Issue 46: Autumn / Winter 2024

RISKworld

The Newsletter of Risktec Solutions

In this issue

Welcome to Issue 46 of RISKworld. Feel free to pass this edition on to other people in your organisation. You can also sign up here to make sure you don't miss future issues.

We would also be pleased to hear any feedback you may have on this issue or suggestions for future editions.

Contact: Steve Pearson or David McDade
steve.pearson@risktec.tuv.com
david.mcdade@risktec.tuv.com

Contents

"It is not in the stars to hold our destiny but in ourselves."
William Shakespeare

As the year draws to a close, we are able to look back on another exciting year at Risktec marked by the completion of many successful projects and significant growth across sectors, and we have been delighted to see many new people join the business.

This has included new colleagues from Safetec, which was recently welcomed into the TÜV Rheinland Group. The additional skills and experience they will bring is an exciting complement and addition to our capabilities, and we look forward to working with our new colleagues into 2025 and beyond.

This edition of RISKworld mirrors our forward-looking ethos, and the selection of articles deals with technology and themes which continue to emerge.

We have different perspectives on some of the key technologies which are expected to play a part in the energy transition. This includes a look at the risk presented by societal acceptance or non-acceptance of new technologies, in this case Carbon Capture and Storage (CCS), and how this can be assessed and managed.

We also explore hydrogen fuel cells, unravelling the safety considerations across industrial and vehicular applications, and take a look at the evolving landscape of Small Modular Reactors (SMRs).

The edition also shines a light on the Safety Critical Task Analysis (SCTA) and Common Safety Method on Risk Evaluation and Assessment (CSM-RA) processes, sharing our lessons learned and knowledge gained from our project experience.

As we look to the future, our commitment to meet and exceed our clients' expectations remains as strong as ever, and the results from our recent bi-annual client satisfaction survey showed that 98% of respondents would recommend our services. This is a testament to the trust you place in us, a responsibility we hold in the highest regard.

I hope that you enjoy the articles in this edition and find something interesting and thought-provoking. As ever, we value your perspective and invite your feedback.

Thank you for your continued trust and engagement throughout 2024, and I wish you all the best for 2025.

Contact: Martin Fairclough
martin.fairclough@risktec.tuv.com

Understanding the risk associated with societal acceptance of CCS

As Carbon Capture and Storage (CCS) is increasingly viewed as a key technology in limiting the impacts of climate change, there are many challenges associated with industrialisation and upscaling. A key priority is the need for society to be prepared for the delivery of large-scale CCS projects, and understanding the risk presented by societal acceptance or rejection of the technology is essential.

INTRODUCTION

Acceleration of the use of CCS to provide significant CO_2 reductions requires close integration of technical, economic and environmental disciplines to support the case for CCS projects. These disciplines have a vital role to play in assisting and informing the decision-making process related to permitting, conformance and securing containment during the execution phase of CCS project.

In addition, potential societal acceptance and embeddedness must also be considered as part of the decision-making and risk assessment process.

For any new project, effective engagement of stakeholder groups is essential for addressing critical concerns in the planning of regional developments. Where there is the use of new or unfamiliar techniques, technologies or materials, there is an added imperative to consider such concerns and how these could affect the project.

SOCIETAL EMBEDDEDNESS

Lack of societal acceptance is often mentioned as a risk for the successful deployment of energy storage projects (Ref.1). However, research has shown that societal opposition is often a response to the project development strategy and the format of the decision-making process (Ref. 2 and 3).

As industry began to develop an increasing awareness of societal issues, it became clear that better insight into the deployment of a new innovative technology was required, and the ACT II DigiMon project made a first step with the Societal Embeddedness Level (SEL) method. This method proposes that industries and regulators organise a feedback loop to translate insight into societal risks into risk governance strategies, incorporating both technical and societal risk reducing measures.

© Shutterstock

The SEL-based research on the societal embeddedness of CO_2 storage projects concluded that CO_2 storage monitoring cannot in itself solve all societal acceptance challenges regarding CO_2 storage initiatives (Ref. 4). Instead, CO_2 storage monitoring forms a part of a broader risk governance strategy for industry and governmental authorities (Ref. 5).

Therefore in order to design an innovative, cost-effective and societal accepted risk governance strategy for CO_2 storage projects, current methods and risk assessment tools, which tend to focus on environmental, technical and economic risks, should also take societal (Ref. 6) and regulatory risks into account (Ref. 7).

DEVELOPING A RISK ASSESSMENT FRAMEWORK

The RamonCO project is a pan-European research consortium with the objective of understanding risks to societal acceptance and development of risk governance strategies, and Risktec is a partner in the consortium.

The RamonCO project is ongoing and is extending the field of application of the SEL Assessment Framework (Ref. 8), as previously applied to CO_2 storage projects (Ref. 9), to all stages of the CCS value chain, namely:

- Capture
- Transport
- Storage
- Monitoring

Focus groups with stakeholders and public surveys are being used to increase the understanding of relevant risks along the whole CCS process chain. Broadening the scope of the SEL methodology provides a better insight, at an earlier stage, into the societal acceptance challenges which may present risks to the business case and societal embeddedness of CO_2 storage activities.

THE BOWTIE METHOD

As the RamonCo project progresses, it will look to build on the SEL method and its output from earlier studies. The bowtie method has been selected as an appropriate tool to deepen insight into the causes of the identified societal risks, the potential consequences, and any possible preventative or mitigative measures (Ref. 10).

Use of the bowtie method will provide an established risk assessment technique that allows detailed analysis of prevention and mitigation measures for specific hazards. The bowtie diagrams will be developed in workshops with experts, stakeholders and the public, covering the four SEL dimensions (Ref. 8):

- Environmental impact
- Stakeholder involvement
- Policy & regulations
- Market & finances

RISK GOVERNANCE STRATEGIES

Based on the outputs of the bowtie studies, RamonCO will ultimately develop societal risk governance strategies and tools for those risks that have been identified as particularly important, using a participatory and interdisciplinary approach (Ref. 4).

The participatory process will consist of workshops with experts, stakeholders and the public to discuss the risk governance strategies. To maximise their applicability, these risk governance strategies and tools will be connected to the interests, language and decision-making routines of, for example, monitoring authorities, permitting authorities, industries and storage operators.

The validated risk governance strategies and tools will then be used to give insight in the Value of Information approach, for a cost-effective and societally acceptable decision-making process and overarching risk governance design.

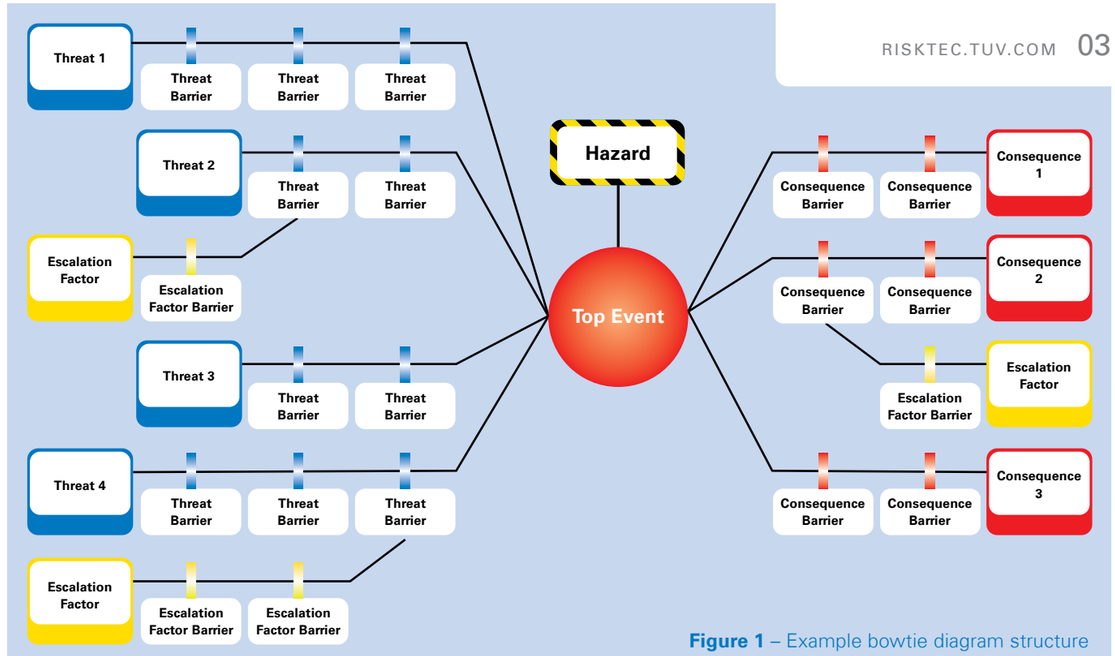


Figure 1 – Example bowtie diagram structure

CONCLUSION

Currently, risk assessment of CCS and CO_2 storage projects rely on techno-economic parameters, but do not tend to consider the risk to the project posed by societal non-acceptance. By integrating the SEL method and including societal concerns within established risk analysis and tools, a more comprehensive assessment of risk can be used to support the deployment of CCS.

This can have a potentially profound impact on the planning and FEED phases of projects, as well as the permitting process, and enable operators, regulators and society to better comprehend and align on risk related to CO_2 storage.

Contact: Andrew Bannister
andrew.bannister@risktec.tuv.com

References:

1. Duijn, M., J. van Popering-Verkerk, K. Sambell, H. Puts (2022). Exploring a value-sensitive design approach to participatory monitoring for improving the societal embeddedness of geothermal initiatives – Insights from the Dutch LEAN project initiative. Conference paper for the EGC 2022 conference.
2. Brus, C., & H. Puts (2020). CO_2 Storage Best Practice indications from Rotterdam area community – Lessons learned from a long-term collaborative research process with a group of Dutch citizens: towards societally embedded CO_2 geological storage projects. TNO Deliverable D5.4 of the EU H2020 ENOS project.
3. Winters, E., H. Puts, J Van Popering-Verkerk, M. Duijn (2020). Legal and societal embeddedness of large-scale energy storage. TNO report TNO 2020 R11116, deliverable for the national research project 'Large Scale energy storage in Salt Caverns and Depleted Gas Fields (Acronym: LSES).
4. Otto, D., Sprenkeling, M., Peuchen, R., Nordø, Å. D., Mendrinos, D., Karytsas, S., ... & Puts, H. (2022). On the organisation of translation – An inter-and transdisciplinary approach to developing design options for CO_2 storage monitoring systems. Energies, 15(15), 5678.
5. Larkin, P., Leiss, W., Arvai, J., Dusseault, M., Fall, M., Gracie, R., ... & Krewski, D. (2019). An integrated risk assessment and management framework for carbon capture and storage: a Canadian perspective. International Journal of Risk Assessment and Management, 22(3/4).
6. Selma, L., Seigo, O., Dohle, S., & Siegrist, M. (2014). Public perception of carbon capture and storage (CCS): A review. Renewable and Sustainable Energy Reviews, 38, 848-863.
7. Zhang, H. (2021). Regulations for carbon capture, utilization and storage: Comparative analysis of development in Europe, China and the Middle East. Resources, Conservation and Recycling, 173, 105722.
8. Sprenkeling, M., Geerdink, T., Slob, A., & Geurts, A. (2022). Bridging social and technical sciences: Introduction of the Societal Embeddedness Level. Energies, 15(17), 6252.
9. Mendrinos, D., Karytsas, S., Polyzou, O., Karytsas, C., Nordø, Å. D., Midttømme, K., ... & Puts, H. (2022). Understanding Societal Requirements of CCS Projects: Application of the Societal Embeddedness Level Assessment Methodology in Four National Case Studies. Clean Technologies, 4(4), 893-907
10. de Ruijter, A., & Guldenmund, F. (2016). The bowtie method: A review. Safety science, 88, 211-218.

Hydrogen fuel cells – functional safety considerations

Hydrogen fuel cells potentially have an important role to play in the energy transition, particularly with the use of fuel cells to power vehicles and machinery. However, as hydrogen can present a significant safety risk, what role do functional safety standards play in the lifecycle of fuel cells?

INTRODUCTION

Hydrogen fuel cells have potential to play a key role for many industries in their transition to provide greener, more sustainable energy, and this is particularly true of the industrial and automotive industries and the applications for machinery, cars, buses and trucks.

However, due to the properties of hydrogen, any loss of containment presents a significant safety hazard, including a high risk of an immediate or delayed ignition and subsequent explosion. Dependent upon the scale of the hydrogen system, this can lead to potentially catastrophic consequences.

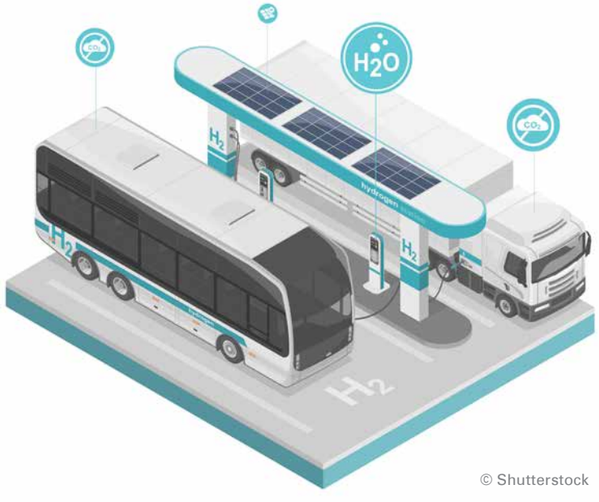
Thorough risk assessment and management is therefore required, and this includes consideration of the type of fuel cell, its ultimate use and the functional safety considerations which this implies.

FUEL CELL TYPES

The main function of a hydrogen fuel cell is to produce and provide electrical energy to a system by utilising hydrogen from an external supply and oxygen from filtered air. The subsequent redox reaction provides electrical energy and pure water as waste product (Figure 1).

Although ultimately performing the same job in the same way, fuel cells can have different configurations and characteristics. For the purposes of functional safety this is best considered at a high level by function delivered, for example:

- A stand-alone fuel cell without machinery directly attached; or
- A fuel cell with a machinery directly attached and housed within one system enclosure.



© Shutterstock

Figure 1 – Example hydrogen fuel cell vehicles

This distinction is important, as it impacts the relevant functional safety standard to follow, and the associated Safety Integrity Level (SIL) determination process.

INDUSTRIAL APPLICATIONS

For a stand-alone fuel cell without machinery directly attached, IEC 61508 (Ref. 1) is applied, and where the fuel cell powers directly attached machinery within one system enclosure, IEC 62061 (Ref. 2) and ISO 13849-1 (Ref. 3) apply.

Focussing on stand-alone fuel cells falling under IEC 61508, a checklist-based hazard identification is utilised. Often, the number of identified hazards is quite high, and a phased approach in the determination of the SIL can be used.

The first phase is the use of the risk graph methodology. The risk graph method is assumed as overconservative for SIL determination, therefore any hazards rated as without a SIL requirement during this conservative risk graph assessment can be assumed to have a non-SIL rating if a less conservative approach was used. The example risk graph calibrations in IEC 61508-5 can then be utilised to get the first indications for the SIL rating.

The second phase is to utilise a less conservative approach, such as Layers of Protection Analysis (LOPA), to assess the remaining hazards. Based on the risk graph analysis and the follow-on LOPA, the SIL ratings can be determined and allocated to certain functions and equipment, leading to the identification of the Electrical, Electronic and Programmable Electronic (E/E/PE) safety-related systems.

IEC 61508:2010		ISO 26262:2018		Comment
SFF	SIL	SPFM	ASIL	
< 60%	n/a			
60 - < 90%	SIL 1		ASIL A	ASIL A satisfies SIL 1
90 - < 99%	SIL 2	≥ 90%	ASIL B	ASIL B satisfies SIL 2 (SFF 90-97%)
	SIL 2	≥ 90%	ASIL C	ASIL C satisfies SIL 2 (SFF 97-98%)
≥ 99%	SIL 2	≥ 99%	ASIL D	ASIL D satisfies SIL 3

Figure 2 – ASIL-SIL mapping (HFT 0 and Type B)

AUTOMOTIVE APPLICATIONS

Automotive safety uses the ISO 26262 functional safety standard (Ref. 4) which is very prescriptive regarding the risk assessment methodology.

While in IEC 61508 the safety functions are determined as for industrial applications, ISO 26262 identifies the hazards based on the vehicle function with this recorded in the hazard register.

The hazard register is used in conjunction with a situation catalogue, which depicts basic situations and their parameters for use in hazard and risk analysis, for example VDE 702 (Ref. 5), to determine Automotive Safety Integrity Levels (ASIL).

The criticality and therefore the ASIL rating of the fuel cell also depends on the application of the fuel cell. Typical vehicle applications are:

- Provision of electrical energy to the powertrain
- Provision of electrical energy to auxiliary equipment
- Provision of electrical energy to secondary power storage (e.g. a battery pack)

IEC 61508 IN THE AUTOMOTIVE ENVIRONMENT

The ISO 26262 standard assumes that some vehicle types represent a quasi-industrial application, and this is the case for Truck and Bus (T&B), trailers and semi-trailers which are large and assumed to be produced in low quantities.

Within ISO 26262-8, Clause 16 describes how equipment developed according to other functional safety standards can be utilised for use in these quasi-industrial applications. One requirement is to justify the application of this clause by providing evidence of a functional safety compliant development.

Assuming an IEC 61508 development, an appropriate mapping of the SIL and ASIL for a Hardware Fault Tolerance (HFT) of 0 and Equipment Type B is shown in Figure 2. In this case the Safe Failure Fraction (SFF) and the Single Point Failure Matrix (SPFM) are used to map both standards.

The main weakness of this approach is that the application in industry and the automotive sector are different. While an industrial environment is a protected environment, in automotives the fuel cell is used within the public domain, with the associated potential of fatalities in the event of a loss of containment and a subsequent explosion. This might lead to differences in the SIL and the expected ASIL rating.

In ISO 26262 the safety functions are on vehicle level, and in cases where the hydrogen system includes equipment outside the fuel cell system boundaries, additional measures may be required to achieve ASIL D. Additional measures at vehicle level may include hydrogen sensors throughout the driver cabin, chassis, passenger or goods compartments, as well as measures around the hydrogen storage tank. This means that any gaps in the ASIL rating between equipment design and safety function requirements need to be addressed at an overall vehicle level.

CONCLUSION

Where hydrogen fuels are expected to be used in the industrial and automotive setting, it is important to recognise the different consequences, protection measures available, and ultimately the standards which drive the functional safety needs of the system.

Integration of non-ISO 26262 equipment into T&B applications is possible, but the conclusions from previous functional safety assessment must be used with caution as they may be different in terms of safety functions and SIL/ASIL ratings, even in cases where ISO 26262 Clause 16 is applied.

Contact: Lars Broegelmann
lars.broegelmann@risktec.tuv.com

References:
1. Functional safety of electrical/electronic/programmable electronic safety-related systems, IEC 61508:2010
2. Safety of machinery - Functional safety of safety-related control systems, IEC 62061:2021
3. Safety of machinery - Safety-related parts of control systems, Part 1: General principles for design, ISO 13849-1:2023
4. Road vehicles - Functional safety, ISO 26262-6:2018
5. Low-voltage electrical installations, DIN VDE 0100-702:2012-03

Is the next big thing in nuclear really small? The rise of the microreactors

Although currently experiencing a revival, the concept of Small Modular Reactors (SMRs) is not a new idea with designs first emerging in the 1950s for a variety of uses. There is currently much interest in even smaller 'microreactors', but what are the features and design considerations associated with these?

INTRODUCTION

As the name suggests, SMRs are small nuclear reactors, which generally have a power capacity of up to 300 MW(e), approximately 2-4 times less than typical commercial size reactors.

An intriguing subset of new SMRS are the so-called microreactors which typically have a power capacity of up to a few tens of MW(e). Currently there are estimated to be more than 80 SMR designs in development, of which over 30 are microreactor projects (Figure 1).

SMR DEVELOPMENT

A key driver for SMR development is the potential to have standardised, factory-fabricated modules which can be readily transported by truck, rail or even air transport to the site of deployment, although for larger SMRs on-site construction of a power station and surrounding infrastructure is still required. For microreactors the potential for the whole reactor system to be factory fabricated, transported to a deployment site and 'plugged-in' as required exists.

Hence microreactors promise shorter and more efficient construction periods and flexible installation which can be expanded with more units added if more power is needed. Some of their potential uses are to provide heat or power to remote communities or industrial applications including sea water desalination, hydrogen production or steel making.

Some designers are considering their use as transportable power 'batteries', for example for deployment to disaster-hit areas or to provide carbon-free load support to intermittent renewable generation. Most recently, the use of microreactors to power AI data centres (Figure 2) has hit the headlines as an early potential use of such reactors.

However, to enable this future for microreactors, there are some key challenges.

DESIGN BASICS

Whereas many (but not all) of the initial wave of SMR designs are based on established reactor designs (e.g. pressurised water reactors or boiling water reactors) albeit often with enhanced passive safety systems, the majority of microreactor designs are at the vanguard of the next generation of what are termed 'advanced reactors'.

Many of these advanced microreactor designs shift the dial in terms of their fuel, cooling technology, control requirements and safety philosophy. For example, many microreactors are proposing to use higher enrichment fuel than standard designs. Some propose to use robust ceramic-encapsulated fuel pellets which are resilient to failing in accident scenarios.

When it comes to heat removal and emergency cooling, we start to see real differences from traditional nuclear designs. Systems based on helium cooling are common due to its low corrosive properties, low neutron absorption and high thermal conductivity, but other systems are under active consideration, including molten salt and liquid metal coolants.

Emergency heat removal is often based on passive systems, for example air convection systems which are either 'always-on' or which are initiated by passive means (e.g. melting a sacrificial plug to initiate the system).

SAFETY DESIGN

From a safety perspective, and to achieve 'walk away safe', microreactors make extensive use of inherent and passive safety characteristics. Designs make use of significant negative temperature feedback characteristics for reactivity, meaning their power is modulated by their physical characteristics with substantial margins against reactivity insertion hazards.

Many designs claim that decay heat can be passively removed from the reactor without the need for active systems and, importantly, without the need for electrical power supplies. Where transportability isn't necessary, many designs are planned to be located in robust underground bunkers which give protection against external hazards.

Figure 1 - SMR designs in development globally (Ref. 1)

As SMRs may be located in more remote sites than traditional reactors, additional Unattended Remote Monitoring Systems (USMRs) may also be employed to provide an additional layer of defence and may also be of significant benefit due to their data generation, collection and transmission capabilities.

SECURITY AND SAFEGUARDS

An interesting area to consider is how the security of a microreactor can be assured given their potential uses and their possible remote locations.

Now, more than ever, the principle of 'security by design' is key to project success. This principle requires that the designer seeks to design out security risks and vulnerabilities rather than taking a more traditional approach of adding active protection such as security systems or providing a response to incidents. Clearly, the more that can be done to ensure the inherent security of the design, the better to achieve the potential benefits of this class of reactors.

Although advantages may exist in the use of remote monitoring (or even control) of facilities in distant locations, this will require consideration from a cyber security perspective.

© Shutterstock

Figure 2 - Data centre

KEY CHALLENGES

As an exciting and rapidly developing field which is pushing the traditional approach to reactor design, microreactors will face some future challenges.

Some of these challenges are familiar to us; for example the development of a suitable safety case for the reactor to support licensing and operations. For application to microreactors, this may require new methodologies and guidance, particularly where novel features or new approaches are being proposed, for example in the assurance of passive safety systems, reduced on-site manning levels or incident response. Such features will provide a challenge both to designers and regulators.

As we have seen, microreactors could be deployed in a wide range of locations and on a variety of different sites. For example, a facility could be required in a remote community in the arctic tundra, an earthquake zone (e.g. to support disaster relief) or as part of an industrial complex. Understanding the potential siting envelope for its deployment and ensuring that the microreactor is robust to the hazards it could be exposed to while being economically viable is a significant challenge.

As for all new nuclear facilities, consideration must also be given to their eventual decommissioning. Transportable reactors offer the potential to be decommissioned in a central facility which may streamline the often-complicated process. However, novel aspects, particularly fuels, may not be currently well understood from a long-term storage and disposal perspective.

CONCLUSION

The global demand for sustainable energy in a variety of locations and environments is ever increasing. The small size but rapid and flexible use of microreactors means that they may have a considerable part to play in our future energy needs.

Contact: Mustafa Osman or Emilia Gajda
mustafa.osman@risktec.tuv.com
emilia.gajda@risktec.tuv.com

References: 1. World Nuclear Association. (16. February 2024). Small Nuclear Power Reactors. Von World Nuclear Association: https://world-nuclear.org/information-library/nuclear-fuel-cycle/nuclear-power-reactors/small-nuclear-power-reactors

CSM-RA and EN 50126 - a difference of perspective?

Where the Common Safety Method on Risk Evaluation and Assessment (CSM-RA) must be applied for technical, operational or organisational changes to railway systems in the European Union, railway product suppliers tend to follow EN 50126 to fulfil the risk assessment role. This can lead to potentially complicated interfaces between parties, so how can this be managed?

INTRODUCTION

In the European Union and beyond, Railway Undertakings, which can be defined as "any public or private undertaking which provides services for the transport of goods and/or passengers by rail" (Ref. 1), must apply the CSM-RA (Ref. 2) for changes to the operational network. Railway product suppliers are not required to, and usually do not, follow CSM-RA. They instead choose to follow EN 50126 (Ref. 3) which, although Reliability, Availability and Maintainability (RAM) focussed, also provides a method of managing safety.

Whilst the two standards have differences, they fundamentally cover the same scope, with the Control, Command and Signalling (CCS) National Technical Specification Notice (NTSN) stating that compliance with EN 50126 (along with EN 50128, 50129 and 50159, as applicable) is "a means to fully comply to the [CSM-RA] risk management process" (Ref. 4).

UNDERSTANDING THE DIFFERENCES

A simple example of the differences between the standards is the different stated aims of hazard identification.

Under CSM-RA the aim is to identify "all reasonably foreseeable hazards", a broad goal that would include minor accidents from a range of causes. However EN 50126 states that: "The purpose is not to catalogue every trivial hazard", implying a focus on hazards with a higher severity.

This and other differences in approach can lead to potentially complicated interfaces between parties, overlap and gaps in external assessment and the development of safety arguments.

At a broader level, the differences in the standards can be best understood in the context of applying CSM-RA at the railway system level and EN 50126 as a process for incorporation of Safety Critical Systems into that system. It is useful to think of this as four separate, but connected, aspects:

- Scope
- The Safety Case
- Verification & Validation
- External Assessment


© Shutterstock


© Shutterstock

SCOPE

CSM-RA covers changes of a "technical, operational or organisational" nature, a wider prevue than stated in EN 50126 which covers "Command, Control and Signalling, Rolling Stock and Fixed Installations", noting that there is no mention of operational or organisational changes in this definition.

This difference speaks to the assertion that CSM-RA applies better to the operator, at rail system level, as the implementer of day-to-day activities on the railway.

EN 50126, on the other hand, provides a method for making a safety argument at the generic product or generic application level, where CSM-RA provides no guidance. EN 50126 essentially provides a method for the development of a system, but without clear knowledge of the way in which it will be used.

THE SAFETY CASE

The biggest difference in terms of the output of the safety management process is perhaps the requirement for a safety case. EN 50126 requires the production of a document that outlines; "the documented structured safety justification which provides the evidence of how the system under consideration complies with the specified safety requirements, within the defined scope of its proposed use", or a safety case to you and I.

CSM-RA has no such requirement, however the intention of the safety case is somewhat achieved through other means. The Hazard Record is used to provide evidence of closure of Safety Requirements (called Safety Related Application Conditions (SRACs) under EN 50126) and independent assessment is undertaken throughout the process. Safety Requirements applicable in operation are usually transferred on to the Railway Undertaking for management.

VERIFICATION & VALIDATION

Verification and validation provides assurance through the project lifecycle that requirements are being developed and met correctly. EN 50126 uses the V model to represent the lifecycle, with specification and verification of requirements a central aspect of the model.

CSM-RA does not mention verification or validation in its process at all in relation to the management of Safety Requirements, but does acknowledge that verification is required within CSM-RA through the wider Safety Management System (SMS).

The level of independence required in EN 50126 is focussed around the level of risk in question, again implying a focus on specific higher level risks than CSM-RA, where a broader set of hazards is implied.

INDEPENDENT ASSESSMENT

External independent assessment differs greatly between the two processes. The Independent Safety Assessor required under EN 50126 is required, amongst other responsibilities, to "give a professional view on the fitness of the developed outcome for its intended use". This is a higher bar than that provided under CSM-RA, in which The Assessment Body is tasked with assessing that the process has been applied, as well as evaluating the results produced by the process.

Again, the outcome here is a potential difference in the level of assurance being provided by the two bodies, and therefore an implication on the types of risk expected to be managed under it.

CONCLUSION

The differences between CSM-RA and EN 50126 can be viewed as a difference in perspective. EN 50126 is a more highly controlled process focussed on the detailed analysis of fewer higher risk hazards, taking a bottom-up approach. It aligns more to the development and integration of specific safety products, such as a Train Protection & Warning System (TPWS) or a points machine.

CSM-RA, on the other hand, is top-down focussed assessment of a change to the railway system, and aims to manage a wider set of hazards, including those with a lower risk level.

EN 50126 can therefore be too onerous and focussed to be the best approach for projects with a broader range of lower risk hazards, but when interacting with CSM-RA, there is the ability to rely on EN 50126 compliant safety cases to make the specific safety argument for Safety Critical components.

Contact: Sam Sellers
sam.sellers@risktec.tuv.com

References:
1. https://www.legislation.gov.uk/eur/2018/643/2020-01-31/data.pdf
2. Office of Rail and Road, Common Safety Method for Risk Evaluation and Assessment, Guidance on the application of Commission Regulation (EU), 402/2013, September 2018, https://www.orr.gov.uk/sites/default/files/om/common-safety-method-guidance.pdf
3. Railway Applications. The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS), BS EN 50126, Nov 2017
4. September 2018 National Technical Specification Notice, Control, Command and Signalling (CCS), 1 January 2021, https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fassets.publishing.service.gov.uk%2Fmedia%2F5fe0972b8fa8f5149718d66c%2FNTSN_Control__Command_and_Signalling__CCS_.odt&wdOrigin=BROWSELINK

The task at hand - SCT vs SCTA

With Safety Critical Task Analysis (SCTA) receiving increased attention in recent years, this can lead to confusion with the term Safety Critical Tasks (SCTs) used in bowtie assessments. But do these overlap? And can the techniques be considered as complementary?

INTRODUCTION

Where control measures or barriers involving hardware have a relatively well-known path for managing long-term effectiveness, the approach to managing human tasks which prevent or mitigate major accidents can sometimes be less clear. The successful completion of these tasks can have a major impact on the management of hazards, so it is vital that such tasks are identified and managed in a logical, measurable and coherent manner.

There are various techniques available to support this aim, with 'SCT' and 'SCTA' often being discussed and considered as key terms and methods for identifying and managing such tasks.

TASKS

The International Association of Drilling Contractors (IADC) defines a HSE Critical Activity/Task as an "activity or task which provides or maintains barriers" (Ref. 1) which is a definition often used for bowtie analysis. Another definition, this time from the Energy Institute and with a Human Factors (HF) perspective, defines a Safety Critical Task as "a task where human factors could cause or contribute to a major accident." (Ref. 2).

These definitions are essentially saying the same thing – critical tasks have a role to play in the management of Major Accident Hazards (MAHs), and as such require detailed consideration and analysis, with the SCTA and bowtie methods both potentially having a key role to play.

BOWTIE SCTS

The bowtie technique is commonly applied to hazards which have been identified as presenting the highest risk level at the company or site, the MAHs. For each MAH at the site, there is a corresponding bowtie diagram which identifies the barriers in place to prevent control of the hazard being lost, or to mitigate the consequences if control is lost. These barriers will be hardware (Safety Critical Elements), tasks/activities which people perform (SCTs), or a combination of the two.

Where an SCT is identified within the bowtie, supporting information is also recorded, including:

- The person responsible for completing the task
- The procedure associated with completion of the task, so the individual knows how and when to do the task
- The means of verification of completion of the task

The bowtie method gives a robust means for identifying the tasks and the role they play in protecting against specific threats or mitigating the consequences of major accidents.

Generally, however, the bowtie will not investigate the individual steps or actions taken when performing the SCT itself, and this is where SCTA is of benefit.

SCTA

Human psychology and physiology are not flawless, and therefore the fact that human error that can often be a potential contributor to major accidents, is an inherent part of every workplace.

Managing human failure and optimising performance are key to accident prevention, and this is best achieved by designing systems that work for people (i.e. are inherently safe), rather than relying on individuals to prevent accidents.

SCTA is a workshop-based method which identifies and analyses SCTs by assessing the task in detail, identifying types of potential human failures involved in the task, and recognising Performance Influencing Factors (PIFs) which make failures more or less likely. This analysis then assesses the measures in place to control and mitigate human error, as well as recommending additional measures where appropriate.

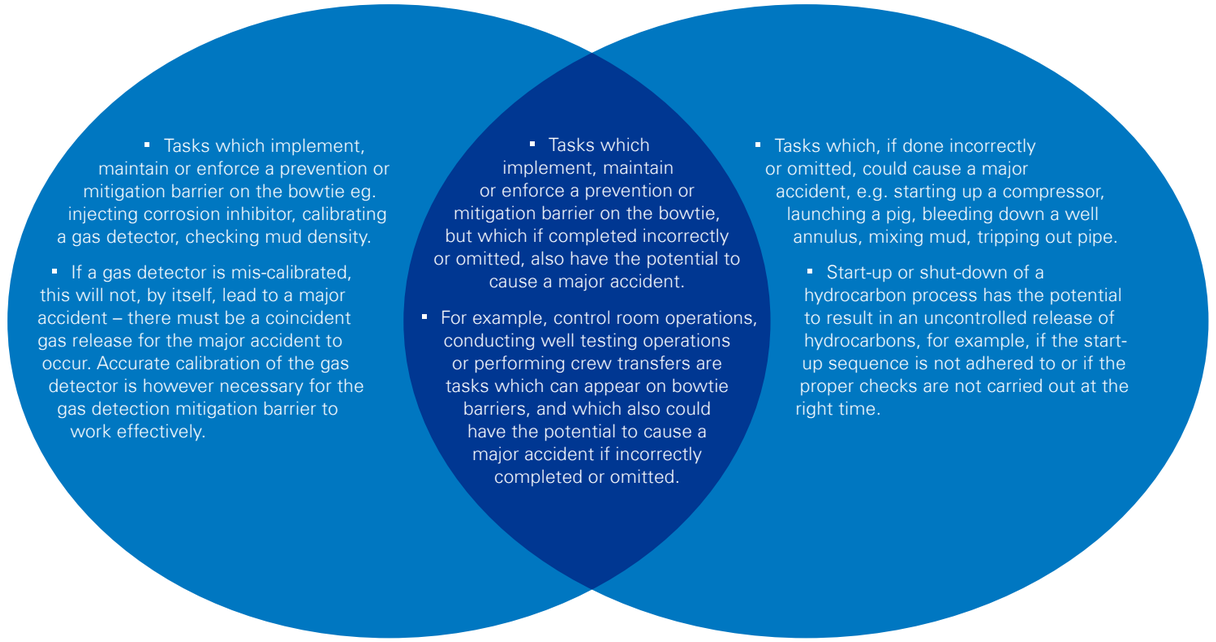


Figure 1 - Overlap of bowtie SCTs and SCTA SCTs

PREPARING FOR SCTA

In preparation for conducting SCTA, a screening exercise is undertaken to determine which on-site activities can be deemed 'safety-critical' and therefore require further assessment.

Often the list of procedures from the asset is a starting input for the screening exercise, however this is not a guaranteed way to catch all activities performed. There may be some not covered by procedures, so individuals are encouraged to consider all activities they perform.

UTILISING BOWTIES

So, knowing that there is a list of SCTs and their associated procedures from the bowtie analysis begs the question, how can we use this information in SCTA?

The answer is that to use it, we must also acknowledge the limitations. Where a bowtie's strength is in identifying SCTs which have a role to play in the management of MAHs, it is not necessarily capable of catching all SCTs which can directly cause a MAH. The bowtie analysis may also not have considered scenarios outside of normal operations, for example start-up or shut-down (see Figure 1).

The bowtie-identified SCTs do however provide additional insight into which tasks and procedures have a role to play in MAHs. The detailed bowtie workshop has assessed every MAH, with consideration of human involvement on a threat-by-threat, consequence-by-consequence basis.

Due to this direct linkage to MAHs, the bowtie-generated SCT and procedure list therefore provides more detail regarding activities which require SCTAs than just a general list of company or asset procedures without context.

Utilisation of the information from the bowties at the SCTA screening stage, as well as input from individuals, procedure listings and other studies, can therefore ensure that all SCTs and associated procedures are captured from the outset of the SCTA process.

CONCLUSION

Where a task has been deemed as 'safety critical' this implies that if the task is completed incorrectly, or not done at all, there could be a serious safety implication.

These tasks can be identified and analysed in different ways, and it is important to consider that the SCT listing and supporting information from a bowtie assessment can form a useful input into the SCTA process, particularly when considered as part of the screening process.

Utilising the bowtie assessment can help to ensure that no SCTs and procedures have been missed in the SCTA, and can provide extra clarity and the ability to sanity check the output of the SCTA process.

Contact: Jana Mihulkova or David McDade
jana.mihulkova@risktec.tuv.com
david.mcdade@risktec.tuv.com

References: 1. International Association of Drilling Contractors Appendix 1 to Health, Safety and Environment Case Guidelines for Offshore Drilling Contractors, Issue 3.6, January 2015
2. Energy Institute. Guidance on Human Factors Safety Critical Task Analysis ISBN 978 1 78725 165 6, 2nd Edition, January 2020.

Other topical articles from our Knowledge Bank you might enjoy...

DECOMMISSIONING BY DESIGN DESIGNING FOR THE FUTURE

The design of early nuclear facilities often ignored or paid little attention to the future need for decommissioning and dismantling. How, though, can our hard-won lessons learned help inform future designs and make things better for future generations?

INNOVATION VERSUS REGULATION CAN CREATIVITY AND SAFETY CO-EXIST?

Following the tragic loss of the Titan submersible in June 2023, it transpired that its pilot, also the CEO of OceanGate, had argued in 2019 that regulation stifles innovation. We ask to what extent is this generally true, and how can regulation adapt to help foster innovation?

SHARING THOUGHTS ON RAIL SAFETY

For Rail Safety Week, some of our team shared their thoughts on safety and the role it plays on their day-to-day working lives. Three members of our team at varying stages of their Risktec career told us about their experience and thoughts on safety.

DEFINING INHERENT AND RESIDUAL RISK

When reporting a risk assessment there is often a desire to differentiate between the impact that control measures have on the risk level compared to doing nothing. The 'before controls' and 'after controls' risk is frequently referred to as 'inherent risk' and 'residual risk' respectively, but defining these terms is not always as straightforward as it first appears.

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
Bristol
Derby
Edinburgh
Glasgow
London
Rijswijk

Middle East
Dammam
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:
LinkedIn
@TUVRisktec
YouTube
@TUVRisktec