Issue 44 / Autumn 2023

RISKworld

The Newsletter of Risktec Solutions

In this issue

Welcome to Issue 44 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

"For me context is the key – from that comes the understanding of everything"
Kenneth Noland, American painter

With 2023 drawing to a close we have seen another busy year for Risktec with many new faces joining the company and continued demand in all sectors.

There have been many notable projects covering a wide spectrum of industries, technologies, lifecycle phases and safety and risk assessment and management techniques. In this respect, the importance of context, and the part it plays in effective and fit for purpose safety and risk management, is paramount – a theme that we explore in this edition.

We start by looking at the importance of basic terminology – and making sure that everyone is using the same terms in the correct way. That we fully understand any hazards is also fundamental, as we show in a case study of hydrogen that highlights how an appreciation of its unique characteristics can shape the approach and outcome of hazard identification and assessment studies.

Of course, some risks are a legacy of the past, whilst others relate to cutting edge technologies. Two of this month's articles explore each end of the spectrum, and their diverse needs, as we consider why decommissioning is different, before launching into the world of cyber security, with an introduction to threat path analysis.

We also have time to reflect on the sometimes conflicting topics of regulation and innovation, exploring what a good balance can look like now and into the future.

As part of our own focus on consistently meeting our clients' needs in the present, we have again measured client satisfaction in our bi-annual survey, with the most recent results showing that we continue to maintain very high levels of client satisfaction.

Our overall score of 'good' or 'very good' for the technical knowledge of our personnel was 97%; with 99% of respondents saying they would recommend Risktec to other organisations or other parts of their organisation.

I hope you enjoy the articles and find them interesting and even thought-provoking. As always, we welcome your feedback and look forward to your continued support.

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

Launched: Sept 2001 **Projects:** 10,401 **Clients:** 1,982
Employees: 354 **Offices:** 16 **risktec.tuv.com**

TÜVRheinland®
Risktec

Inherently Confusing

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.

INTRODUCTION

Undertaking and communicating an effective risk assessment requires a common understanding of the terminology involved. For starters, 'risk' is typically expressed as the combination of 'likelihood' and 'consequence'. If we credit control measures to reduce the likelihood of an event, or mitigation measures to reduce its consequences (or both), then we reduce our initial risk.

To gauge the effectiveness of control and mitigation measures, it is useful to be able to assess the risk before and after their consideration – which is what is meant by 'inherent risk' and 'residual risk' respectively.

DICTIONARY DEFINITIONS

For a concept that is much used, particularly when using a Risk Assessment Matrix (RAM) to assist in risk assessment, it is perhaps surprising that these terms are so poorly defined in risk management standards. For example, ISO 31000, ISO 31010, ISO 17776, IEC 61508 and IEC 61882 don't even mention the concept of inherent or residual risk, much less define the two terms.

Moreover, there is some confusion across the risk/safety industry. In some cases, the term 'inherent risk' includes existing controls and mitigation measures; and residual risk is the effect of implementing improvements, which is clearly useful to know. This also makes sense from a semantic viewpoint, where according to the Oxford Dictionary, 'inherent' refers to 'a basic or permanent part of something' and 'residual' means 'remaining at the end of a process'. Interestingly, in the nuclear industry, the terms 'unprotected' or 'unmitigated' are widely used in the context of frequency or consequences (or both, i.e. for risk) to convey an absence of safety measures.

Rather than getting bogged down, though, perhaps the lesson here is a simple one: To define terms explicitly as a necessary precursor to risk assessment. In that spirit (for the rest of this article at least), we define:

- Inherent risk as that which exists in the absence of controls and mitigating measures
- Residual risk as the risk that remains after controls and mitigating measures are accounted for
- Improved risk as the risk that remains after the implementation of additional or revised controls and mitigating measures

However, equally correct terms, appropriately defined, could be unmitigated, inherent and residual risk, for instance.

POWERFUL PEDANTRY

As some readers may already have divined, there is a good reason behind this otherwise apparent pedantry: the three types of risk help with decision making. More specifically, inherent risk is a useful litmus test for deciding whether credit for safety-related control or mitigation measures is warranted at all and can be used to screen out hazards from further assessment, allowing more time to be spent on those that really matter.

Once controls and mitigation measures are applied to those hazards that remain, their residual risk allows them to be ranked and prioritised for further consideration by ALARP assessment – i.e. answering the question, what improvement is reasonably practicable, given the level of overall risk? And in judging the merit of available options, one factor will be the risk benefit, which is described by the improved risk (or rather the reduction in risk characterised by the difference between the improved risk and the residual risk of the hazard in question).

PITFALLS AND PUDDLES

This all seems straightforward in principle, but in practice it is easy to lose sight of the underlying reasons for the three types of risk.

A common pitfall when assessing inherent risk is to remove those systems or structures that are normally functioning. For example, if we were looking at the risk associated with the storage of hydrocarbons, it would be perverse to assume that the primary containment was absent (giving a large puddle on the floor). Evidently, failure of this passive (though fallible) engineering still needs to be considered in the inherent risk estimation. What is also interesting about this example is that it is easy to miss the implicit claim on primary containment, which should be explicitly recognised and managed (e.g. through appropriate design and maintenance requirements). If not, it may fail more frequently than estimated or in a more severe failure mode than allowed for.

Inherent risk relates to the chances of a person falling from scaffolding and suffering injury or death as a result; residual risk credits the guardrails and the fall arrest harness, both of which only come into play as the accident unfolds and serve to reduce both the frequency and consequences of the initial fall.

Including the guardrail as part of the 'inherent risk' evaluation may be warranted if there is industry data on falls from scaffolding with guardrails (given this is standard practice) and the only decision concerns how best to further protect against a fall (e.g. fall arrest harness, safety net or soft landing system), noting that this may ultimately be decided on practical grounds.

Another common issue surrounds the use of historic failure data in estimating the frequency of occurrence, such as crane-related dropped load. If, as often happens when using a RAM, the frequency of the hazardous event itself is assessed – e.g. using frequency bands with descriptions such as, "has occurred in industry" – then it can be unclear whether this relates to inherent or residual risk. If the existing controls are industry-standard, then it is likely that the assessed risk represents residual risk.

Assessing inherent risk using a RAM with qualitative bands relating to historical occurrences is therefore very difficult, and great care must be taken to avoid undue pessimism or optimism. In this case, it would be better to gather frequency data on the 'initiating event' – i.e. the cause or causes of the hazard, before credit for controls are taken (e.g. wire rope failure, hoist brake failure, etc.).

In such circumstances, especially if the associated risk is significant, a fully quantitative risk assessment method may be more appropriate than a RAM.

CONCLUSION

There is, quite understandably, some confusion over the terms inherent risk and residual risk, stemming from a lack of definition in risk management standards, from their meaning in the English language and from their inconsistent use.

Whatever terms are used, what's important is the utility of the different measures of risk in supporting decision making, with regard to gauging the extent of assessment necessary and the benefit of improvements. Keeping this in mind, and some of the pitfalls, the key take-away is to define explicitly what is meant by each term so that all involved have a common lexicon.

Contact:
Andy Lidstone
andy.lidstone@risktec.tuv.com

The Element of Surprise

Risk assessment for hydrogen systems

As the use of hydrogen continues to increase, so too does the number of hydrogen related plant and supporting infrastructure. Well-established risk assessment techniques are often a key part of the associated risk assessment process, but what are the key considerations you should know for assessing hydrogen hazards?

INTRODUCTION

In recent times hydrogen has been at the forefront of plans to decarbonise the energy sector, necessitating new and innovative facilities and infrastructure to produce and handle hydrogen.

Whilst hydrogen has, of course, been produced, handled and stored safely by industry for many years, the drive to increase supply in an environmentally friendly way has led to changes in the facilities and processes involved, from small-scale pilot plants to larger plants for mass hydrogen distribution.

Many tried and tested risk assessment techniques have a long track record of successful application across a variety of industries, and their generic nature makes them useful for hydrogen risk assessment, such as Hazard Identification (HAZID), Hazard and Operability Study (HAZOP), Layers of Protection Analysis (LOPA) and Quantitative Risk Assessment (QRA) techniques. However, a bit of thought is needed upfront to tailor them for this specific application.

HYDROGEN PROPERTIES

In common with any risk assessment, it is important to understand the hazard that we are dealing with. For hydrogen, key properties are that it:

- Is a colourless, odourless, and tasteless gas under normal conditions
- Has a very small molecular size, so can easily escape, even from apparently sealed containers (depending on their material)
- Is extremely light – 14 times lighter than air and 57 times lighter than gasoline vapour (Ref. 1)
- Has a high energy content per weight (nearly 3 times as much as gasoline)
- Is highly flammable and has a wide flammability range (i.e. 4% to 74% of the air by volume in comparison to 7% to 20% for natural gas)
- Has a very low minimum ignition energy (0.02mJ) compared to natural gas (0.29mJ) or gasoline vapour (0.24mJ)
- Burns with an almost invisible flame and low radiant heat, making hydrogen fires difficult to detect
- Can cause embrittlement of some metals if molecular hydrogen is transformed to atomic hydrogen, which is readily absorbed, through chemical processes, including corrosion

These characteristics influence the scenarios under which there might be a loss of containment as well as their consequences.

LOSS OF CONTAINMENT

There are many potential causes of a loss of containment event in a process facility, and a great many are as applicable to hydrogen as any other fluid or gas, including human errors, structural failures or external events, such as impacts. There are, however, some factors which are unique to hydrogen, or exacerbated by hydrogen, and therefore require specific consideration.

Hydrogen's small molecular size, low molecular weight and low viscosity gives it the ability to leak at a higher flow rate than other gases. For high-pressure storage systems, hydrogen leaks nearly three times faster than natural gas and over five times faster than propane (Ref. 2).

Hydrogen is also able to permeate through unbroken materials, and has the potential to cause embrittlement, which occurs when hydrogen diffuses into a material, particularly around welds or in castings. Embrittlement becomes an issue when high dynamic stresses occur (e.g. from impacts or load cycling), leading to cracking.

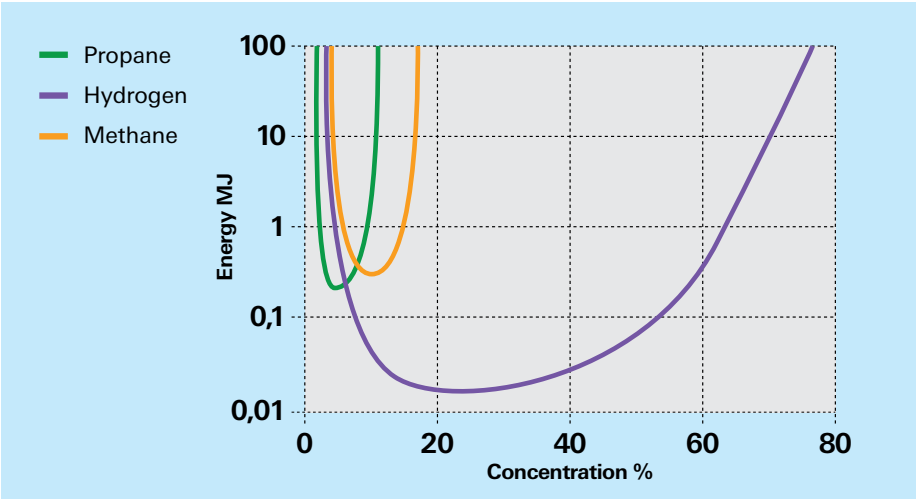


Figure 1 - Ignition Energy and Concentration of Fuel (Ref. 3)

A good example of how to manage leaks and embrittlement is the material selection process, where the discussion typically centres around the use of stainless steel vs carbon steel in hydrogen systems. Fibre Reinforced Polymer (FRP) is another potential option.

Where hydrogen processing involves new or novel equipment, these may bring their own hydrogen-related hazards. For example, electrolysers are commonly used in the generation of hydrogen, but can produce highly corrosive conditions that may challenge containment. Electrolysis also produces oxygen as a by-product, which is not only a new hazard in itself, but also exacerbates the potential for an explosive atmosphere.

CONSEQUENCES

Given its buoyant nature, escaping hydrogen will rise and rapidly disperse in an open environment. However, hydrogen can accumulate in enclosed or congested spaces, mixing with air, with the potential to create a flammable or explosive mixture. Its relatively low ignition energy means early ignition of release is more likely than other gases (see Fig. 1), with jet fire or flash fire a possibility.

Should early ignition not occur under certain conditions, unconfined vapour cloud explosions are also credible. In such conditions, a hydrogen flame front propagates much faster than methane, for example (Ref. 4), which in an over-pressure scenario results in a reduced probability of survival as internal injuries can be more significant.

Where ignition or explosion does not occur, unignited releases also present potential serious consequences:

- A release of hydrogen in a confined space can drive out oxygen with the potential for asphyxiation
- Releases under high pressure can present a threat to personnel safety and can damage plant either due to pressure waves, pipe whip, missiles or extreme cooling
- Hydrogen is a greenhouse gas which has six times the global warming potential of CO_2 – although release to atmosphere may sometimes be the best option from a safety perspective, the environmental effects should not be taken lightly

CONCLUSION

As the scale and technologies of the hydrogen economy develop at pace, it is more crucial than ever that we understand the unique properties and behaviours of hydrogen as they relate to its containment and consequences of release. Only with a firm grip on the hazards of hydrogen can we provide meaningful and insightful risk assessment and help manage the associated risk effectively.

Contact:
Megan Kane
megan.kane@risktec.tuv.com
James Sneddon
james.sneddon@risktec.tuv.com

References:
1. https://h2tools.org/hydrogen-compared-other-fuels
2. https://www.hse.gov.uk/research/rrpdf/rr769.pdf
3. Reproduced from Schmidchen, U (2009), Hydrogen safety facts and myths, 3rd International Short Course and Advanced Research Workshop: Progress in Hydrogen Safety, Belfast, 27th April-1st May 2009, Northern Ireland, UK
4. Hydrogen Safety for Energy Applications Engineering Design, Risk Assessment, and Codes and Standards, 1st Edition, March 25, 2022

The Final Frontier

A paradigm shift in safety thinking

Decommissioning represents the final life cycle stage of any asset, and while its inevitability is ever-present, the unique risks that arise during this stage can present unexpected challenges and require smart solutions.

INTRODUCTION

When an asset such as a nuclear power station, oil & gas production facility or chemical plant reaches the end of its operating life, and refurbishment is not feasible or economically viable, the decision will be taken to begin its decommissioning. For a large, aged facility, this presents a massive challenge, typically requiring a complex and multifaceted process that needs meticulous planning, its own safety case with new safety measures, and a commitment to environmental stewardship. There can be a significant change in the safety and environmental risks normally associated with its operation, all of which must be carefully identified, assessed and managed.

A DIFFERENT MINDSET

Decommissioning requires a shift in thinking compared to new build or operational safety cases, since (for example):

- Hazards are a one-off and the associated increase in risk may be balanced against the longer term risk reduction
- Some hazards may be unknown or have large uncertainties and not be revealed until surveys are undertaken or during dismantling
- Existing systems may be repurposed and operated in ways that they were not originally intended or their performance or reliability may be degraded, given their age
- The introduction of new systems or processes is often highly constrained by existing structures and equipment
- Plant design and as-built/modified configuration information may be out-of-date, hampered by poor record keeping or entirely absent

Figure 1 - The Long Road to Decommissioning the Dounreay Site (Ref. 1)

- Personnel involved with the original design or operation may no longer be available, particularly if there's a long pause before decommissioning begins
- The impact of new legislation and standards will need to be considered, which can prove tricky to navigate when a mix of new and existing equipment and structures is involved

DECOMMISSIONING STAGES

Every decommissioning project is different, but each will almost certainly involve a number of distinct stages as a way to manage the associated risk, uncertainty and timescales. For example, the decommissioning of a nuclear power plant can span decades and is typically divided into three main phases:

1. Immediate Post-Shutdown Phase: This phase begins shortly after the reactor ceases operations for the last time. The focus at this stage is on removing fuel, waste and other hazardous materials from the plant, and safely storing these materials onsite. At this point, the site may enter an interim care and maintenance stage (which could last many years).
2. Safeguarding and Dismantling Phase: During this phase, preparations are made for dismantling the power plant. Contaminated materials are safely removed, and systems that no longer serve a purpose are disconnected. Careful planning is crucial to prevent the spread of residual harmful substances and ensure worker safety. Significant changes to infrastructure may be required, for example removal or addition of roads or transport links, and construction of new buildings as well as the deconstruction of old ones.
3. Final Decommissioning Phase: The final phase involves dismantling the remaining structures and cleaning up the site. Decontamination efforts are intensified, and any residual waste is disposed of in accordance with strict regulatory guidelines. The goal is to restore the site to a condition that allows for its potential reuse or return to nature. This may involve new waste storage and treatment facilities and changes to site utilities such as power and water.

RISK ASSESSMENT

Evidently, there can be changes to hazards and risks both within each stage and between stages – some hazards may be eliminated (which after all is the aim of decommissioning), while other new hazards may be introduced, albeit generally short-lived.

There will be existing safety case resources available from the operational phase, including hazard identification studies and safety assessment, which provide a good baseline from which to identify differences.

Workshops, such as HAZOPs, are an important tool in developing the decommissioning process and understanding the impact on existing systems operating in new scenarios and the requirement for new systems. Questions that are answered include:

- Are the operational hazards and consequences still present and if so, have they changed? Have any new hazards or consequences been introduced? How long will they be present for?
- Is the safety system in question still required under normal conditions or in emergencies? What happens when it is isolated? If it is needed, are the performance requirements more or less onerous?
- When can a system be safely isolated (noting that there still may be an ongoing maintenance burden)? How should this be achieved? Is a new safety system required to replace safety systems that can no longer function or to mitigate new hazards?

If the decommissioning process is labour intensive, workers may be much more exposed to potential hazards than would be the case during the operational phase. New hazards may also relate to waste generation, contamination and environmental emissions; or ongoing maintenance and testing of systems while decommissioning is underway.

Subsequent assessment of the associated risk of decommissioning will typically draw a distinction between quiescent periods, where risk levels are approximately constant, and activities, which may attract a temporary increase in risk followed by a fall in steady state risk as hazards are removed or eliminated. A transparent treatment of unknowns or uncertainties is needed so that risk-based decisions can allow for any associated pessimism introduced as a consequence.

Answering the question invoked by the ALARP principle of what more is it reasonably practicable to do to minimise risk, especially relating to peaks, must take due account of the short time at risk and the final risk reduction achieved. As such, solutions may rely much more on operator action rather than passive or automated safeguards, unless these can be delivered cost-effectively.

DECOMMISSIONING BY DESIGN

While lessons learned can be read across from project to project, at the highest level the greatest lesson is that ideally decommissioning should be designed into all new plant from the outset rather than developed ad hoc at the time. This might involve:

- Dual purpose plant and equipment, such as installed cranes able to lift dismantled plant
- Dual purpose buildings, such as turbine halls that can become waste stores
- A modular design, with units that can be easily removed and refurbished or replaced with purpose-designed plant for decommissioning
- Designing structures in a way that simplifies the demolition process and minimises contaminated waste
- Selecting materials and corrosion tolerances appropriate for the entire lifespan
- Automating the dismantling process where practicable

Alongside this we might imagine a build approval process that requires as much thought about decommissioning as it does for operations; and a culture through life that keeps in mind decommissioning when it comes to modifications, maintenance, record keeping and knowledge capture.

CONCLUSION

The decommissioning of ageing facilities is as inevitable as the rising sun. Lessons learned along the way can be read across from facility to facility, and from industry to industry. Moreover, perhaps this hard-won experience can also inform the development and implementation of new facilities and new technologies to the extent that a considered and future-proof decommissioning plan is built into the design from the outset.

Contact:
Andrew Chan
andrew.chan@risktec.tuv.com
Kerr Gibson
kerr.gibson@risktec.tuv.com

References: 1. Attribution: John at the English-language Wikipedia, https://commons.wikimedia.org/wiki/File:DounreayJM.jpg

Mapping the Cyber Battlefield

The rise of threat path analysis

As we venture ever forward into a digitalised and interconnected world, it is imperative that we take the necessary measures to protect the systems we rely on. However, with the ubiquity of cyber attacks, how do we go about mitigating cyber threats?

INTRODUCTION

The Operational Technologies (OT) environment continues to be a high priority target for cyber criminals. According to the team at Fortinet, three quarters of OT organisations reported at least one intrusion in the past 12 months (Ref. 1). Recent high-profile penetrations of systems include UK police forces and the UK electoral commission.

So, knowing that, what can we do? Whilst there are many steps in creating a comprehensive cyber security management system, one of the most crucial is understanding the potential threat paths and mapping them out.

THREAT PATHS – WHAT ARE THEY?

Threat paths, also known as attack paths, are described as a visual representation of the events that occur when a threat actor (a person conducting the activity) exploits a threat vector and all the interconnected paths to achieve their outcome, such as a ransomware attack.

A threat vector is the means by which a threat actor gains access to the system. In a physical context this could be going through an open door; in a cyber context this could be accessing an unsecure user account.

Understanding paths and vectors allows us to begin plotting out all the physical, digital and human factor-related connections that will ultimately make up a complete threat profile.

WHAT IS THE BENEFIT OF THREAT PATH ANALYSIS?

Threat paths are designed to give the user a way to visualise an attack considering:

- The technical vulnerabilities of a system
- The human interaction element

It enables all the entry points associated with a breach to be identified as the hypothetical attack is developed.

This visualisation in turn provides a more detailed understanding of existing vulnerabilities while allowing a holistic view of how they could potentially be mitigated.

PHYSICAL SECURITY

In the physical world, a threat path is easier to comprehend. It is the path an attacker could take from the border of your facility or from a public area in your facility to the room containing the equipment they wish to compromise. Determination of such paths allows a security professional to place security measures along that path to detect, mitigate or prevent the attack from succeeding. Such security measures could include physical access controls (i.e. doors and walls), CCTV monitoring of approaches and the positioning of security checkpoints to screen all persons passing through the area.

Even in large sites with complex facilities and targets across multiple buildings and multiple floors, clear entrances and choke points, such as stairs, lifts and doors, can be identified for suitable protection. A number of computer programs are available to automatically determine routes from access points to target areas; or in simple cases the assessment can be performed manually using target locations and facility floor plans.

CYBER SECURITY

In the cyber world, there are many variations of cyber security threat paths, with each path unique to the environment under consideration. However, there are some good frameworks that can be used.

A useful resource for considering threat vectors is the MITRE ATT&CK model (Ref. 2 and Fig. 1), which gives example techniques used by attackers. When you combine this with your own system model, the user can begin to identify their key nodes and the associated potential vulnerabilities.

Alongside this, there are many tools available which can support threat analysis, such as the Microsoft threat modelling tool (Ref. 3) which is a free to access platform. Although not necessarily as comprehensive as the MITRE ATT&CK model, it is contained in a user-friendly environment and covers six areas known as STRIDE: Spoofing, Tampering, Repudiation, Information disclosure, Denial of service; and Elevation of privilege.

With the MITRE ATT&CK model and Microsoft threat modelling tool (or one of the many other threat path analysis tools available), it is possible to start answering the question, "Is my cyber system secure?"

WHERE TO START?

When considering threat path analysis, the user needs to consider the initial source of compromise. How would an attacker get in? To answer this, it is essential that a clear understanding of the system architecture is available. Then it's time to look at how the attacker might gather information and move around the system. This process could involve mapping out the interconnection points, such as physical entry, digital entry, human factor weaknesses, and so on. Considerations should include the motive of the attacker: What might they be targeting, what might they be trying to achieve and how would they go about it?

The last part of the puzzle is to predict how an attacker might cover their tracks, what would they need to do to prevent detection during the attack or after they have achieved their goal.

With all these thoughts in mind the user will be in a strong position to build their threat paths and to develop some of the mitigation strategies that may be required to strengthen their security position.

CONCLUSION

It is impossible to protect systems and their parent facilities against unidentified security risks. To help counter this, conducting a threat path analysis exercise provides an end-to-end view of the threats and the extent of their interconnection, while identifying the vulnerabilities and suggesting means of mitigation along the way.

With ever-developing technological advancements it is now more essential than ever to pro-actively map out the security weaknesses of our digital world to ensure that appropriate levels of protection are in place.

Contact:
David Allen
david.allen@tuv.com
Richard Perks
richard.perks@risktec.tuv.com

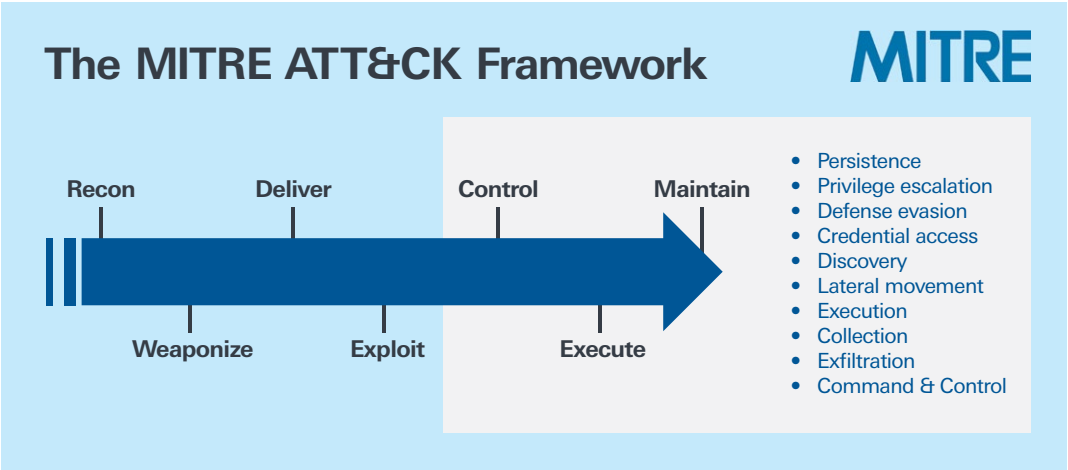


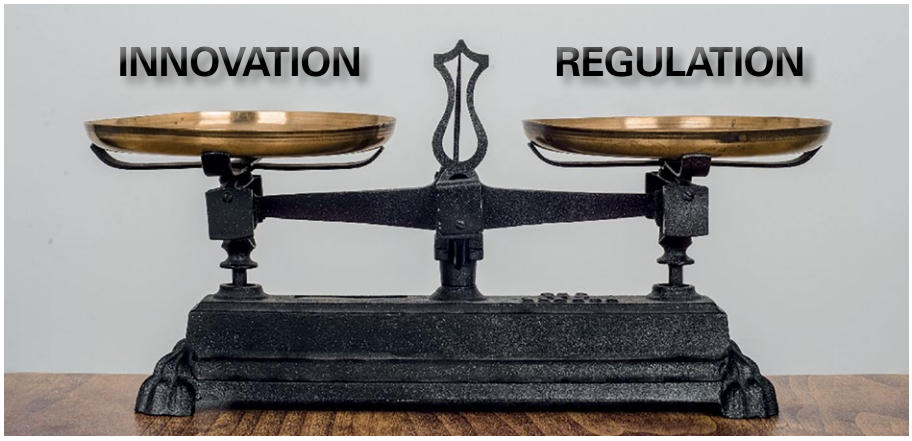
Figure 1 - The MITRE ATT&CK Framework

References:
1. Fortinet Press Release, Fortinet Global Report Finds 75% of OT Organizations Experienced at Least One Intrusion in the Last Year, 24 May 2023
2. https://attack.mitre.org
3. Microsoft Threat Modeling Tool, https://learn.microsoft.com/en-us/azure/security/develop/threat-modeling-tool

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 (Ref. 1). While the causes of the Titan disaster are still under investigation, we ask to what extent is this generally true, and how can regulation adapt to help foster innovation?



Regulation typically arises in the aftermath of major accidents, or from societal concern, with the nuclear industry a good example of both creation stories. Following the demonstration of the destructive power of the atom bomb against the cities of Hiroshima and Nagasaki in August 1945, the subsequent development of nuclear power for peaceful purposes was, understandably, very strictly controlled. In the US, this initially prevented the development of commercial reactors for power generation (Ref. 2). However, once this early reticence was overcome in the 'nuclear power race' of the cold war era, the US Atomic Energy Commission (AEC) was tasked with both promoting and regulating the nascent civil nuclear industry.

REGULATION VS INNOVATION

Interestingly, while it was recognised that an accident could set back the industry by many years, amongst AEC officials there was a common fear of too much regulation, as articulated by Commissioner Libby in 1955: "Our great hazard is that this great benefit to mankind will be killed aborning by unnecessary regulation." Perhaps as a result and certainly because of the rapidly developing nature of the technology, regulation was not overly prescriptive and licence applications were considered on the merits of bespoke safety assessment on a case-by-case basis.

Responding in part to criticism that the AEC's dual responsibility for promoting and regulating nuclear power was like "letting the fox guard the henhouse", in 1975 it was split in two, with regulation coming under the independent Nuclear Regulatory Commission (NRC). Any notion that this reorganisation was too heavy handed was dispelled with the occurrence of the Three Mile Island accident in 1979, which saw a partial core meltdown from an unforeseen combination of equipment and human failures. Subsequent regulatory changes included more stringent requirements relating to operator training, control room design, the use of simulators, review of operational experience of peer plants, and emergency planning and preparedness.

Today, the NRC regulates every aspect of reactor design, assessment and operation, and is regarded as highly prescriptive in its approach. This is proving challenging for the licensing of new technologies, to the extent that NRC has recently proposed an alternative risk-informed, goal-based regulatory framework which aims to be 'technology-inclusive' (Ref. 3).

In the UK, it was the Windscale core fire in 1957 that prompted the establishment of a new regulator, now known as the Office for Nuclear Regulation (ONR). Although the ONR generally takes a more goal-based approach to regulation, the expectation for safety features to be of 'proven design' and to use 'proven materials' (Ref. 4) often means that it is preferable to adopt existing codes and standards and design solutions. The alternative is to undertake extensive and time-consuming R&D to produce the necessary evidence for a high level of confidence, which may be prohibitively expensive or otherwise deter innovation. One example is the selection of reactor vessel material for novel reactors with a high operating temperature (which is desirable from an efficiency point of view). If a designer is limited to steels that are codified by the American Society of Mechanical Engineers (ASME), which provides comprehensive specifications for nuclear applications, they may choose an inherently inferior material with respect to creep behaviour, for instance, compared to potentially superior alternatives that are less well understood or not yet codified.

A MATTER OF TIMING

Regulation is also being shaped by custom and practice, the timing of innovation and the nature of the hazard with respect to the potential number of simultaneous fatalities, all of which shape societal attitude to risk.

An interesting thought experiment is to ask the question: If motor cars had not yet been invented, would they (and roads) be permitted in their current form? In the UK, the Health and Safety Executive (HSE) expects hazards to the general public from work-related facilities or activities to cause no greater than one death in 10,000 per year (the limit of tolerability), with an aim of less than 1 death in a million per year (Ref. 5). In comparison, road traffic accidents in 2022 caused 1,695 fatalities (Ref. 6) which, averaged over a population of 67 million (Ref. 7), equates to 1 death in 39,500 per year. For some individuals (e.g. long distance commuters or pedestrians living near busy roads), their risk will be much higher than the average and may well approach the limit of tolerability (noting, however, that HSE's enforcement responsibility in this respect does not extend to the public highway). Recognising that cars are controlled manually and preventing accidents largely depends on the driver alone, a safety engineer (and regulator) might well conclude that if we were to apply the ALARP principle, we would be obliged to consider what more could be done to reduce risk (over and above existing safety features such as speed limits, seat belts, air bags, ABS brakes, and crumple zones).

Perhaps because of our long-held love of the motor car and the typically singular nature of casualties, this hazard generally falls into a societal blind spot, compared to, say, the hazard of nuclear power, which on paper at least is over an order of magnitude safer. More generally, it appears that the safety bar for new technology will always be higher than if it were pre-existing.

INNOVATION WITH REGULATION

So far, we may conclude that regulation certainly has the capacity to stifle innovation – through overbearingly prescriptive rules, which may penalise or preclude novel solutions; or if safety-related R&D is prohibitively costly or time-consuming.

Flipping this on its head, this means that while there is no such thing as a free lunch, achieving innovation safely and cost-effectively should be possible if regulation is goal-based (so far as is possible); and if R&D programmes integrate safety assurance requirements from the start (rather than adding safety R&D as a bolt-on at the tail end). Another possibility is to back-up innovative safety features with those that are tried-and-tested, as happens with modern nuclear reactor designs where the software-driven shutdown mechanism is backed up by a separate, diverse hard-wired system.

Whilst it goes without saying that operators and designers (and their supply chain) need to be open minded to the safety benefits of innovation in the first place, regulators can also foster innovation pro-actively. For instance, in 2021, the UK's ONR appointed a Head of Innovation, responsible for helping to promote, develop and test the application of new technologies and processes in a 'safe space' – so called 'regulatory sandboxing'.

A recently completed pilot involved regulators and industry and explored the use of Artificial Intelligence through the lens of two diverse applications: a robotically operated glovebox, and in supporting structural integrity claims (Ref. 8). In this way, regulators are informed about the state-of-the-art and can develop their regulatory thinking. The output, in turn, gives industry useful intelligence on regulatory concerns and acceptable approaches for safety justification – all of which breaks down barriers to innovation.

CONCLUSION

Embracing innovation while assuring safety is evidently possible with the right mindset. For operators and designers, this means baking safety thinking into development and testing, so that the evidence needed is produced incrementally and cost-effectively. For regulators it means recognising the potential safety benefits of innovation, adapting regulation (preferably goal-based) and pro-actively engaging with industry to 'sandbox' regulatory approaches.

Contact:
Steve Pearson
steve.pearson@risktec.tuv.com

References:
1. Smithsonian Magazine, A Deep Dive Into the Plans to Take Tourists to the 'Titanic', Innovation June 2019
2. Walker, J. S. & Wellcock, T. R., A short history of nuclear regulation, 1946-2009, US NRC, October 2010.
3. NRC, Rulemaking and Guidance for Advanced Reactors
4. ONR, Safety Assessment Principles for Nuclear Facilities, 2014 Edition, Revision 1 (January 2020).
5. HSE, Reducing Risks, Protecting People: HSE's decision-making process, 2001.
6. Department for Transport, Reported road casualties Great Britain, provisional results: 2022
7. Office for National Statistics, Population estimates for the UK etc: mid-2021
8. ONR, End-of-project dissemination event for AI regulatory sandboxing pilot

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

PEM 101 – AN INTRODUCTION TO PHYSICAL EFFECTS MODELLING

Physical effects modelling forms a key part of risk-based decision making in many industries. Before undertaking any modelling, however, it is always a good idea to revisit the fundamentals of why and how we conduct such a study.

CYHAZOP – BRINGING CYBER TO THE HAZOP

As cyber assessment techniques and tools continue to be invented, it is worth considering what the tried and trusted Hazard and Operability (HAZOP) study methodology could bring to the cyber world.

TOMORROW'S WORLD: THE FUTURE OF RISK AND SAFETY MANAGEMENT

What will the future of our industry look like? The scale of complexity and uncertainty quickly reduces the problem to one of speculation rather than science and engineering. So then, speculating, what does the future hold for the coming 20 years?

ON REFLECTION: ADVANCES IN RISK AND SAFETY MANAGEMENT OVER THE LAST 20 YEARS

We reflect on some of the main advances in risk and safety management we've seen over the first two decades of the 21st century.

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:
@TUVRisktec
LinkedIn
YouTube