shropshire, SY2 6PR	http://www.theiet.org/events/local/206486.cfm?nxtId=224752
15th	SaRS Event: ISO55000	ATKINS Aldershot GU11 1PZ	http://www.sars.org.uk/branches/solent-branch/
16th	IET Event: Critical Infrastructure Security	Bearsted Road, Maidstone, ME145AA	http://www.theiet.org/events/local/228994.cfm?nxtId=226727
22nd	Hf Event: Annual General Meeting	Institution of Civil Engineers, One Great George Street, Westminster, London, SW1P 3AA	admin@hazardsforum.org.uk
22nd	Hf Event: Infrastructure Resilience (Provisional Title)	Institution of Civil Engineers, One Great George Street, Westminster, London, SW1P 3AA	admin@hazardsforum.org.uk

The Hazards Forum's Mission is to contribute to government, industry, science, universities, NGOs and Individuals to find practical ways of approaching and resolving hazard and risk issues, in the interests of mutual understanding, public confidence and safety.

The forum was established in 1989 by four of the principal engineering institutions because of concern about the major disasters which had occurred about that time.

The Hazards Forum holds regular events on a wide range of subjects relating to hazards and safety, produces publications on such topics, and provides opportunities for interdisciplinary contacts and discussions.

The Hazards Forum
One Great George Street
Westminster
London SW1P 3AA

E-mail: admin@hazardsforum.org.uk
Telephone: 020 7665 2230
Fax: 020 7799 1325

Website: www.hazardsforum.org.uk

Registered charity number 1047047