Hazards Forum News

No.100 – Spring 2019

Welcome!

For all your news, views and events

In HFN #100, we present notes from the September 2018, December 2018 and January 2019 Hazards Forum events, together with a reflection on the Hazard Forum lecture at the ICE Global Engineering Congress in October 2018. RSSB's Greg Morse also looks back to the Clapham rail accident of 1988 and its implications for corporate memory retention. There's also our usual news round-up and a calendar of forthcoming events.

Contents

Click to navigate...

In the news

Global Risks Report 2019

The Global Risks Report 2019 - 14th Edition is now available in both Executive Summary and full report formats. The report, produced by the World Economic Forum in a partnership with Marsh & McLennan Companies and Zurich Insurance Group, asks: 'is the world sleepwalking into a crisis?' It considers that global risks are intensifying, yet the international collective will to tackle them appears to be weakening, and divisions hardening. The report, structured around eight well-researched papers, suggests that rising geopolitical and geo-economic tensions are the most urgent risks in 2019, and the main blocks to making collective progress on other global challenges.

Environmental risks continue to dominate the annual Global Risk Perception Survey (GRPS). With domino affects impacting biodiversity, health and socio-economic development.

The race of evolution of **cyber and technological threats** present blind spots, the report highlighting that we still do not fully appreciate the vulnerability of networked societies.

Human vulnerability to **rising sea levels** due to rapidly growing cities in coastal regions is a concern. An estimated 800 million people currently live in 570 coastal cities that would be vulnerable to sea-level rise of 0.5 metres in 2050.

A **future shocks** section considers ten potential sudden and dramatic breakdowns. Some are more speculative than others, yet some build on risks that have already begun to crystallise. These are more 'what-if' scenarios, not predictions, but provide powerful food for thought regarding the need to think creatively about risk and to expect the unexpected.

It comes as no surprise that the Hazards Forum in 2017 identified three strategic themes of Emerging Technologies, Natural Hazards & Socio/economic/political developments to direct a future portfolio of activities, which have been reflected in more recent seminars.

IChemE Accident Database archive now available online

The IChemE Accident Database archive is now publicly available free of charge. It has had a number of launches and revisions since the 1990s, and was last updated in 2000. The Deputy to the Director, IChemE Safety Centre, has advised that whilst *"…there are no plans to update or relaunch the database but we thought it important to preserve the data and make it accessible to everyone…"* The database of over 10,500 records is available in PDF format, and searchable via basic Adobe functions. The data is broken up into various categories, including: activity; causes; consequences; equipment and substances.

Whilst it is regrettable for hazardous industries that a reliable, live and current process incidents database remains elusive, the value of the archive should be recognised, as it provides a further aid to any process hazards analysis exercise, a resource to newcomers to the processing industries, and a refresher to experienced persons regarding what can go, and has gone, wrong.

CSB highlights a common thread between two Oil Refinery Losses

The CSB has highlighted potential common causes between a refinery explosion and fire in Wisconsin, USA on 28 April 2018 and that of refinery explosion in California on the 18 February 2015. Both incidents occurred on the same type of unit, a Fluid Catalytic Cracking Unit (FCCU), and both occurred following misplaced reliance on an operational slide valve during a plant shutdown, which allowed hydrocarbons and air to mix, and subsequently explode. Whilst there are clearly major differences between the two incidents, both highlight the need for greater barrier integrity awareness when managing major accident hazards.

In the oil & gas drilling industry, there is a general widespread practice of having two independent barriers at all times to avoid well control incidents, although this is not practiced uniformly across the hydrocarbon processing industries, and is not always provided by design. These two losses also draw attention to the gap between the level of process hazard analysis when a plant is at steady state, and that provided when the plant is in a non-routine operational mode (such as shutdown or start-up).

Gasoline pipeline deaths

The Mexican authorities have blamed fuel thieves for the tragic chain of events that led to the deaths of at least 79 people in Tlahuelilpan on 18 January 2019. The explosion occurred after the fuel pipeline had been illegally 'tapped', which sent a jet of refined gasoline into the air. Locals flocked to fill containers with the spilt fuel, before the spill ignited a couple of hours later. Fuel theft of this kind is widespread in some Mexican communities, with government sources estimating the practice costs the country US$ 3 billion annually, with 12,581 illegal taps seen in the first 10 months

of 2018. Regional poverty, and a lack of reliable supplies, are the more obvious reasons why the problem is so prevalent. However, it has (in itself) generated shortages, as fuel manufacturers and distributors have resorted to shutting down some pipelines completely, and supplying some regions by road tankers alone.

The government has pledged to come down harder on fuel theft, and is planning for the greater protection of pipelines, although until this can be introduced, supplies remain disrupted as distribution moves from pipelines to tankers.

Nigeria has also suffered for years from an epidemic of pipeline attacks not just on finished product, but crude oil also, which in turn has led to illegal local refining and large-scale illegal bunkering. Such activity has in turn led to a number of tragic accidents with high death tolls. An incident on 18 October 1998, attributed to illegal tapping, led to the deaths of over a 1,000 people.

CCPS Safety Beacon – February 2019

The February 2019 CCPS monthly Safety Beacon, refers to a 1999 Alumina Processing Incident in Gramercy, LA, USA. The incident occurred after safety critical instruments and equipment (including a high-pressure interlock and a relief valve) had been bypassed and disabled in the name of 'PRODUCTION FIRST'. The plant had experienced operational issues arising from poor plant design leading to operational compromise to keep the plant on line before.

Wittingly or otherwise, Plant Management had 'endorsed' this behaviour by not doing anything about the design, and resulting in a situation of *'normalizing the abnormal'* or, alternatively, the management *'got the level of safety they demonstrated they were prepared to accept'*.

Thankfully cases of isolated relief systems are rare, although there is knowledge of one major loss in the hydrocarbon processing industries in 2018, where an isolated relief system led to vessel rupture and widespread damage.

Control over, and management of, safety critical equipment is quite rightly of great priority to industry in general, and in an ideal world it should not be possible to compromise the integrity or operation of a safety critical device. Yet we do not operate in an ideal world, and operators are routinely faced with decisions on the need to operate without or with an impaired safety critical feature. Systems need to be in-place that formally justify continued operations in such a position, supported by risk assessment and identification of other barriers in place to mitigate (sometimes in part only) the loss of a safety critical function.

Designers, licensors and operators have a responsibility to ensure that designs are safe, and ideally inherently safe (i.e. **building safety in**). Where inherent safety cannot be achieved, passive and then active hardware features should be considered, and as a last resort reliance on procedure and human action (these all being examples of **building safety on**). There is then a responsibility to ensure these 'built on' safety critical features are available and working, and when they are not (this should be seen as rare exception) that it is carefully managed, with high levels of awareness at a site level, and clear guidance for when a situation is not going to be tolerated by management and the plant shutdown. Situations were safety critical equipment is bypassed or impaired should also be highly visible to the site management team, and routinely reviewed at director level.

Back to top

An evening with…

Cyber Security: Implications for High Hazard Industries, IET, 18 September 2018

Cyber Security & Safety Critical Systems

Cyber-attack poses a growing threat to the security and therefore the safety of infrastructure in Great Britain, including high hazard industries. Expert opinion and research suggest that cyber systems are likely to contain vulnerabilities through insufficient protection.

This emergent and rapidly developing threat poses challenges in a number of areas, such as:

- How we assess and regulate cyber risks and responses
- How we integrate well developed elements of high hazard risk assessment with cyber response measures
- How we assess cyber risks as part of insuring a broader portfolio of risks

This Hazards Forum event drew expert speakers from a range of sectors, who addressed these issues from direct and practical experience. It was chaired by Andrew Buchan of Sellafield Ltd, in his role as President of the Safety and Reliability Society and member of the Technical Advisory Committee of Hazards Forum.

All the speakers and the chair came from organisations associated with Hazards Forum, which highlights the capabilities and interests across the wider Hazards Forum group. The event had 40 booked delegates and there was extensive opportunity for discussion and questions both during and following the event. The presenters and their presentations are summarised below.

Colin Griffiths has been with ONR since 2012, where he is the CS&IA specialist for nuclear new build and leads CS&IA for ICS cyber security. Over the last few years, he has been fostering a closer working relationship with Control & Instrumentation engineers both to gain an understanding of Industrial Control Systems and share learning from conventional IT networks.

Formerly of the Royal Air Force, where he gained experience in Physical, Personnel, Air Transport, Information & Computer Security, Counter Intelligence and Law Enforcement, he holds an MSc in Information Security from the RHUL, CISSP and GICSP certification.

Colin introduced the context to Nuclear Regulation highlighting:

- Nuclear Industries Security Regulations (NISR) 2003
    - Theft and Sabotage of Nuclear Material or other radioactive material
    - Non-proliferation of enrichment technology
    - Compromise of Sensitive Nuclear Information
- Nuclear Installations Act 1965
    - Licensing nuclear installations and operations
    - License conditions in the interest of safety
- H&S at Work Act 1974

    - Conventional H&S on nuclear licensed sites
- Networks and Information Systems (NIS) Regulations 2018
    - Essential services that play a vital role in society
    - Operators of Essential Services
- You cannot have safety without security
- Security can impact the reliability or availability of systems by either the lack of, or over restrictive security controls

An overview of the transition to Security Assessment Principles (SyAPs) from the Nuclear Industry Security Regulations 2003 was given, along with the framework of the SyAps. Moving from a prescriptive framework to a more outcome focus regime allows duty holders to develop and justify appropriate arrangements. Duty holders should maintain arrangements to ensure that CS&IA risk is managed effectively. Inspectors should also consider:

- Is the risk assessment methodology appropriate for the size and scope of the organisation?
- Is it operated by suitably qualified and experienced personnel?
- Is it auditable?
- Does the risk assessment consider risks from partners and supply chain companies?
- Is there a threat assessment informed from relevant sources and does it cover the correct scope?

Colin highlighted a number of widely available risk assessment methodologies that can be used as the basis for the duty holder risk assessment and these include:

- ISO 27005:2011
- IEC (ISA) 62443-3-2 Security risk assessment and system design
- US National Institute of Standards and Technology SP 800-30
- Octave Allegro
- Information Systems Audit and Control Association: Control Objectives for Information and Related Technologies 5
- Information Security Forum – Information Risk Analysis Methodology
- Open Group FAIR Risk Analysis Standard
- IS 1&2
- SE Operational Guidance 86

ONR Regulates Cyber Security by:

- Use of cascading sets of Principles and Guidance documents
- Clearly defined set of outcomes
- The Claims, Arguments and Evidence made by a duty holder that the outcomes have been achieved, it is effective and audited

- The regulatory judgements and decisions made by ONR inspectors based on their skills and assisted by the guidance documents
- Some prescription – Classification Policy

Ongoing Assurance requires:

- ONR (CNS) Inspections for adherence to the plan
- Effective internal assurance and audit activities
- Use of external auditors to validate internal audits
- Use of external auditors to fill skill gaps in internal audit

James Amende is the Human Factors Development Manager at Corporate Risk Associates and has worked in Engineering Consultancy for over 30 years, Human Factors being his primary focus for over 20 years. His business development experience has been gained in many sectors, including defence, rail, nuclear, shipping, airports & air traffic management, medical devices, built environment, consumer goods and retail. James contributed to the development of Human Factors into a more broadly recognised and valued business discipline whilst Co-founder and MD of the world's largest human factors consultancy. He has extensive experience in varied safety and risk management consultancy services in APAC, Middle East and Europe. He has recently been actively involved in developing cyber security based services at CRA, including supporting the R&D projects described in this Hazards Forum presentation.

The UK's Civil Nuclear Security Strategy in February 2017 identified cyber-attacks and blended attacks as a major concern for the UK's civil nuclear industry. In addition, 75% of large and 32% of small organisations have suffered cyber security attacks due to human error. HRA (Human Reliability Assessment) tools have long been successful in understanding and reducing human errors for operational tasks in the nuclear industry. CRA has been awarded a grant from Innovate UK, the UK's innovation agency, to research the applicability of HRA tools for understanding, quantifying and managing human error in cyber security for nuclear facilities. This research includes undertaking task analyses at Cyber Security Operations Centres (SOC) to understand the key steps involved in scanning for and responding to cyber threats. The research aims to deliver a quantitative analysis tool which will provide a basis for assessing the reliability of cyber security defences in response to a cyber attack.

Specific areas will consider the use of Human Reliability Assessment tools (HEART) in a cyber context, identifying some generic error producing conditions and appropriate performance shaping factors taking into account conditions with a Security Operations Centre environment. Another area of work will be to consider current human reliability data collections being undertaken internationally from modern digital control room environments. A further stream being considered is the use of STAMP type process (Systems-Theoretic Accident Model and Processes developed by MIT). This technique utilises system theory to analyze accidents, particularly system failures (particularly involving processes above component level). In this conception of safety, accidents occur when external disturbances, component failures, or dysfunctional interactions among system components are not adequately handled by the control system, that is, they result from inadequate control or enforcement of safety-related constraints on the development, design, and operation of the system.

By use of these different techniques CRA hope to develop new understandings and risk evaluation and reduction tools, which will be useful in the field of Cyber Security.

John Munnings-Tomes, is the Chief Risk Engineer at Navigators, and he is a Chartered Chemical Engineer, Registered Safety Professional and a Fellow of the IChemE. He has extensive experience in the petrochemical and insurance sectors, having worked with Fluor Daniel, Chevron and Marsh in several senior risk engineering roles. He is a trustee of the Hazards Forum and a committee member of the IChemE Safety and Loss Prevention SIG. He is a representative on several oil & gas insurance market risk engineering forums.

Navigators specialise in provision of insurance within the oil and gas sector and have over 1.3 million insured across 350 different industries. The need for cyber security within the energy market is driven by an increased reliance on (now digitised) industrial control systems, client awareness and demand, and an increased understanding that it is a coverage need which clients require and that insurance providers have to understand and provided competitively.

John highlighted the need for a good understanding of cyber safety as a starting point to determine cyber security vulnerabilities and potential losses. Over the last 15 years, many insurance policies have excluded losses arising from cyber attack events or have limited cover to specifically identified items. The more recent increased awareness of cyber vulnerabilities has driven a deeper understanding of possible events which may lead to a loss.

A minimum set of objectives is required around limiting system and device access, configuration control, detection of abnormal events and system recovery. Once these basics have been assured a more detailed risk assessment processes can be used depend on the level of cover required. The basic underwriting activities will then take account of policy, design, risk management processes, training, emergency response and audit information. Guidance has been produced by the Lloyds Market Association in a publication Cyber Security & Safety Considerations For Oil, Gas & Petrochemical Risk Assessment. Specialist third party software product and specialist consultancies can evaluate the extent of threat posed to an insured party based on an understanding of susceptibility to an attack and motivation for an attack.

However, field observations are extremely important in evaluating cyber security understanding of staff, overview and oversight of systems and specific issues around third parties supporting industrial control systems or other systems which may be connected.

In conclusion, John emphasised that from an industrial property insurance perspective cyber safety is a sub set of process safety and is based around controlling major accident hazards. Process, risk and control system engineers need to have a mutual understanding of what severity of event is possible, and the resulting consequences. It was highlighted that cyber risk should be managed as part of an overall risk management process.

Back to top

Structural fire resilience

How we are getting it wrong and why – a lecture given by Professor Luke Bisby at the ICE Global Engineering Congress on 24 October 2018

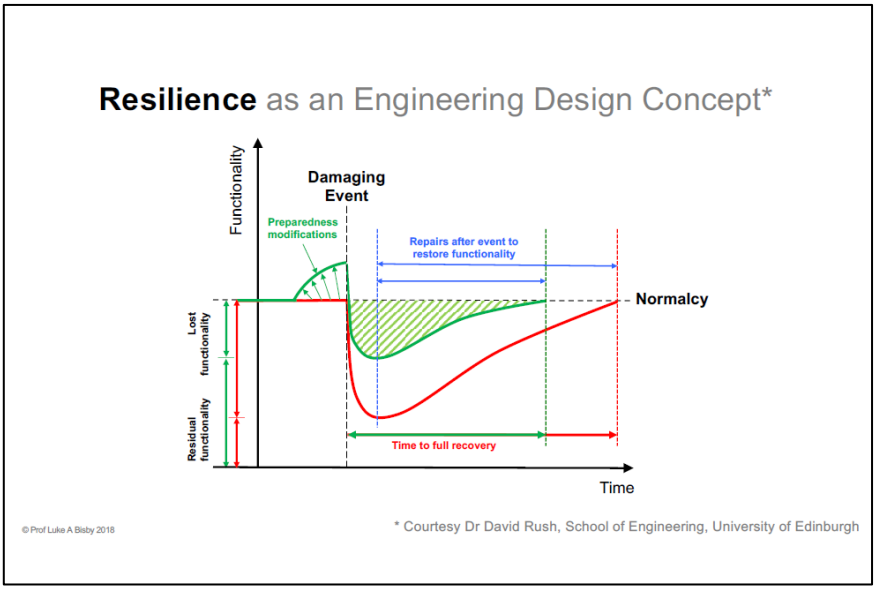
Professor Luke Bisby holds the Chair of Fire and Structures at the School of Engineering at The University of Edinburgh. Educated in Canada, Professor Bisby undertook research at McGill and

Queen's Universities before emigrating to Scotland in 2008. He is a Member of the ICE Standing Committee on Structural Safety and an instructed expert witness to the Public Inquiry into the fire at Grenfell Tower.

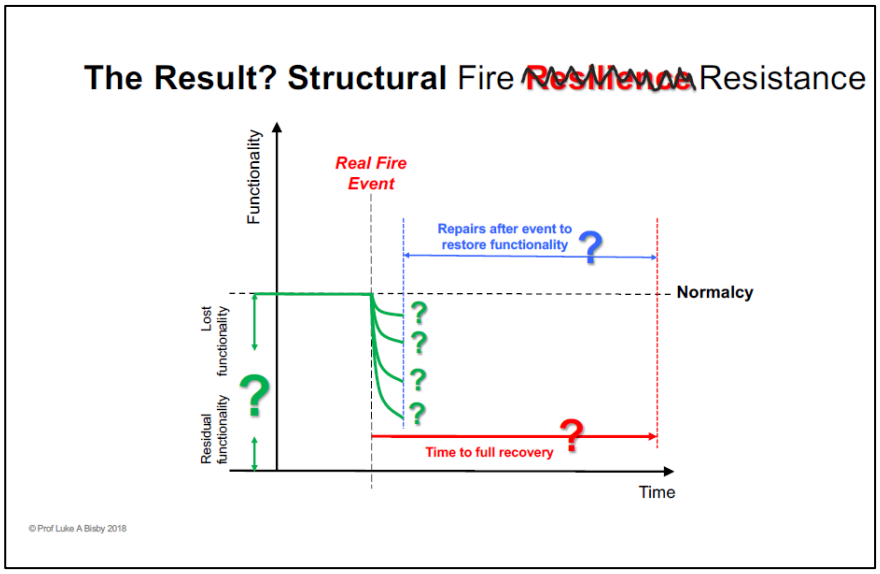
The ICE Global Engineering Congress brought together mainly younger engineers from around the world to discuss global challenges. The congress provided the Hazards Forum with an opportunity to present a lecture on hazards that would be of wide interest. With the construction of even more high-rise buildings in the major cities of the world, the Hazards Forum selected a lecture on fire safety as an appropriate topic given current discussions within the industry.

Professor Bisby highlighted the difference between fire 'resistance' and fire 'resilience'. The 'fire resistance' of a building to fire is normally measured in terms of the time of exposure to a standardised temperature versus time curve before failure is experienced by one of three prescriptive and historically-based criteria. The failure criteria are based primarily on life safety considerations, and do little to explicitly preserve functionality either during or after a fire. Importantly, Professor Bisby highlighted that fire resistance times are not real times – they merely represent coarse, comparative measures of the severity of potential real fires. On the other hand, 'fire resilience' would require designers and regulators to consider the tolerability of potential fire outcomes in terms of time, difficulty and cost of repairing or restoring a building after it had been damaged by a fire. Professor Bisby cited an example from seismic engineering of buildings in Christchurch New Zealand that had withstood a severe earthquake and allowed people to escape with relatively low numbers of fatalities given the magnitude of the seismic event, but were damaged beyond repair to such an extent that they had to be demolished. In New Zealand this has been viewed by the general public and by government as a failure of structural seismic engineering, despite the life-safety focus of most seismic structural design codes and design approaches.

While modern designers of buildings do give fire 'resistance' some attention, they only very rarely give the same degree of attention to fire 'resilience'. Modern buildings may therefore be sufficiently safe as regards life safety but may not perform well in terms of damage during, and repairability after, a fire. In contrast, buildings from previous eras – which may have been designed with greater uncertainty and hence larger factors of safety – may be more robustly designed and constructed, with greater redundancy and repairability.



Professor Bisby noted that the existing standards for fire safety are generally connected with fire 'resistance', for example, a fire resistance rating of two hours generally required for residential buildings over 30m high in England. Fire containment and retention of load bearing function for this fire resistance time are the main criteria used in design – despite the fact that the 'standard fire' used in fire resistance assessments bears little resemblance to a real compartment fire in a building. Improper or unthinking application of such fire resistance design measures could, in some circumstances, be a serious threat to fire 'resilience'.



Designing for resilience to fires appears currently to be more of a commercial concern, and indeed it should be of interest to building business owners, and to insurers. The use for building structures of novel, engineered materials such as mass timber and polymer composites is becoming more popular, yet the effect on both resistance during and resilience after a major fire remains uncertain in many cases. Professor Bisby suggested that there was a case for both fundamental and large-scale testing on structures made – in part – from these materials.

Concluding, Professor Bisby said that the buildings sector relied too heavily on custom and practice with regard to providing assurances of satisfactory structural performance in fire. He asked builders and insurers to consider the social and economic case for fire resilience, and to adopt a proportionate risk-based approach to design. This, in turn, required better science, better understanding, and better (i.e. more competent) people.

Back to top

Learning and learning systems

Learning from Experience – Barriers and Opportunities, a report on an event at the IMechE on 6 December 2018

"…Those who were operating…did not have knowledge of the dangers associated with loss of lean oil flow…Nor did those charged with supervision of the operations have the necessary knowledge…"

"…Key individuals…displayed lack of applied skills and knowledge and there was a lack of supervisory presence and oversight…"

The above quotations were taken from the public domain official investigations into two major incidents, both resulting in loss of life and major plant damage, and both involving oil majors. The incidents whilst separated by 7 years had within their root causes worrying similar factors.

In 2015, seven offshore workers were killed and 45 were injured in an explosion and fire on an offshore hub platform. Investigations showed that remote platforms feeding hydrocarbons to the damaged platform failed to stop flow, significantly increasing the flammable inventory, and escalating the incident. In 1988, on the Piper Alpha platform, the tragic loss of 167 lives was without doubt escalated by the failure of other platforms to stop their flow of hydrocarbon to Piper Alpha.

Why do we continue to see the same root causes with incidents, with the examples above all within the same oil & gas sector, and in three out of the four cases receiving global publicity and benefit from a high-quality public investigation?

For our December 2018 Hazards Forum event, sponsored by the IChemE, we had the pleasure of three esteemed speakers, who considered both the challenges and possible solutions to the above question from three different and complementing perspectives.

The meeting was chaired and kicked off by Ken Rivers, President of the IChemE. Ken emphasised his passion for process safety, yet lamented that there are few if any new lessons from losses, just repeats of what we already know, but yet to learned by all. In this regard, Ken emphasised that key is getting information to both a new generation of engineers, and to re-emphasise this to older generations. Getting the information in a useful and readily useable format is critical, and should be sensitive to cultural differences and challenges both at a company and regional level. A learning culture needs to be embedded, and for this to happen strong and committed leadership is essential.

Dr Nancy Leveson, Professor of Aeronautics and Astronautics at MIT, spoke first via a video link, and raised the notation of "…root cause seduction..", and in the desire to establish a root cause, which can give an illusion of control, we can often over simplify the root causes, and miss opportunities to understand the interactions between causal factors. In this regard hindsight bias can stop of us from fully learning from the incident, and we need to identify why it made sense for people to do what they did. Nancy stressed that that blame is the enemy of safety, and whilst this may be a function of a court of law, it has no place in an open learning culture, as it stops people reporting errors, leads to information being hidden, and inhibits learning. The engineer's goal is to understand why accidents occur in order to prevent them.

Nancy then challenged a traditional and incorrect view of placing the blame on the Operator, and the lazy way in which 'operator error' is thrown out as a root cause or causal factor. The late Trevor Kletz was always quick to point out that "…for a long time people were saying most accidents were due to human error and this is true in a sense but it's not very helpful. It's a bit like saying that falls are due to gravity…". Nancy expanded on this, by taking a systems view of operator error, in which human error is a symptom and not a cause, and that behaviour is affected by the context (system) in which it occurs. We also need to recognise that the role of the operator in our systems is changing, and to do something about error we must look at the system in which people work, and be prepared to challenge: the design of equipment (such that error is not inevitable); usefulness of procedures; and existence of goal conflicts and production pressures.

Nancy then considered the manner in which we investigate incidents, in which linear 'chain of event failure' event models are used, where each event is a direct result of the preceding event. Whilst these models are popular and simple to use, and in many circumstances entirely appropriate, they do have limitations. In this regard users of a linear model approach should recognise that they cannot for example (always) handle complex human behaviour, systemic factors (such as managerial/production pressures), design flaws in complex systems, organisational/social factors, or accidents involving non-failures. Such shortcomings have led to CAST (causal analysis based on system theory), which changes the investigation process from examining failures, to asking "why were designed controls ineffective?" It is noted that CAST is explained in more detail in a free to view online textbook Engineering a Safer World.

The second speaker of the evening **Faith Wainwright**, a Director of Arup, considered the challenges of how an organisation can create a sustained learning culture. Using Arup as a case study, Faith discussed the cultural and organizational aspects of fostering a connected organization where colleagues freely share their expertise, and how communities of practice generate both the vision for future capabilities and the infrastructure for capturing and re-using knowledge gained particularly lessons learned.

Faith provided a quote from Ove Arup himself, from 1942, which rings as true today as in the time it was written: "…only limited use is made of all the existing technical knowledge…a wealth of new knowledge, new materials, new processes has so widened the field of possibilities that it cannot be adequately surveyed in a single mind…" .

With this in mind, Arup (as a company) has developed a learning process that embeds a culture of knowledge sharing everywhere, makes sharing effortless, and enables a business-aligned visionary and strategic approach to knowledge for Businesses and Groups. A step-change in this concept was made in 2014 to introduce skills leaders and networks, that complement existing organisational structures to support creativity, innovation and change.

Faith shared a number of examples where use of such skills networks have provided for innovative solutions for clients. One very poignant example was the developing of a methodology for assessing the structural safety of textile factory buildings in Bangladesh in the aftermath of the Rana Plaza disaster of 24 April 2013, which claimed 1,136 lives when an 8 storey building collapsed. The resulting building assessment methodology, which was adopted across Bangladesh, involving the inspection of 3,700 factories balanced the immediate need of preventing another Rana Plaza without shutting down an entire industry, critical to the national economy.

Having established skills networks that offer value, it unlocks a generosity of response.

Faith concluded that key to facilitating a 'lessons learned culture' was:

- Behaviours – seeking (curiosity and building on past experience) and sharing (recognising the value to others);
- Facilitation – provision of platforms, structures and organisation, all requiring leadership;

- Systematic approach – embedding for success.

The final speaker of the evening, **Robert Robinson**, Global Head of Energy Risk Engineering for Aon, considered the question from the perspective of the Oil & Gas Insurance sector. Robert provided an extensive and chilling summary of major incidents in the Oil & Gas sector dating from the 1960s to the present day presented where the lessons were not learned and the same mistakes subsequently repeated elsewhere at great cost. As well as providing a foundation for a very pragmatic 'what has gone wrong' training guide for the industry, Robert also strove to go beyond mere awareness of such incidents, but also to provided suggestions as to what might have been the barriers to the lessons being learned, and what could be done to reduce the risk of being condemned to repeat the failures of the past.

Robert suggested that the passage of time, and distance (from the incident) are possibly two of the biggest enemies of learning. Emphasis was given to the need for each generation of engineers to be made aware of the major incidents in the past, and the identified root causes behind these incidents. He 'painted a picture of incidents' in different parts of the world, with similar root causes, and offered a challenge that in the internet age that time and distance should not be an issue.

He went on to draw from his own experience that other reasons for not learning include:

- A closed mind that puts up a barrier of 'not in my company – it can't happen here';
- Belief that following the legal requirements is enough;
- A lack of risk awareness from failings in technical education and training;
- Failings in leadership, where you get the level of safety that you demonstrate you want to have.

In conclusion, Robert turned to the thoughts of the late Trevor Kletz, and asked why do people make mistakes? He considered this can be:

- Inadequate training or understanding;
- Lack of physical or mental capability to perform the required task; or
- Lack of motivation (usually lack of enforcement).

But even then, we sometimes simply forget, so we need to design for this!

Back to top

Hazards from an ageing infrastructure

John Wintle reports on an event held on 15 January 2019

Across many industrial sectors and public services, there is infrastructure that is showing the signs of ageing, either from deterioration, obsolescence, or where after many years of service the true current condition is not properly known. Where ageing infrastructure is part of a high hazard installation, such as a nuclear plant or an offshore platform, or where there is the capacity for a major public accident such as a bridge collapse, the management of ageing becomes a high priority for the duty holders. On 15 January 2019, the Hazards Forum held an evening seminar event to discuss hazards from ageing infrastructure in conjunction with the Thomas Ashton Institute of the University of Manchester.

The Thomas Ashton Institute is a partnership between the University of Manchester and the Health and Safety Executive (HSE). Drawing on their combined knowledge and experience the Institute aims to deliver research into contemporary hazards and risks, learning and regulatory insights to widen discussion and enable a better and safer working environment. The Institute is developing a programme of PhD and other research projects and held a workshop to identify topics for potential research projects to address the challenges of ageing infrastructure before the Hazards Forum seminar.

The seminar provided three industry perspectives on the challenges and hazards of ageing infrastructure. First, **David Glass** from the HSE presented his view on the importance of leadership in managing ageing and asset integrity in the on-shore process chemicals sector. **Professor Philip Irvine** from Cranfield University then looked forward to how ageing infrastructure could be better managed through increased surveillance and real-time monitoring with big data analysis, drawing on his knowledge of how the civil aircraft industry manages ageing aircraft and estimates remaining service life. Finally, **Bruce Wilson** from Sellafield Sites discussed how the need to reduce the risk from an ageing redundant stack at Sellafield necessitated its demolition and the challenges that ageing brings for decommissioning in the nuclear sector.

A Principal Specialist Inspector with HSE, and head of a team of professional mechanical engineers within the Chemical, Explosives and Microbiological Hazards Division, **David Glass** is responsible for managing research, informing policy and pursuing the strategic topic of Ageing Plant. David and the team visit COMAH sites with hazardous installations throughout the UK, inspecting arrangements for initial and ongoing integrity, maintenance and other mechanical engineering issues.

Prior to joining HSE, David worked for fifteen years for multi-national companies in the batch chemical industry. He stressed the importance of maintaining primary containment in process installations and preventing hazards from release of dangerous chemicals and substances. He highlighted a report from Lloyds in 2016 that showed that loss of primary containment was still responsible for a majority of major insurance losses in the petrochemicals sector despite the campaigns that regulators were using to focus duty holders on the need to manage the ageing appropriately and prevent loss of containment. He noted that there were still over 850 high hazard COMAH sites in the UK, although that there had been a reduction in the number of such sites from an estimated 1,200 a few years ago.

To illustrate his point, David gave two recent examples where ageing degradation had led to a loss of containment and the potential for a major incident. In the first of these a ‘T’ from an oil/gas receiving pipe at a UK terminal had thinned due to corrosion from the inside and was leaking hydrocarbons into the atmosphere and on the verge of a guillotine failure with the risk of explosion. The second example was an oil leak from a crude oil pipe that had externally corroded on its underside where condensation would gather, and where a major environmental incident was only narrowly averted after oil was found on the ground. In both cases the site management had not given enough attention to ensuring inspection planning was effective to address the risks from ageing degradation.

David highlighted the various publications, guidance and research reports that HSE had produced on the management of ageing that were available to freely download from the HSE website. These included HSE Research Report 509 on the Management of Ageing Plant containing Pressure and Hazardous Substances, Research Report 823 on Managing Ageing Plant – a Summary Guide, and a more recent HSE document: Managing Risk – a Guide to Process Safety.

Professor Phil Irvine has been applying, teaching and conducting research in the fields of fatigue, fracture and life prediction of components and structure for much of his working life. After a short period working for the National Physical laboratory, he joined GKN Automotive in Wolverhampton to perform research into service life prediction in the automotive industry. He then moved to Cranfield University to take a Civil Aviation Authority-sponsored Chair in Aircraft Fatigue and Damage Tolerance. He became increasingly interested in the contribution that health monitoring systems and prognostics could make to reduce inspection and maintenance costs in the aircraft industry, and has published many papers on structural health monitoring and life prediction.

In his presentation, Prof Irvine spoke about degradation of airworthiness of aircraft hulls, engines, control systems, transmissions and rotors in three phases: manufacturing defects, mid-life accumulation of fatigue damage from manufacturing defects, and finally initiation of widespread fatigue cracks, corrosion and mechanical damage in later life. While the regulatory policy of the CAA was to demonstrate damage tolerance for all safety critical components, where this was not possible an approach based on safe life may be permissible. This approach was to undertake repeated inspections at intervals related to the time for defects that could not be reliably detected by inspection to grow to the size where the residual strength became less than the design load limit.

Prof Irvine illustrated these ideas by citing the delamination of adhesively bonded aircraft panels due to corrosion and the progressive taking up of load by rows of rivets leading to arrays of small cracks from the rivet holes that are individually of low probability of detection but collectively reduce the residual strength of the joint. The major failure of the fuselage of the Aloha airlines Boeing 737 in 1988 was due to an accumulation of widespread fatigue damage for which the aircraft had already been inspected. As a result, the industry established by testing a ‘time limit of validity’ before the point where accumulated damage which cannot be reliably detected would degrade the ability of the aircraft to withstand the design load limit.

For high strength materials used in rotating machinery, such as helicopter transmission systems, no cracks are considered to be permissible. The aircraft industry therefore uses a safe life approach based on the period of operation for which the probability of fatigue cracks initiating is very low. It considers that for rotating machinery subjected to large numbers of fatigue cycles the time available before failure for detection of fatigue cracks after they have initiated to be too small for the damage tolerance approach to be practical. The greatest threat was exposure to unpredicted failures arising from inadvertent undetected damage occurring either during manufacture, installation or service.

Consequently, the aircraft industry had invested in developing vibration health monitoring for transmissions in helicopters where a small change in signal was an indicator of the presence of a precursor to cracking, such as pitting, wear or other defect. As a result, structural health monitoring systems for rotating machinery are now relatively mature compared with those for structures. Most current research focus is on analysing and interpreting the signals and defining thresholds corresponding to remaining useful life, where there is still poor correlation and prognostic capability.

Prof Irvine described how the rail sector had developed similar vibration monitoring systems for detection of damage to rail bogie bearings. Where real time monitoring of bearings was combined and correlated and with GPS positioning data this could indicate areas of bad track. Here was an example of how the analysis of ‘multiple big data sets’ was able to provide new and greater insights than the data sets on their own.

In contrast to vibration monitoring of rotating machinery, permanently installed structural sensors on wings or the fuselage are considerable less mature. There has been a lot of development work over the past thirty years, with many different techniques proposed, but significant difficulties in achieving sufficient resolution to detect local damage remain, while global monitoring of modes of vibration is generally not sufficiently sensitive to detect local damage. Whereas SAE had published Guidelines for Implementation of Structural Health Monitoring on Fixed Wing Aircraft, annual inspection of structures was still the main approach to maintaining safety.

In conclusion, Professor Irvine said that the aircraft industry had well developed approaches for managing ageing of aircraft based on damage tolerance and safe life, with different approaches being used for structures and rotating systems. The use of vibration monitoring of rotating systems was increasing and this had potential for wider application in other industry sectors. The correlation of separate streams of big data offered new possibilities for more holistic management of ageing of interconnected structures and systems.

Bruce Wilson is a graduate chemist and member of the Association of Project Management with over 30 years of experience in the nuclear industry. He served 15 years in the Thorp Commissioning and Operations team at Sellafield, holding the positions of Safety Case Manager, Operations Support Manager and Manufacturing Manager. In 2006, Bruce joined the Project Management Capability. He managed both new build and decommissioning projects before Sellafield appointed him in December 2016 to the Head of Projects role in the Remediation Value Stream. His current £160m portfolio encompasses demolition and decommissioning projects across the Sellafield site.

Bruce explained that there were a large number of redundant structures at Sellafield Site that had fulfilled their original purpose and usefulness and were now ageing and awaiting demolition. There were strong drivers to remove these structures from the site in order to reduce the risks of the nuclear and conventional hazards associated with them, to clear the land for other uses, eliminate the on-going costs of care and maintenance and improve the skyline and external profile of the site. Some of these structures had aged and were contaminated with radioactive material to an extent such that their removal could not be undertaken simply by reversal of their construction.

The first example that Bruce cited was the removal of the chimney of Pile 1. This structure had been built in the 1940s to standards well below those of modern codes and the presence of sensitive facilities nearby excluded conventional demolition. Extra precautions were therefore necessary for its safe removal in stages using a tower crane. The filter gallery at the top of the chimney had now been taken down and work was progressing on the diffuser and barrel sections.

A similar challenge was presented by the removal of the concrete stack of the first-generation reprocessing building. Here the approach was to develop a lifting platform that could be jacked up the stack. The height of the stack was painstakingly reduced layer by layer using a diamond drill, a process that produced 640 tonnes of low-level waste that could be safely disposed. The main contractors for the work were Nuvia, Delta, Alimak and Hilti. Under the project management of Sellafield Sites, the work was completed to schedule, much to the satisfaction of the Nuclear Decommissioning Authority.

Summarising, the chair, John Wintle of TWI and Trustee of the Hazards Forum, thanked the speakers for their presentations and the Thomas Ashton Institute for hosting the event. He said that awareness of the importance of managing of ageing infrastructure had developed over the past 15 years in different industry sectors. The next stage would be to support the management of ageing

through more advanced technology for condition monitoring, data analysis and fitness for service assessment, and he expected that the research at the Thomas Ashton Institute would work towards this objective.

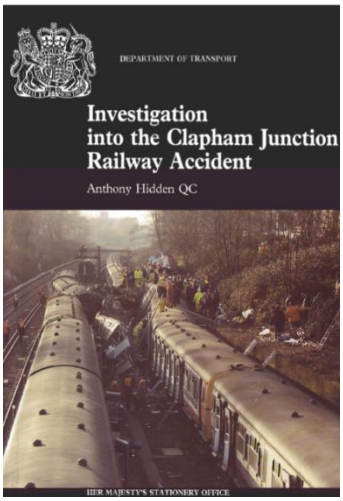
Back to top

Making sure Clapham's lessons aren't hidden

RSSB's Greg Morse looks back at the multi-fatality train accident of 1988

Eight minutes. Eight minutes from Clapham to Waterloo. I am on a train. Everything seems normal. It always does. I travel into the city with a million Reginald Perrins and Nicola Borings every day. We always get to our offices. We always moan. But back in 1988 we might not have made it at all. Back in 1988, a wrongside signal failure led to a multi-train collision that killed 35 people. Eight minutes from Clapham to Waterloo. Eight minutes, yet it's also thirty years. All-too-easy to forget what we knew thirty years ago...

Clapham resulted from an under-trained, over-worked technician leaving a bare wire dangling instead of cutting it back, tying and insulating it. A fortnight later – on 12 December 1988 – further work jolted the wire, causing it to touch a terminal, make a connection and prevent a signal from returning to danger after the passage of a train.



Later that morning, a crowded passenger train collided with the rear of another that had stopped at a signal just south of Clapham Junction. Another collision then occurred with an empty train travelling in the opposite direction. Thirty-five people died; 484 more were injured.

As we all know – or should know – Clapham was subject to a public inquiry. That inquiry, chaired by Anthony Hidden QC, would reveal issues around fatigue, training, reorganisation, communication channels and a complacent attitude to safety.

The inquiry had barely begun when there were two more fatal train accidents, just two days apart in March 1989. This time, signals passed at danger (SPADs) were the cause: at Purley, where 5 people were killed and 88 were injured, and Bellgrove Junction, where the driver and a passenger were killed, and 53 more were hurt.

As Hidden would write: 'the appearance of a proper regard for safety was not the reality. Working practices, supervision of staff, the testing of new works […] failed to live up to the concept of safety. They were not safe, they were the opposite'. Reorganisation had not caused the situation, but failed to 'come to grips' with it.

Regarding fatigue, the technician had undertaken constant, repetitive work and excessive levels of overtime, both of which had 'blunted his working edge'. To be more explicit, he'd had one day off in the previous 13 weeks. Among the report's many recommendations was one to 'ensure that overtime is monitored so that no individual is working excessive levels of overtime'. This led to the development of criteria for what was considered acceptable levels of working and a process to monitor it. New processes and instructions were also introduced regarding the installation and testing of signalling works.

Regarding safety culture, it was recommended that 'British Rail continue to press ahead with its Total Quality Management Initiative and the application of British Standard BS5750'. Originally termed 'Organising for Quality', this led to a greater focus on business-led 'profit centres' within BR's Sectors, but also (to quote historian Terry Gourvish) 'involved the identification of very clear lines of responsibility for safety […] validated by the Safety & Standards Directorate'. BR's 'holistic' structure made this a relatively straightforward process and thus a generally safe railway was handed over when Railtrack took control of the track and signalling at the start of privatisation in 1994. As 35 had died and as the British Railways Board was fined £250,000 for breaching the Health and Safety at Work Etc Act, we might say these lessons were hard won. Hard won lessons tend to stick.

And yet, corporate memory exists only while we remember it, and over the Christmas and New Year period of 2016/17, we seemed to forget. At this time, extensive resignalling and track remodelling work was being carried out in and around Cardiff Central. Some of the new layout was brought into use on 29 December. At 08:37 that day, the driver of a Treherbert service noticed that the points his train was about to take were not in the correct position. He stopped the train just before reaching them.

The Rail Accident Investigation Branch (RAIB) would conclude that the points had been left in this 'unsafe condition' because they hadn't been identified as needing to be secured by the point securing team. Furthermore, no one had checked that all the points that needed to be secured during the works over the Christmas period had actually been secured. Route proving trains had also been cancelled, and a work group culture had developed between long standing members of the project team that led to 'insular thinking about methods of work and operational risk', meaning that team members 'relied on verbal communications and assurances'. The Branch also felt ineffective fatigue management to be a possible underlying factor.

Simon French, RAIB's Chief Inspector, drew a clear line from Cardiff back to Clapham, pointing out 'how easily things can go wrong when railway infrastructure is being upgraded and renewed,' pointing out the importance of managing the working hours of people doing the job 'when organising intensive periods of commissioning work'. 'Back in 1988,' he went on, 'the disastrous collision at Clapham Junction happened in part because working for weeks on end without any days off was part of the culture in some areas of the railway'. The events at Cardiff showed 'how easy it is to forget the lessons of Clapham and slip back into those habits under the time pressures of a big commissioning'.

One can only agree. But there's more… A few months later – in August 2017 – a train departed Waterloo on a green, but was incorrectly routed and collided with an engineer's train on the adjacent line. Luckily the driver saw the way the points were set and managed to brake, meaning the collision occurred at low speed and resulted in no injuries. Modification to the wiring of the point detection circuits meant that a 'desk' set up to aid testing no longer simulated the detection of the points in question correctly...because it hadn't been modified to account for changes made to the detection circuit.

On the weekend of 12/13 August 2017, while trains had been stopped from running on the lines leading to the points, a temporary wiring "mod" was made in the relay room in an attempt to restore the correct operation of the relevant switch on the test desk. But the mod wasn't reviewed by a signalling designer and was wrongly left in place when the railway was returned to operation on the morning of 14 August.

Not only could we quote Mr French again here, we could quote Mr Hidden again too. In short, it's all about understanding and managing risk. Hidden suggested BR had become almost blind to the risk from wrongside failures, contrasting it with its focus on SPAD risk. BR was probably right to put proportionately more focus on SPAD risk in the late 1980s, but not to the exclusion of wrongside failures (or any other hazard, come to that). Indeed, there'd been a number of "Claphams in the making" that a greater emphasis on learning from operational experience might have highlighted. More specifically, there'd been a 'cluster' of wrongside failures in November 1985, during the installation of new signalling. Most worryingly, a signal at Oxted had shown green when it should not have done, because a relay had been energised irregularly, a fault which would have been discovered by a wire count, but – as with Clapham three years later – no such count had been undertaken. Worse still, the resulting 'flurry of paperwork' provided important information, but was shared with very few people and therefore did not feature in anyone's thinking during the work at Waterloo.

We all know we can increase the accuracy of our risk picture by collecting, analysing and learning from information, not just about accidents but also their precursors and the activities that prevent them. The thing is, as Cardiff and Waterloo remind us, data and information – from the past and the present – are only any use if we analyse results, understand what they mean and act on them...out on the railway, not just on paper…

Back to top

Coming up

The Events section of our website has more information and details of any updates, which may include additional events or amendments to those shown below. Attendance is by invitation.

We would like to remind our engineering, corporate and associate members that all individual members of your organisation have the opportunity to attend our events without further charge, subject to numbers.

Date	Event	Venue	Contact/further information
May 2019			
22-24	Hazards29	ICC, Birmingham, UK	https://www.icheme.org/hazards29
June 2019			
18	**Artificial Intelligence and Automation: Impacts for Energy, Manufacturing and Transportation in smart cities**	ICE	https://hazardsforum.org.uk/event/artificial-intelligence-and-automation-impacts-for-energy-manufacturing-and-transportation-in-smart-cities/ This event will also reflect on the successes of the Hazards Forum in this its 30th anniversary year.
September 2019			
17	**Man-machine hazards in transport – perception, automation and climate change**	London, actual venue to be confirmed	
Autumn 2019			
tbc	**Natural Hazards for Climate Change**	Manchester	
December 2019			

3	**Forensic engineering and failure investigation**	London, actual venue to be confirmed	

…and finally, opportunities for new trustees

The Hazards Forum is actively seeking new trustees to join the existing board and help with the strategic delivery of our charitable purpose. We are looking to expand the existing membership and offering, and new trustees bringing fresh perspectives, ideas and skills is crucial in this regard – for more details refer to the Hazards Forum website and the Call for Hazards Forum Trustees

Back to top