Issue 34 / Autumn 2018

RISKworld

The Newsletter of Risktec Solutions

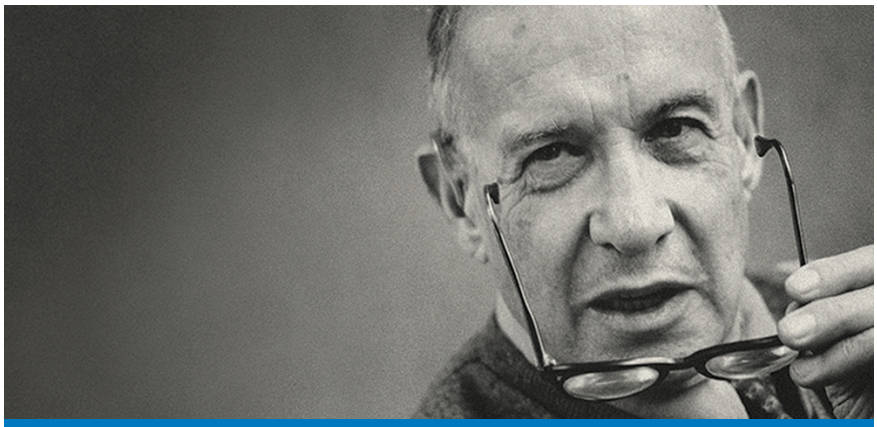
In this issue

Welcome to Issue 34 of RISKworld. Feel free to pass it on to other people in your organisation. We would also be pleased to hear any feedback you may have on this issue or suggestions for future editions.

Contact: Steve Lewis
steve.lewis@risktec.tuv.com

Contents

Innovation, Innovation, Innovation



Innovate or die – Peter Drucker (1909-2005), father of modern business management

We are pleased to report that our latest client satisfaction survey, covering the first half of 2018, shows that we continue to achieve very high levels of client satisfaction. 97% of clients are satisfied with our service, 99% of clients would recommend us to others and 100% of clients would use us again.

Whilst we are understandably proud of these results, what is much more important is the opportunity for clients to provide feedback on our performance so that we can understand how to improve. We strongly believe that listening to our clients and striving continually to improve our performance leads to stronger and long-term relationships.

In other news, we have recently established new offices in Singapore, Kuala Lumpur (Malaysia) and Nottingham (UK). This is a natural extension of our desire to be close to our clients so that we can develop sustainable relationships.

The principal focus for the Singapore and Kuala Lumpur offices will be our oil and gas, petrochemical and chemical clients in the region.

The Nottingham office will provide Asset Integrity Management (AIM) and outage support to the conventional power generation sector in the UK and internationally.

We have also recently moved into a new office in Houston, shared with TÜV Rheinland Industrial Solutions, which will broaden the range of process safety and AIM services we offer to our clients in the US.

Innovation is a key part of our solutions culture and is a theme that runs strongly throughout this edition of RISKworld. To us, innovation means being flexible, pragmatic and creative in a way that delivers the right solutions to clients.

As always we welcome your feedback and look forward to your continued support.

Contact: Gareth Book
gareth.book@risktec.tuv.com

An introduction to functional safety assurance

If you've ever wondered what's meant by the term functional safety assurance, you're not alone. Simply put, functional safety assurance is the process by which we ensure that safety-related systems do what we need them to do, when we need them to do it, so that risk is maintained at tolerable levels. But what does this mean in practice?

The originating standard for functional safety is IEC 61508, which applies to Electrical, Electronic and Programmable Electronic (E/E/PE) safety-related systems. This is a generic standard with industry-specific variations developed from it, including IEC 61511 for the process industry, for example.

Although functional safety assurance principles can be applied to all types of equipment, the term is usually used in connection with E/E/PE systems, for instance railroad signalling, or trip logic for stopping pumps or isolating valves automatically.

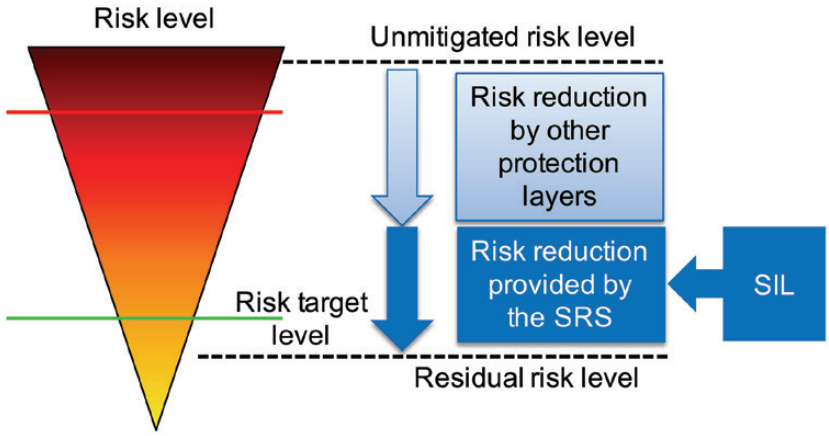


Figure 1 - Risk reduction by safety-related systems

WHAT IS IT?

Functional safety assurance comprises five main activities:

1. Determine safety function and integrity requirements
2. Design system to achieve requirements
3. Verify that design fulfils requirements
4. Validate that functional safety activities have been undertaken correctly
5. Ongoing activities to support the integrity of the system

Unlike some standards which tend to be relevant to a single step of the risk management process, functional safety assurance covers a number of these steps. It may seem like a lot of additional work but, if properly planned for, it can be integrated into existing risk management and design activities with relatively minimal extra effort.

1. DETERMINE REQUIREMENTS

At this stage the project defines the concept design and carries out risk assessment to determine:

- The required safety function
- The level of risk reduction required of the safety function

This is typically presented as a safety requirements specification, which details the functionality and risk reduction requirements of the Safety-Related System (SRS), and then maps that risk reduction to an equivalent Safety Integrity Level (SIL), as illustrated by Figure 1. This step if often called 'SIL determination' or 'SIL assignment'.

The requirements specification should also include requirements relating to testability, maintainability and independence (from other safeguards and fault causes), as well as the specific functionality in the event of detected failure, to help inform the design process.

Optioneering should be conducted to identify the most effective means of achieving the required risk

reduction and arrive at the As Low As Reasonably Practicable (ALARP) solution. For example, it might be simpler and cheaper to fit a key-controlled padlock on an enclosure, rather than design a bespoke E/E/PE SIL-rated interlock.

2. DESIGN SYSTEM

The system proposed to deliver the safety function must then be designed, based on the safety requirements specification and the relevant standard from the IEC 61508 series, which considers factors such as architectural constraints, minimisation of systematic failures and fault detection, and supports the overall demonstration of integrity. This ensures that not only will the SRS reliably perform the required safety function, it will also be suitably robust, rigorously designed and tolerant to faults such that confidence in its correct function is assured.

3. VERIFY DESIGN

At this step the design is critically reviewed against the requirements, typically including reliability analysis to demonstrate that the required risk reduction has been achieved, i.e. 'SIL verification'. Verification must also confirm that the full range of safety requirements have been achieved, e.g. that appropriate redundancy, diversity and robustness have been incorporated into the design.

4. VALIDATE/CERTIFY DESIGN

The validation process is often undertaken by independent parties to ensure objective analysis. The intent of this step is to audit the overall process to confirm that appropriate functional safety assurance tasks were planned for and undertaken when required by suitably competent people, to an appropriate standard and quality. This will initially focus on a high level, but will drill down into specific detailed analysis as required. Equipment manufacturers will often seek formal recognition of the design's validation in the form of 'SIL certification' by an accredited certifying body.

5. ONGOING SUPPORT

The requirements of functional safety do not end once the design is verified and validated. The system must still be installed, tested, maintained, monitored and managed so that it continues to perform as intended and that the assumptions and claims of the assurance process as a whole remain valid.

SO WHAT CAN GO WRONG?

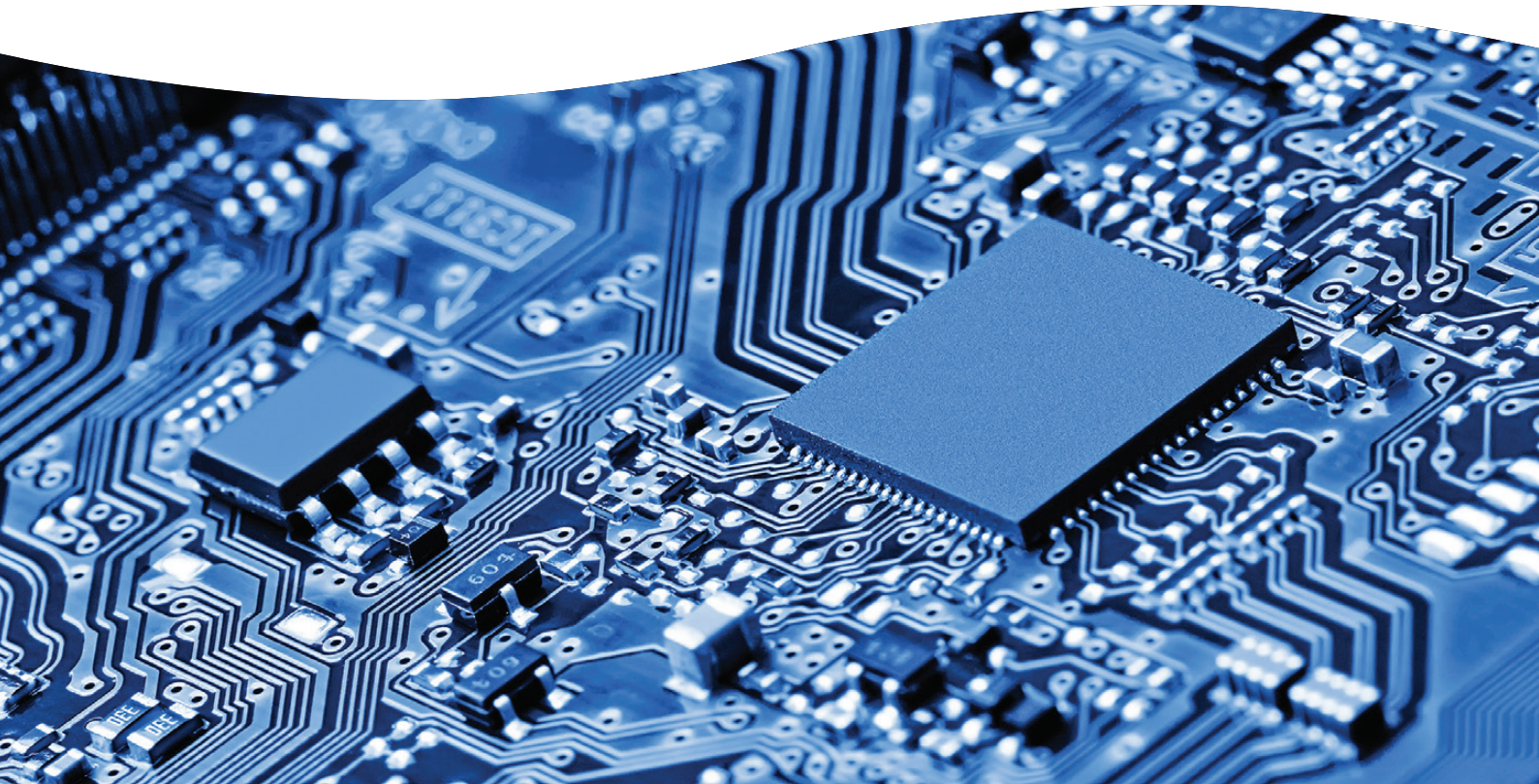
Although at a high level the functional safety assurance process is relatively simple, there are some common pitfalls, which are equally applicable to risk management activities more generally. For example:

- Activities not anticipated or planned
- Work not undertaken by competent persons
- Poor traceability between hazards, requirements and design
- Ill-defined or missing safety requirements specification
- Weak or missing design evidence
- Key design ALARP decisions not documented

CONCLUSION

In the right hands, functional safety assurance is a mature, standardised process for designing, delivering and operating fit-for-purpose E/E/PE safety-related systems and their associated safety justification.

Contact: Kevin Charnock
kevin.charnock@risktec.tuv.com



Cyber-security meets functional safety

The cyber-threat to industrial control systems is very real, as demonstrated by high profile attacks in recent years. That said, many defensive measures put in place to assure functional safety will also protect against cyber-attacks. But is that enough? What else needs to be done?

The control systems that operate physical processes in an industrial plant work within a so-called Operating Technology (OT) environment. OT systems' priorities are reliability, availability and maintainability. Whilst corrupted data in standard Information Technology (IT) systems can be disruptive to a business, it is not life threatening. However, when transmitted to thousands of sensors in an industrial plant, for example, it can cause major business interruption and, potentially, a major accident with a catastrophic impact on people, assets, environment and reputation.

Stuxnet, Industroyer and Triton are just a few examples of malware attacks in recent years on digital systems that control critical infrastructure (see below). Other plausible cyber-threats include the possibility of gaining unauthorised control of systems remotely or locally, or seeding systems with unauthorised data (via USB ports for example). With the frequency of cyber-attacks growing rapidly, clearly industry needs to focus on protecting automation and control systems against what must be assumed to be an inevitable attack.

EFFECTIVE CYBER-SECURITY

Effective cyber-security for OT systems is delivered by a blend of:

- Cyber-security defensive measures covering the system lifecycle, from design to operations and the subsequent decommissioning of the systems and individual components.
- Cyber-risk assessments of the systems to establish any additional security measures required to protect them from cyber-threats (e.g. following security standard IEC 62443 or NIST 800-82).
- The integration of cyber-security alongside physical and procedural security measures within the context of overall security.
- Cyber-security vulnerability assessment and penetration testing of the installed systems.

ALIGNMENT WITH FUNCTIONAL SAFETY

The development of functional safety requirements and their delivery are well-established and both generic (IEC 61508) and industry-specific (e.g. IEC 61511 for process industry and IEC 61513 for nuclear industry).

STUXNET

In January 2010, Stuxnet became the first discovered malware known to spy on and subvert industrial control systems. Stuxnet targets SCADA and PLC systems and is believed to be responsible for causing substantial damage to Iran's nuclear programme by causing the fast-spinning centrifuges at the Natanz uranium enrichment facility to tear themselves apart. Although unconfirmed, the worm is believed to be a jointly built American/Israeli cyber-weapon. Stuxnet was uploaded by an infected USB flash drive.

INDUSTROYER

One fifth of Ukraine's capital, Kiev, lost electrical power for one hour in December 2016, the result of an attack by the Industroyer malware, specifically designed to disrupt the working processes of industrial control systems used in electrical substations. A similar attack had been experienced precisely one year earlier.

TRITON

In December 2017, the safety systems of an unidentified power station, believed to be in Saudi Arabia, were compromised when the industrial safety technology was targeted by Triton malware. This exploited a vulnerability in computers running the Microsoft Windows operating system and is believed to have been a state-sponsored attack. The plant shut down and no harm was done.

These standards address the software, hardware and management aspects associated with a system's lifecycle, all of which are potentially vulnerable to a cyber-attack.

As it turns out, defensive cyber-security measures are often closely aligned with measures introduced during the project lifecycle to deliver functional safety. Where true, this alignment presents an opportunity for cyber-security assessment to take credit for safety measures that are necessarily put in place to deliver functional safety in existing systems, since many of the means of achieving systematic safety integrity are similar to those required to defend software, hardware and procedures from cyber-attack. Resources can then focus on plugging any cyber-security holes.

INTEGRATING CYBER-SECURITY AND FUNCTIONAL SAFETY

However, to deliver a truly cost-effective control system, which is optimised for both cyber-security and functional safety, requires an integrated approach. The earlier the integration of cyber-security and functional safety, the greater the benefits that can be reaped.

For effective integration, the vulnerability to a cyber-attack needs to be considered during each phase of the functional safety lifecycle. Ideally, safety hazard and cyber-threat identification would occur at the same time, so that optioneering can consider solutions that eliminate or reduce the risks from both sources.

Achieving adequate cyber-security could include ruling out remote terminals and data ports, relocating equipment to a manned central control room, avoiding programmable systems in remote areas and introducing air gaps where data transfer requirements are minimal, especially between control and protection systems. Other provisions include limiting access both physically and by password protection. Importantly, considering such options at an early stage not only reduces downstream time, trouble and cost, but it also allows decisions to be weighed equally against the needs of operational effectiveness and functional safety.

The outcome would be an integrated set of functional requirements that embrace both safety and cyber-security requirements, and ultimately a compliant design and effective supporting management system.

This approach is not without its pitfalls, however. Take the setting of Safety Integrity Levels (SIL) as an example. SIL targets for safety systems quantify the level of safety integrity required for each safety function in order to meet overall risk targets. Four levels are designated in IEC 61508 with SIL4 denoting the highest integrity requirement. These are very precisely defined. The corresponding Security Levels (SL) in IEC 62443 are much more subjective, both in terms of their selection and definition, which reflects the subjective nature of the threat. As such, the early integration of cyber-security and functional safety requires a pragmatic approach as well as holistic security thinking, since over-specifying SL targets to meet a hypothetical cyber-threat could potentially lead to an overly designed and costly solution.

Contact: Mel Davies
mel.davies@risktec.tuv.com

CONCLUSION

The integration of cyber-security, functional safety assessment and design makes sense for delivering cost-effective and optimised industrial automation and control systems, but requires care to avoid over-specifying and over-designing to address a subjective cyber-risk.

Managing fire risk in high rise buildings – the case for bowtie safety cases

Multi-occupancy Higher Risk Residential Buildings (HRRBs) have the potential for significant societal impact, with a large number of people concentrated in a small space exposed to foreseeable events such as fire. This was all too starkly highlighted by the Grenfell Tower fire in London in June 2017, which caused the deaths of 72 people – the worst fire in the UK since the 1988 Piper Alpha disaster.

In her independent review of UK building regulations and fire safety following the Grenfell Tower fire (Ref. 1), Dame Judith Hackitt identifies deep flaws in the current system and proposes that the key principle of risk ownership and management needs to be applied alongside a simpler, outcomes-based regulatory framework.

A goal-setting, safety case approach as applied in major hazard industries, and in particular the use of bowtie analysis of significant risks, is one way of addressing Dame Judith's recommendations. We consider some of the key themes contained in her report (reproduced in italics) and illustrate how a bowtie-based safety case may provide a practical, effective solution.

RISK OWNERSHIP

"There is lack of clarity…over where responsibility lies, exacerbated by… fragmentation…and precluding robust ownership of accountability."

HRRBs are *"complex systems where the actions of many different people can compromise the integrity of that system."*

A fully developed bowtie analysis can be used to illustrate, clearly and unambiguously, the safety-critical responsibilities of the parties involved in an HRRB project, including the client, designer, contractor, owner and operator/maintainer. By coming together to build a bowtie model for potentially significant risks, all parties can agree and understand their contribution to the case for safety, and appreciate the contribution made by others as well as any constraints and conflicts that may arise. Collaboration is encouraged and thinking in 'silos' is reduced.

Furthermore, a properly completed bowtie analysis provides reassurance to other stakeholders, not least residents, about the safety of their home and demonstrates who is responsible for what when it comes to managing risks.

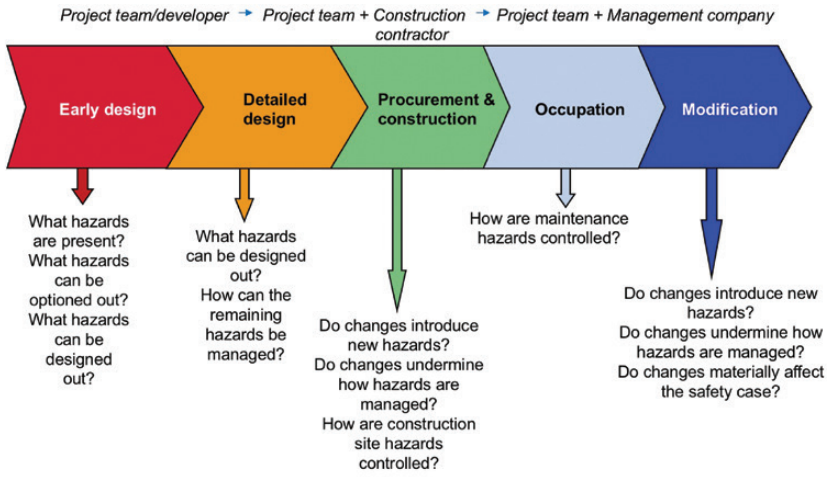


Figure 1 - HRRB Safety case lifecycle

GOLDEN THREAD

"Transparency of information and an audit trail all the way through the lifecycle of a building from the planning stage to occupation and maintenance is essential."

At the outset, the case for safety is made at a relatively high level, and would then evolve with the building, becoming more detailed and complete with each phase of the project (see Figure 1). The focus is on designing and constructing a safe HRRB, and then maintaining it and managing change so that it continues to be safe.

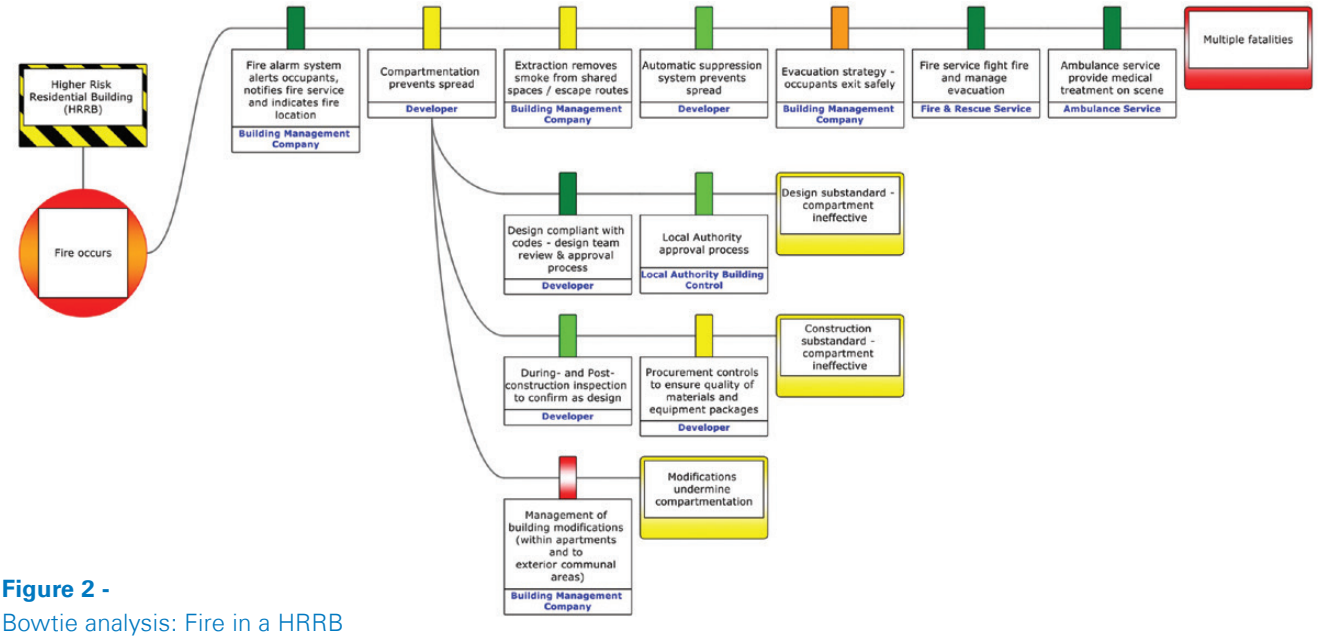


Figure 2 -
Bowtie analysis: Fire in a HRRB

Change control is a key area for HRRBs where, historically, management of risks has been undermined. Changes may occur frequently during design, construction and ongoing occupation, with little or no thought given to, or even awareness of, the risk basis behind preceding decisions. The bowtie diagram can highlight those risk controls which are susceptible to deterioration as a result of poorly thought through or inadequately managed modifications to a building's design, construction, maintenance and operation.

BUILDINGS AS A SYSTEM

We must think of *"buildings as a system so that we can consider the different layers of protection that may be required to make that building safe on a case-by-case basis."*

The completed bowtie diagram illustrates clearly, and in one place, the multiple layers of protection and how they are supported by safety-critical activities and competencies, defined safety-critical equipment, and effective, documented management systems.

Figure 2 illustrates an extract from a bowtie for fire in a HRRB, including example mitigation controls defined at the design stage, enacted at the construction stage and maintained during the occupation stage to reduce the risk of multiple fatalities as low as is reasonably practicable.

EFFECTIVE USE OF RESOURCES

"The new framework is designed to create a more simple and effective mechanism for driving building safety."

Whereas the risk levels in industries such as nuclear power generation or oil and gas extraction warrant a project-specific safety case and detailed analysis of the significant risks, any safety case approach for design and construction of HRRBs must be proportionate, reflecting the resources likely to be available.

The bowtie approach for significant risks allows technical analysis to be captured, communicated, applied and re-applied in a straightforward and accessible manner.

The knowledge and experience already exists within the industry to create a generic bowtie model for HRRB fire risk management (such as that shown in Figure 2), which could then be made available through industry guidance. The generic model could be customised by specific projects to produce a true picture of the integrity of their proposed building against fire. It could be reviewed when modifications are proposed; and it could be used as an audit tool to assess periodically the building's current condition, providing ongoing risk monitoring and assurance.

CONCLUSION

Properly implemented, a bowtie-based safety case can provide a practical, effective solution to the many challenges associated with achieving fire safety of HRRBs.

Contact: Sheryl Hurst
sheryl.hurst@risktec.tuv.com

References: 1. Building a Safer Future – Independent Review of Building Regulations and Fire Safety: Final Report, May 2018.

Carbon capture and storage: An upcycled solution to climate change?

With the Intergovernmental Panel on Climate Change (IPCC) now concluding that the Paris Climate Change Agreement stretch target — to limit the rise of global average temperatures in 2050, from pre-industrial levels to 1.5°C — must be achieved to avoid significant and irreversible harm to the planet (Ref. 1), the challenge of reducing carbon dioxide (CO_2) emissions is becoming more and more pressing. Carbon Capture and Storage (CCS) is expected to play a crucial role in meeting this target, but what is it, what risks does it present, and how should they be managed?

LESS IS MORE

Power generation, where CO_2 is produced as part of the combustion process, is a major source of global CO_2 emissions. There are three ways we can reduce emissions from power stations, as illustrated in Figure 1.

CARBON CAPTURE AND STORAGE

Carbon Capture and Storage (CCS) is the name given to the industrial-scale process of capturing CO_2 before it is released into the atmosphere and transferring it into deep subsurface rock formations, such as depleted oil and gas reservoirs, where it can be safely and permanently stored (see Figure 2).

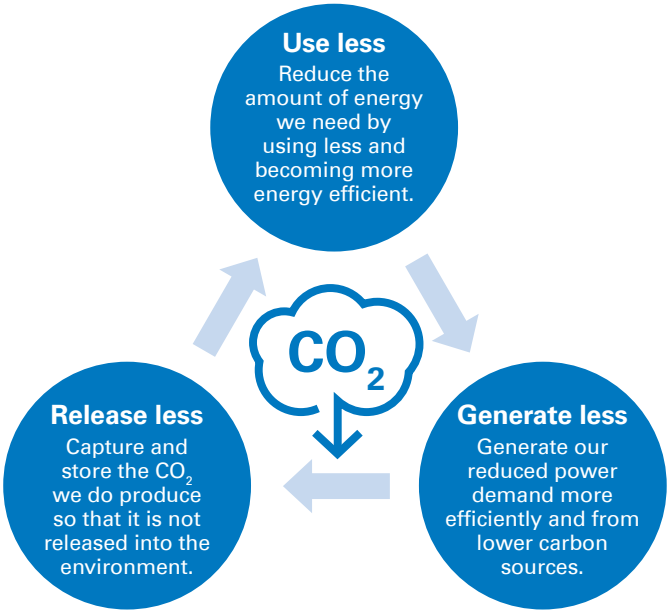


Figure 1
Opportunities to reduce CO_2 emissions from power generation

But the benefits of CCS stretch well beyond the power generation industry. It can be used to capture the CO_2 produced from other industrial processes and when integrated into an overall carbon capture network, as depicted in Figure 2, it can play a highly cost-effective and efficient role in reducing global carbon emissions.

SIGNIFICANT REWARDS

It is predicted that CCS can deliver 17% of the UK's 2050 CO_2 reduction target (Ref. 2), while its inclusion within a mix of low-carbon technologies is seen as the lowest cost route to decarbonisation. Without CCS, the cost of meeting the target would increase by 40%.

WHAT ARE THE RISKS?

CO_2 is not harmful to health at low concentrations. It is not flammable and will not support combustion. However, at high concentrations it can cause headaches, dizziness, confusion and loss of consciousness. With CO_2 being heavier than air, fatalities from asphyxiation have occurred when it has entered confined spaces and displaced oxygen. As such, CO_2 has been recognised as a significant workplace hazard for over a century; and highly effective standards and legislative controls have evolved to manage today's risks effectively.

CCS, however, will involve CO_2 being handled in quantities many orders of magnitude greater than today. Whereas in existing facilities, an inadvertent release of CO_2 may create a small-scale hazard only affecting those in the local vicinity, a very large release of CO_2 from a CCS facility has the potential to produce harmful effects over a wide area affecting many more people and the environment.

There are engineering challenges too. CO_2 is corrosive in wet and impure conditions; therefore careful consideration is required in the design and material selection for storage, transport and injection facilities.

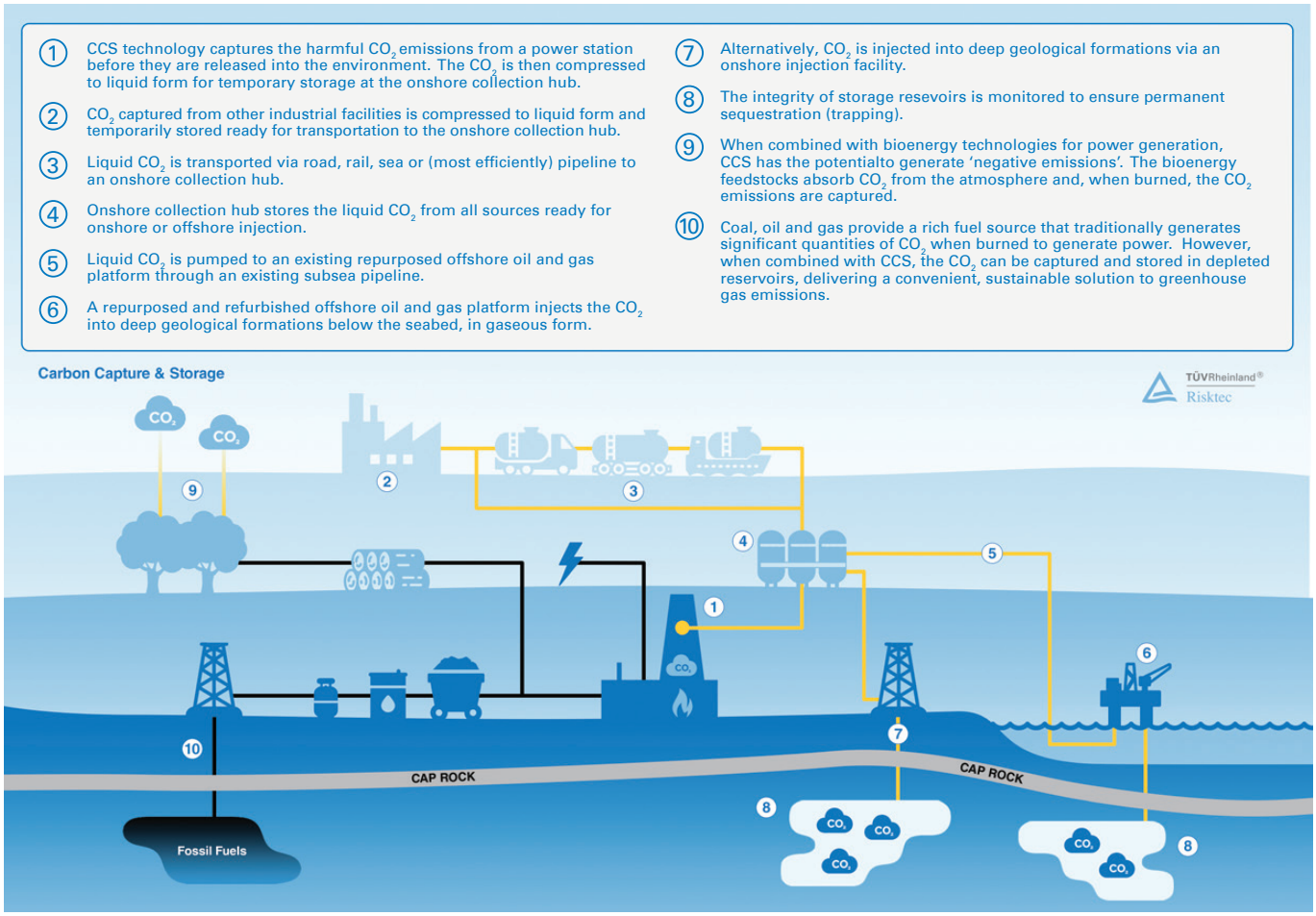


Figure 2 - The CCS process

Geological security is clearly paramount to the success of CCS. Unless the long-term integrity of underground storage can be ensured, the environmental benefits of CCS will not be achieved and public health and environmental protection could be compromised.

SOMETHING OLD, SOMETHING NEW, SOMETHING BORROWED…

Perhaps the greatest risk to the sustainable proliferation of CCS is in treating it as something entirely new and innovative. Whilst clearly a novel concept with significant new challenges, it will rely on many existing systems and processes. Granted, these will often be used in reverse (e.g. using an offshore platform and subsea pipeline to inject CO_2 rather than extract oil and gas) and will accommodate a different medium, but many of the tools and techniques required to assess and manage these risks will be very similar; and much of today's offshore design and operating experience can also be brought to bear.

'Upcycling' may be defined as "Creative reuse - the process of transforming by-products, waste materials, useless or unwanted products into new materials or products of better quality or for better environmental value" (Ref. 3). By this definition, CCS is upcycling on an industrial scale and the approach to managing the associated risks should be tailored to suit. We must innovatively rework and repurpose existing infrastructure, knowledge, experience, processes, tools and techniques to learn from the past and benefit from the tried and tested, whilst developing solutions to the new challenges presented.

CONCLUSION

CCS can play a starring role in the fight against climate change, but comes with a range of technical, geological, health, safety, environmental and ethical challenges. However, by repurposing the old, borrowing the proven and innovating the new, CCS can meet these challenges and achieve its full potential in a safe and sustainable way.

Contact: Gareth Ellor
gareth.ellor@risktec.tuv.com

References: 1. Intergovermental Panel on Climate Change – Global Warming of 1.5°C, October 2018.
2. The Economic Benefits of Carbon Capture and Storage in the UK, CCS/TUC, February 2014.
3. Wikipedia, https://en.wikipedia.org/ wiki/Upcycling, accessed October 2018.

Safety and risk management: Help or hindrance to innovation?

There is a common perception in industry that safety and risk management can be a blocker to progress and innovation, or that it is a 'tick box' exercise to be endured rather than embraced. However, proactive implementation of safety and risk management techniques at all stages of the product lifecycle can optimise designs and minimise overall cost. So can these same techniques accelerate the market readiness of innovative technologies?

Regardless of whether innovative ideas are being introduced by start-up organisations or established multinationals, return on investment is key to the business case. Safety and risk management should always add value and offer solutions with due consideration for commercial constraints.

SAFETY THROUGH THE PRODUCT LIFECYCLE

Innovation is often most successful when an organisation's strengths are harnessed to address current or future market needs. However, organisations may fail to consider hazard elimination or reduction through substitution of alternative lower risk solutions that could achieve the same functional needs – often at a lower cost.

Undertaking conceptual hazard identification and being open to asking 'could this be done better?' at the early stage of product development can eliminate hazards and wasted effort, and deliver a more profitable, saleable product.

Safety and risk management not only adds value at the concept design stage, it can do so throughout all stages of the product lifecycle. Structured hazard analysis stimulates innovation by identifying and implementing safety requirements for design, operation, training and maintenance, to enable the commercialisation of technology. In many cases this process is required to demonstrate regulatory compliance and hurdle industry barriers to entry but, in doing so, it will help validate the completeness of product development and readiness for market.

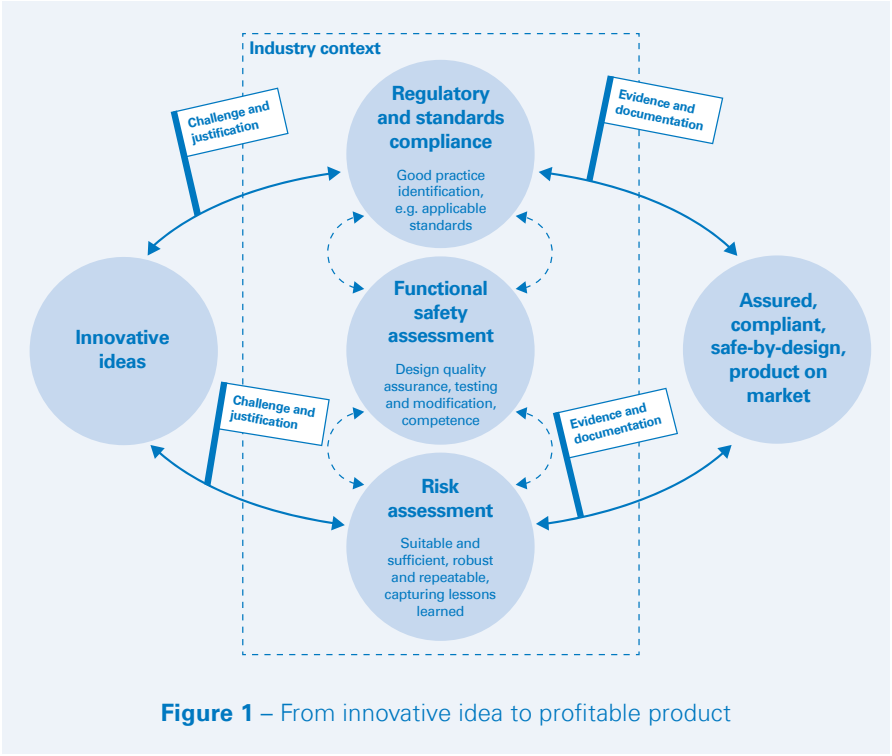


Figure 1 – From innovative idea to profitable product

APPLYING GOOD PRACTICE

Reducing the safety risks of an innovative system as low as is reasonably practicable is the primary goal of safety management. This can seem nebulous, but the first task is always to identify good practice, i.e. those codes and standards that are applicable. Yet when a product is novel, the obvious question becomes, 'Is good practice available?' The answer is almost

certainly, 'Yes… to some extent,' and good practice from other established industries can usually be read across. Even in the developing field of autonomy for example, where gaps in good practice are known to exist, there is still a viable legal and engineering framework to build upon (e.g. Ref. 1).

Figure 1 illustrates how innovative ideas can be driven through the complex regulatory environments of different industries all the way to assured, compliant, safe-by-design products serving their target market.

In the rail industry, the Common Safety Method for Risk Evaluation and Assessment (CSM-REA) provides a framework of three risk acceptance principles. The first is to follow relevant codes of practice. Where these are not fully applicable or developed then CSM-REA allows similar reference systems and explicit risk estimation to be considered. Guidance from Oil and Gas UK (Ref. 2) suggests engineering risk assessment when good practice is incomplete, and wider stakeholder engagement for novel approaches.

AN EXAMPLE

The Non-Intrusive Crossover System (NICS) in the rail industry, patented by NICS Ltd., allows the seamless movement of a train from a track under repair onto a second track and then back onto the first track beyond the repair site, all achieved without cutting into existing rails. This innovative solution reduces disruption and cost.

Applying CSM-REA, the resulting safety case demonstrated how NICS Ltd. had identified relevant hazards and controlled associated risks by developing its design, training, installation, operational and maintenance manuals and business processes. NICS was always an innovative system capable of serving an important market need; but the body of safety assurance evidence has enabled NICS Ltd. to move beyond proof of concept to market readiness.

CONCLUSION

Even if a suitable and sufficient safety risk assessment isn't required by law, it is still hugely beneficial. It can help to avoid potential pitfalls with innovative technologies and identify improvements. This process should be seen as an integral part of innovation, supporting the delivery of a profitable, safe-by-design new product to the market.

Contact: Ed Thomas
edward.thomas@risktec.tuv.com

References: 1. Legal framework for small autonomous agricultural robots, AI & Society, April 2018.
2. Guidance on Risk Related Decision Making, Oil and Gas UK, Issue 2, July 2014.

RISKTEC OFFICES WORLDWIDE

UK Principal Office
Wilderspool Park
Greenall's Avenue
Warrington WA4 6HL
United Kingdom
Tel +44 (0)1925 611200

TÜV Rheinland Headquarters
TÜV Rheinland Group
Industrial Services
Am Grauen Stein
51105 Cologne, Germany
tuv.com

Europe
Aberdeen
Crawley
Derby
Edinburgh
Glasgow
London
Nottingham
Rijswijk

Middle East
Dubai
Muscat

North America
Calgary
Houston

South East Asia
Kuala Lumpur
Singapore

For further information, including office contact details, visit:
risktec.tuv.com
or email:
enquiries@risktec.tuv.com

You can also find us on:

@TUVRisktec

LinkedIn

YouTube