Issue 41 / Spring 2022

RISKworld

The Newsletter of Risktec Solutions

In this issue

Welcome to Issue 41 of RISKworld. Feel free to pass this edition on to other people in your organisation. You can also sign up 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 Lewis
steve.lewis@risktec.tuv.com

Contents

"When nothing is sure, everything is possible"
– Dame Margaret Drabble, English novelist

The human tragedy of Russia's invasion of Ukraine makes any articles we write on risk and safety management feel trivial. Our thoughts are with the people of Ukraine at this very difficult and uncertain time. TÜV Rheinland and Risktec's global operation is fully complying with the sanctions imposed on the Russian Federation.

With Ukraine rightly dominating the news, the COVID lockdown restrictions of last year now seem a distant memory. The mitigation provided by the vaccination programmes and the introduction of new treatments have enabled most restrictions to be lifted and a return to more normal working.

Despite the COVID impacts, Risktec had a very good 2021 with growth in the business across all our chosen industry sectors. Whilst in 2020 many projects were suspended or cancelled due to the pandemic and resulting economic uncertainty, we have seen a significant increase in projects with companies looking towards the future and ready to invest.

The clean energy sector in particular saw exceptional growth as we worked with new and existing clients on the energy transition. We supported developments across offshore wind, carbon capture and storage and hydrogen, each with its own unique risk and safety management challenges.

We have increased our focus on sustainability in both assisting our clients in achieving net carbon zero and in all of our own activities. We recently published our updated Sustainability Policy and have been challenging ourselves and implementing actions structured around the 17 UN Sustainable Development Goals.

The most recent client satisfaction survey results were particularly pleasing, confirming we have maintained our high standards throughout times when communication with our clients has been very different. Our overall satisfaction score was 98% and, for the second survey in a row, 100% of respondents indicated they would recommend Risktec to others.

This edition of RISKworld includes an article from 2MC, a sister company, which provides technology-related services to help solve governance, risk and compliance challenges.

We hope you enjoy this edition of Riskworld, and thank you for your continued support.

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

Launched: Sept 2001 **Projects:** 9,330 **Clients:** 1,850
Employees: 320 **Offices:** 16 **risktec.tuv.com**

TÜVRheinland®
Risktec

SPV Management – Simple, but brilliant!

Managing Single Point Vulnerabilities (SPVs) within industrial systems can improve safety, reduce unplanned losses, aid maintenance optimisation and rationalise spares holdings. So what are the main steps needed to establish an SPV management system and realise these benefits?

Equipment reliability plays a crucial role in supporting the safe and profitable operation of industrial plant. Introduction of a management system for SPVs is a simple but effective way of controlling critical components and reducing unplanned losses. But, how many plant operators have a strong understanding of their SPVs?

Whilst there have been notable exceptions – the Boeing 737 MAX aircraft crashes in 2018 and 2019 being two recent examples – safety-related SPVs do not normally exist in highly regulated industries because formal safety cases need to satisfy the 'single failure criterion'. This requires that no single component failure is able to render the safety function of a system unavailable. As a result, the management of SPVs usually focuses on avoiding component failures that adversely affect the availability of a facility.

DEFINING AN SPV

The concept of SPVs has been used within the US nuclear power generation industry for many years, where an SPV is defined as:

"A single component whose failure will lead to an immediate automatic or manual trip of the reactor or turbine."

However, SPVs are not unique to the nuclear industry and their effective management is beneficial to any plant operation where unplanned losses can have a significant business impact.

The first step in the SPV management process is therefore to create an SPV criterion applicable to the specific plant, for example:

"Any single component failure which will result in a loss of production for more than 4 hours."

IDENTIFYING ALL SPVS

Once the definition of an SPV has been established for the specific plant, the process of identifying SPVs can begin.

This process will vary, depending on the complexity of the plant, but is likely to include:

- Review of previous loss events
- Review of the plant maintenance history
- Plant walkdown and discussions with maintenance and operations personnel
- Assessment of operational experience at similar plants
- Review of plant drawings and manuals
- Studies such as failure modes and effects analysis or reliability block diagram assessment

The exercise allows those critical components within a system that meet the defined SPV criterion to be identified and recorded. The number of SPVs identified will vary greatly, depending on the SPV definition and the complexity of the plant.

Figure 1 - Making each SPV highly visible

REDUCING RISK

With all SPVs known, opportunities to reduce the associated risk can be investigated. Elimination of an SPV is the most desirable approach because it completely removes the potential for an unplanned loss. It could be achieved, for example, by installation of a second pump or valve, but it is not always possible or practicable, given layout or cost constraints. In these cases, appropriate mitigation can be put in place to reduce the SPV risk to an acceptable level.

Potential mitigation measures include strategies such as labelling, condition monitoring, maintenance planning and spares optimisation.

Labelling

SPVs can be flagged within the computerised maintenance management system and the equipment physically highlighted on the plant. Such measures help ensure additional care is taken when planning and working on or around an SPV component (also known as a critical component).

One real-life example of successful labelling comes from the UK nuclear industry, where Risktec has been working closely with EDF Energy. To highlight the importance of critical components to all personnel, regardless of their role, EDF Energy has painted them pink (see Figure 1).

This simple and low cost action creates a dramatic visual impact, turning a paper exercise into something which all personnel can easily understand. Immediately, as you enter a plant area, any critical components stand out and everyone is reminded of their importance.

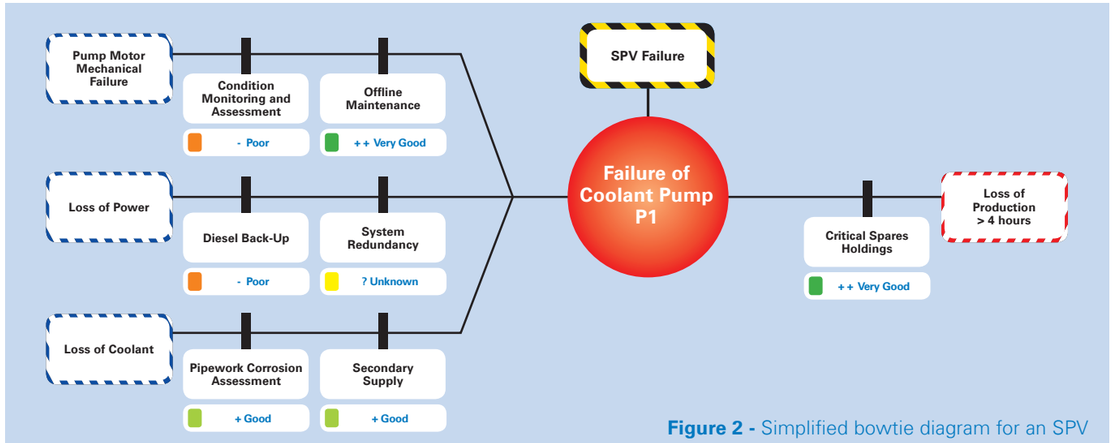


Figure 2 - Simplified bowtie diagram for an SPV

Condition monitoring

Another mitigation measure is the use of condition monitoring techniques. In particular, non-invasive techniques, such as thermal imaging and vibration monitoring, provide early warning of incipient component failure and allow for the optimum planning of corrective maintenance.

Maintenance planning

It is essential that an adequate maintenance plan is in place for all critical components. This plan may include activities such as:

- Assessing physical condition by routine plant walkdowns
- Reviewing condition monitoring data
- Identifying ageing and obsolescence factors and timescales
- Confirming all associated drawings and manuals are up to date and correct
- Evaluating records of previous maintenance
- Ensuring the most appropriate maintenance techniques are utilised
- Verifying that maintenance workers are suitably qualified and experienced
- Requiring that all components used during maintenance are correctly specified and of high quality
- Allowing adequate time for completion of maintenance

It is crucial that the overall plant maintenance strategy finds the right balance between the maintenance of critical and non-critical components. By identify critical components, the SPV management process supports maintenance optimisation and the efficient use of resources.

Spares optimisation

Identifying the timeframe of ageing critical components, together with any obsolescence issues, allows for optimisation of spares holding, which can limit the impact of an unplanned loss. Reviewing maintenance activities with the maintainers can further help to optimise the spares strategy. This can reduce the cost of spares by only holding sufficient inventory to allow a rapid return to service should an unplanned loss event occur owing to a single failure.

MONITORING THE MITIGATION MEASURES

A great way of visualising the mitigation barriers in place for each SPV is through bowtie analysis. The bowtie diagram shows the mitigation barriers for each possible cause of failure of the SPV, as well as the current effectiveness of those barriers (see Figure 2).

REVIEW

Having established an SPV management system, it is vital that it is reviewed on a regular basis to ensure that it remains fit for purpose, especially in light of any recent plant modifications. Based on the bowtie diagram, actions can be taken to ensure the mitigation barriers continue to meet the required level of effectiveness. This will include activities such as regular plant walkdowns, review and update of maintenance plans and analysis of any single failures (or near misses) that meet the defined SPV criterion.

CONCLUSION

Whilst SPVs are a simple concept, do operators really know each SPV at their plant and have a clear understanding of the impact of their failure?

Implementing a simple process for the management of SPVs can reduce unplanned losses, improve safety and optimise maintenance activities and spares holding.

The cost savings from reducing unplanned losses alone are significant. Can you really afford not to implement an SPV management system?

Contact: Steven Roach
steven.roach@risktec.tuv.com

Cyber-space – Emerging issues and solutions in the cyber-security of operational technology

The risk to facilities arising from the cyber threat to industrial automation and control systems – Operational Technology (OT) – continues to attract more attention. But it should not be assessed in isolation. There is a need for a holistic approach to security that recognises the complementary nature of safety and security outcomes and highlights issues and potential fixes in the challenging area of cyber-security.

Let us first consider why cyber-security is becoming such a hot-topic. With increasing emphasis by regulators, governments and international security organisations, it is clear that risks to cyber-security of OT are being taken seriously. As the world moves to a future where computer controlled industrial systems are embraced, this opens up organisations to a greater variety of risks. A clear understanding of, and easy access to, cyber-security risk information is required. Coupled with an increasingly aware public, the potential for major reputational damage means organisations cannot afford to ignore the very real risks introduced by the computerisation of industrial systems.

COMPLEMENTARY OUTCOMES

An understanding of this OT world starts by recognising there is an overlap between safety and security. The required outcomes are complementary, but they can be used to support each other.

Safety protects against unintended events that are hazardous to life and the environment. Security protects against deliberate, malicious acts targeted at creating damage to equipment, process or life, depending on the goal of the threat actor. Collectively, they aim to protect what is important to society and the business.

Notably, for a system to be truly safe, it must also be secure.

IT / OT – WHAT IS THE DIFFERENCE?

The boundary between Information Technology (IT) and OT is becoming increasingly blurred. As more IT based technologies are introduced into the OT space, care must be taken to define their boundaries, recognising their potential effect (or absence of effect) on safety and cybersecurity.

Figure 1 - Six elements for the secure protection of an asset

The definitions of these spaces are individual to each organisation. The two statements below offer a simplistic view of the IT/OT divide, but it is a starting point for further consideration, and offers a guide for organisations in creating their own definitions.

- If it goes wrong and it causes no direct real world physical consequence or no impact on industrial or essential infrastructure services, then it is likely IT.
- If it goes wrong and the consequences could be physically catastrophic to either individuals or wider society, then it is likely OT.

HOLISTIC SECURITY

Increasingly, organisations need to look at security in a holistic way when it comes to protecting their assets. Figure 1 shows the six domains of security, each of which is important to consider when protecting any asset. These domains should no longer be seen as separate layers, but as interconnected elements of security.

The goals and level of rigour applied to each domain will depend on a range of factors such as business goals, the threat environment the asset operates in and the level of resources available to invest in security.

THE ISSUES WE FACE

Many organisations are struggling with the security of their OT and it is not always clear to them where to start. Guidance around cyber-security is frequently skewed to the tactical fix rather than an overall approach to security.

In the past, the need for physical access to, and specialised knowledge of, OT provided some degree of security. Today, the connected, information-driven world we now live in has eroded that protection.

Cost is frequently seen as a large barrier to effective security risk management, with organisations often feeling that financial resources are better spent on products sold to fix tactical cyber-issues. This often leads to decisions being made based on incomplete risk information.

The commonly established cyber-security techniques that organisations rely on for their IT systems do not directly correlate to the objectives and requirements of the OT systems they operate. This can result in security controls that do not effectively perform their function in the OT environment.

The consequences of cyber-attack can be drastically different between IT and OT, and may not be fully appreciated by IT based cyber-security teams. This may lead to misunderstanding of the types of controls needed, the impacts of introducing certain controls and how these should be evaluated.

The cyber community itself has also created its own problems. As an industry, the language that is used is very specific to the discipline. Different approaches are used and, unlike the safety domain where information on accidents is widely shared (in many cases as a regulatory requirement), secrecy is common when it comes to security incidents, thereby missing out on the benefits of learning from shared knowledge.

Cyber-security organisations produce products and sell these as solutions to all cyber-ills and, whilst this is an attractive idea, it is unfortunately flawed. Tactical fixes are very unlikely to solve the overall security risk problem, or be cost-effective in the long-term.

LIGHT AT THE END OF TUNNEL

While this outlook sounds gloomy, there is hope.

Figure 2 - Aligning security with the business goals

Cyber-security consultants can start to match the language they use to the client's environment, ensuring that definitions are consistent and security concepts are introduced in an understandable way.

As Figure 2 illustrates, understanding the most important business goals and translating those to pragmatic security objectives, and then ensuring that the risk assessment outputs and control recommendations are supportive of those objectives, helps to properly target security controls.

Arguably the best way to achieve effective cyber-security is to use processes such as HAZOP and LOPA style studies, building on their success in the safety industry. Cyber-specific HAZOP and LOPA activities can be a very time- and cost-efficient way to assess cyber risk, and are already familiar to the high hazard industrial sectors.

As the discipline moves forward into the future, the most important thing that can be done within the cyber-security space is to learn from other disciplines such as engineering, safety and human factors. Finding and adapting the best techniques from other well-established disciplines will help to guide us to more effective security risk management.

CONCLUSION

The world we live in is at the mercy of rising cyber-security threats. As more connected and computerised technology is introduced into industrial facilities, identifying appropriate controls, measuring their success and understanding their weaknesses, is vital for organisations.

The cyber-security domain needs to look at the engineering and safety worlds to develop holistic approaches and methods to bring cost-effective, impactful security risk management to as many organisations as possible.

Contact: Stephen French
stephen.french@risktec.tuv.com

Uncertain Times – Dealing with uncertainty in quantitative risk assessment: A CCS case study

Effective risk-based decision making relies on an accurate characterisation of the likelihood and severity of possible outcomes. This assessment is guided by experience, honed over time as data are gathered and understanding of the risk improves. But what if there is no track record? What if the risk we are assessing is subject to interpretation and based on assumptions? Here we present a real life example of different approaches that have been applied to risk assessment for CO_2 leakage from the subsurface storage reservoir of a Carbon Capture and Storage (CCS) project.

RISK IN RELATION TO RESOURCE

By definition, risk-based decisions are made on the basis of an estimate of the risk. We devote more energy to reducing the highest risks – particularly where they are found to exceed tolerability thresholds (e.g. the red lines in Figure 1) – confident that we are directing our resources efficiently.

Risk ranking is often quantitative, such that the calculated risk can be compared to these threshold values. However, for any quantification, inevitably there are underpinning assumptions or analyses that have uncertainties attached. It is important to address these uncertainties to ensure we have good confidence that the underlying risk is faithfully represented, and that the efforts to manage it are, in fact, proportionate.

THE UNCERTAINTY ISSUE

Uncertainty is always present when anything is evaluated or estimated. This is especially the case for risk in new endeavours, where novel technologies are implemented or new hazardous activities are undertaken.

Take, for example, the risk of leakage of CO_2 from a subsurface storage reservoir. With the CO_2 storage industry in its infancy, there is only limited operational experience from a handful of storage sites. Coupled with the already tricky task of characterising and predicting the behaviour of geological structures several kilometres below the surface, CO_2 leakage risk assessment is riddled with uncertainty.

One way to handle uncertainty is to err on the side of caution and make conservative simplifying assumptions. This builds in a safety factor and provides reassurance, however it tends to inflate the risk level and may invite excessive scrutiny of the risk (e.g. from regulators or stakeholders), when in fact the actual risk is low. At the same time, it can also lead to a disproportionate allocation of effort and cost in attempting to reduce the risk.

Provided by Global CCS Institute

UNCERTAINTY IN CO_2 CONTAINMENT RISK ASSESSMENT

In the relatively short operational history of CCS there have been several incidents at storage sites. These issues have been predominantly associated with mischaracterisation of the subsurface environment – which is uncertain owing to its heterogeneity and anisotropicity – due mostly to a lack of data. For example:

- At Snøhvit, Norway, injectivity was lower than predicted due to the uncertain nature of the geology. This resulted in a costly redesign with the injection targeting a different section of the reservoir (Ref. 1)
- At In Salah, Algeria, the unrevealed presence of a fault and fracture network in the caprock led to ground uplift surrounding the injection site and the early termination of injection (Ref. 2)

Evidently, unfavourable outcomes can result when:

- The risk is not identified and therefore not managed
- The risk is incorrectly assessed as acceptably low, and therefore not examined in sufficient detail

Quantifying the uncertainty in the estimation of a risk – which is a requirement of ISO 27914 (Ref. 3) – helps us understand our confidence that the risk is not higher (or lower) than expected.

EXPERT JUDGEMENT OF CO_2 LEAK RISK

One typical scenario relates to CO_2 leaking through a fault, eventually reaching the sea bed through overlying rock. For the scenario to occur the reservoir injection pressure limits must be exceeded, the fault must act as a conduit to CO_2 flow, and secondary impermeable layers above the caprock must also fail to contain the CO_2.

How can a numerical estimate of risk be derived?

TOP-DOWN SINGLE POINT EXPERT JUDGEMENT

A starting point is to use expert consensus based on the pre-defined categories of a risk matrix. The likelihood and severity both lie within a range, corresponding to one box on the matrix; as indicated by the black dot in Figure 1, i.e. 'remote' probability and 'serious' consequence.

It is clear that this box is in the 'low' risk band, but what about the uncertainty in this decision? One category either way? More? Less? By using order of magnitude categories we are constraining our estimate.

TOP-DOWN THREE POINT EXPERT JUDGEMENT

Rather than picking a single value for a parameter, it is perfectly possible for assessors to define their own range with minimum and maximum values. Together with the central best-estimate value, this defines a triangular probability distribution. This emphasises the central value and gives less weighting to the low and high extremes, reflecting the judgements made. The ß-PERT distribution uses the same three inputs, but is preferred because it produces a smoother distribution that is a more realistic representation of a real world parameter.

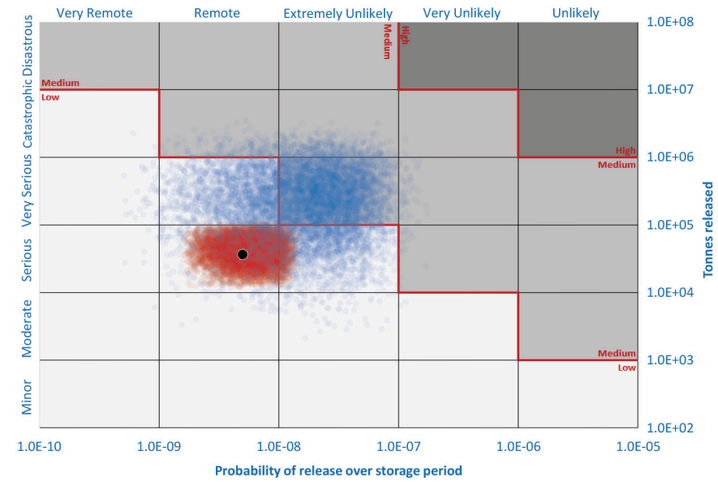


Figure 1 – Expert judgements of CO_2 leak risk

Using Monte Carlo simulation we can sample from the distribution and produce a range of results. For example, applying a most-likely estimate with an order of magnitude range for the minimum and maximum values to both the likelihood and total mass released, 10,000 simulations produces the red cloud of values in Figure 1.

The top-down three-point expert judgement predicts a 91% chance that that the risk is 'serious' and 'remote' (as per the initial single point judgement), but note how some of the simulations result in an 'extremely unlikely' probability, and/or a 'very serious' consequence. Overall, 99% of the simulations predict a low risk.

BOTTOM-UP MODELLING

For a leak path to exist or develop, several barriers must fail. We can apply an approach akin to Layer of Protection Analysis (LOPA) or event tree analysis by multiplying the likelihood of the leak occurring by the probabilities with which the barriers are estimated to fail.

Similarly, the estimated release rate (tonnes per year) and duration (years) can be estimated and multiplied together to yield the total mass lost.

We can extend the idea of parameterising expert judgement through the ß-PERT distribution to each of these parameters, resulting in a bottom-up quantification of the risk.

The results of 10,000 simulations are seen as the large, blue cloud of values in Figure 1. The simulations are even more spread out, reflecting the compounding of the uncertainties by multiplying the tails of several parameter distributions. Just over half of the simulations have crept into the medium risk zone, and about 50% are in the 'very serious' category. We have to conclude that our original single point expert judgement, and even the three point approach, underestimated the true risk.

CONCLUSION

Where data are scarce and expert judgement is required to interpret risks, we should account for the uncertainty explicitly in our estimation of risk.

Taking CCS as a case study for trialling top-down and bottom-up estimations of CO_2 leakage risk, it becomes clear that as uncertainty analysis becomes more refined it can have a significant impact on conclusions.

Contact:
Matt Baggaley or Angus Busby
matt.baggaley@risktec.tuv.com
angus.busby@risktec.tuv.com

References:
1. Shi et al., Snøhvit CO_2 Storage Project: Assessment of CO_2 Injection Performance through History Matching of the Injection Well Pressure Over a 32-months Period, 2013
2. Ringrose et al., The In Salah CO_2 Storage Project: Lessons Learned and Knowledge Transfer, 2013
3. ISO 27914:2017, Carbon dioxide capture, transportation and geological storage – Geological storage

Barrier Management – Driving process safety improvement

Industrial facilities in the process sectors have many barriers in place to prevent or limit the effects of a major accident. But how do we know that these barriers continue to perform their intended function every day, month and year? What information do we need to gather and how can that be displayed effectively?

Internationally acclaimed academic and author Professor Andrew Hopkins, in his capacity as an expert witness at the hearing into the Longford gas explosion of 1998, observed that: *"prior to any disaster there will always be information somewhere within an organisation that trouble is brewing,"* (Ref. 1).

He expanded, *"critical information must not be allowed to lie around unrecognised, ignored or buried like some landmine waiting to be triggered. The challenge is to find ways to assemble this information and move it up the hierarchy to the point where it can be understood and reacted on responsibly."*

PROCESS SAFETY INFORMATION

The assembly of information relating to safe operation of a facility is crucial, as highlighted by Professor Hopkins, and can span many departments and disciplines within an organisation. This is often achieved through the implementation of a robust Process Safety Management (PSM) system, which provides a disciplined framework for managing the integrity of operating systems and processes that handle hazardous substances.

PSM systems are routinely employed within industry, in part driven by the various frameworks and regulations which exist in different jurisdictions, including OSHA PSM regulations (USA), COMAH regulations (UK) and Seveso III Directive (EU). A key component in assuring safe, efficient and reliable operations is the communication throughout the organisation of the critical information contained within the PSM system.

A PSM system may be applied across your organisation but, more generally, how can you ensure that it is robust, it remains so, and that risks inherent in your operations are being appropriately managed?

The development of Key Performance Indicators (KPIs), or metrics, can play a valuable role in revealing the strengths and weaknesses of a PSM programme, and help an organisation work towards achieving and maintaining outstanding process safety performance. This is of particular importance when addressing the identification and control of major accident hazards.

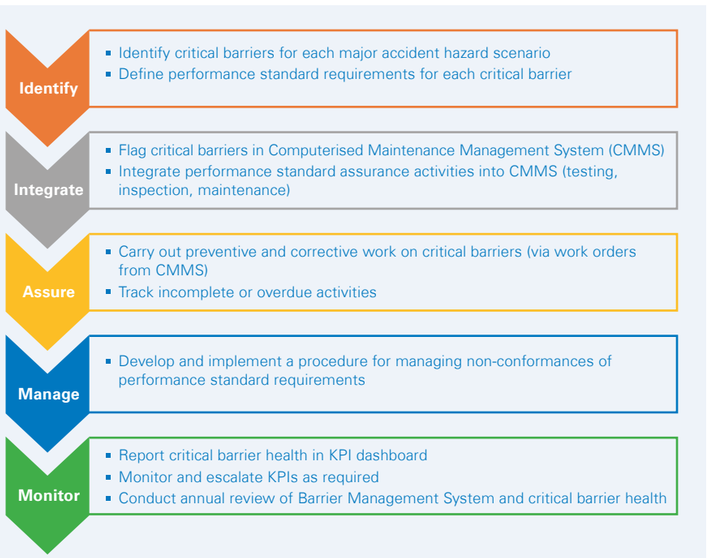


Figure 1 – Barrier management system

SO WHAT DO WE NEED TO KNOW?

At a foundational level, a robust PSM system should allow us all to answer the following critical questions:

1. **What could cause us harm?**
   What are our major hazards that could lead to a potential incident?
2. **What will protect us?**
   What are the critical barriers (safeguards) we rely upon to control these risks?
3. **How do we know?**
   Are we confident the barriers will function as designed when required? What is the minimum level of performance required?
   Are these critical barriers available and effective throughout the life of our asset?

Figure 2 – Example KPI dashboard for a pipeline

A GLANCE INTO THE FUTURE

The first two points are often achieved through the application of standard risk assessment methods (e.g. HAZID, HAZOP, LOPA, bowtie analysis, etc.) whereby hazards are identified, consequences defined and the barriers preventing or mitigating the scenario documented.

This approach determines whether the risks are being appropriately managed. But this determination is like a photograph, a representation that was valid only at the time it was taken. Point 3 challenges us further – how do we assure ourselves that these risks continue to be managed to an acceptable level throughout the lifecycle of a facility? How do we know there isn't a *"landmine waiting to be triggered"*?

BARRIER MANAGEMENT SYSTEM

The concept of barrier management helps us address this concern. The Norwegian Petroleum Safety Authority (PSA) states the purpose of barrier management is *"to establish and maintain barriers so that the risk faced at any given time can be handled by preventing an undesirable incident from occurring or by limiting the consequences should such an incident occur,"* (Ref. 2).

We can provide a level of assurance in the continued effectiveness of our critical barriers by defining minimum testing, inspection and maintenance requirements. The oil and gas industry typically captures such requirements within a performance standard for each critical barrier, but the basic logic holds regardless of application. Figure 1 provides an example flow diagram outlining how a barrier management system can be implemented for the control of major accident hazards.

KPIs

The ongoing health of critical barriers can be monitored though the use of a KPI dashboard, which can inform whether:

- Identified preventive maintenance (PM) tasks are being completed on time
- All requirements of the performance standard are being met for each critical barrier
- The responsible or accountable persons are taking ownership of the critical barriers

Example metrics tracked on a dashboard can include:

- Status of assigned testing and inspection (complete, due, overdue)
- Status of PM and any noted non-conformances
- Critical barrier PM backlog
- Number of PM tasks completed on safety-critical equipment (per time period, per critical barrier type, etc.)

A range of modern business intelligence tools may be leveraged to sustainably build a KPI dashboard, notably Radiant360, PowerBI, Scoro and Datapine. Data can be fed in real-time from the Computerised Maintenance Management System (CMMS) to populate the dashboard.

Figure 2 provides an example of how a set of barrier health metrics can be displayed in a simple, highly impactful way within a dashboard.

The dashboard is accessible to all key personnel, including process unit and asset managers. They would typically interrogate the dashboard on a weekly basis to determine whether the health of the safety-critical equipment is deteriorating and, if that is the case, they know where to focus resources to restore the equipment to good health.

CONCLUSION

The Longford explosion highlighted a deficiency in the way in which many organisations collect and communicate key process safety information. The definition and application of KPIs can help an organisation ensure efficient assembly of this information and, more importantly, highlight and communicate this information up the management chain where it can be acted on responsibly.

The barrier management approach, coupled with a live KPI-based dashboard, enables risks inherent in an organisation's operations to be better understood and hence proactively managed, not only today but through-life.

Contact: James Sneddon
james.sneddon@risktec.tuv.com

References: 1. Lessons from Longford: The Esso Gas Plant Explosion, Hopkins, 2000
2. Principles for Barrier Management in the Petroleum Industry, PSA, 2013

Governance, Risk and Compliance – A technology-led approach to managing risk

Most business leaders are hard-wired to seek growth opportunities and create value by taking risks. Risk management is often an afterthought and usually tackled by silos within the business. But organisations lose value by failing to manage risk routinely – it is crucial for the organisation to know continually what risks it is taking and that they are appropriately managed. Technology-based solutions for governance, risk and compliance (GRC) are being increasingly deployed to help achieve this goal.

WHAT IS GRC?

GRC aims to assure an organisation reliably achieves its business objectives, addresses uncertainty and acts with integrity.

- **Governance** is the corporate processes established and executed by the board of directors and reflected in the organisation's structure and approach to achieving goals
- **Risk** is about managing those threats to the organisation which could prevent it from reliably achieving its objectives (often called ERM - Enterprise Risk Management)
- **Compliance** refers to adhering with applicable laws and regulations, as well as the company's own policies and procedures

GRC aims to synchronise information and activity across these three facets in order to:

- Operate more efficiently
- More effectively share and report information
- Avoid wasteful overlaps

A BRIEF HISTORY OF GRC AND TECHNOLOGY SOLUTIONS

It is generally accepted that the structured approach to GRC arose from the Sarbanes–Oxley Act of 2002 ('SOX'), a United States federal law that mandates accounting practices for corporations. SOX was enacted in response to the major corporate and accounting scandals of the late 1990s and early 2000s, including Enron and WorldCom, which cost investors billions of dollars and shook confidence in public markets. Unsurprisingly, given the complexities of managing different types of risks, the GRC efforts at large corporations in the early 2000s were siloed endeavours. There was the inevitable heavy use of spreadsheets and bespoke databases across functions such as IT, security, legal, finance, HR, HSE and customer service, for example.

By the mid-2000s a few specific GRC tools were coming on the market to help manage the processes and information, although most were focused primarily on IT controls. Today, there are multiple vendor platforms capable of managing the entire requirements of GRC. These digital tools overcome the technological challenges associated with operating global processes and thus remove any need to manage data in silos.

Some tools such as RSA Archer are specifically designed for GRC, whereas others like ServiceNow can do much more than just GRC and are able to automate the workflow for almost any business process.

STARTING THE GRC JOURNEY

When an organisation embarks on its journey towards successful risk management with a GRC programme, it needs to take a structured approach to aligning the GRC global platform with its IT and business objectives. Whilst the initial phase involves the introduction of a set of GRC tools and technologies, enterprises often fail to think through the entire technology implementation and forge ahead without sufficient analysis and planning.

An important first step is a meticulous process analysis to:

- Clearly define the project's objectives and capture the requirements and expected results
- Assess and understand the organisation's data
- Simplify and improve the GRC processes
- Propose a seamless GRC ecosystem of digital tools and technologies

The outcome of this analysis sets the stage for the subsequent design, build, prototyping, implementation, roll-out, training and performance monitoring phases, allowing GRC tools to evolve as the requirements or situations demand.

CONSIDERATIONS ALONG THE WAY

Some GRC projects can stall at the first step, as the organisation struggles to understand its data or gets bogged down in the complexities of its own GRC processes. This is where a technology-based solution can really help. Leading platforms have in-built GRC best practice processes and procedures, all of which can be readily customised. In this way, the technology becomes an enabler, helping the organisation to implement GRC processes more quickly and easily. Improvements can always be made later, following annual performance reviews for example.

Another important aspect of the GRC project is to focus on configuration rather than development. Leading low/no code tools are incredibly customisable and so it makes sense to use this functionality and flexibly adapt processes around the tool rather than unnecessarily over-engineer the tool. Instead of exhibiting a developer mindset – *"I need to re-code the tool to work the precise way I want it to work"* – the project is often better served by reducing complexity and standardising existing processes, with a view to future proofing to meet changing objectives.

The project team must be actively engaged throughout the entire implementation, to deepen stakeholder understanding of the project's objectives and the expected results. An educational approach needs to be taken to ensure users become acquainted and confident with using the tools.

Finally, a key consideration throughout the platform implementation is to address cyber-security threats. This requires a robust approach to risk management, including vulnerability and penetration testing.

CONCLUSION

Organisations reach a size where coordinated control over GRC activities is required to operate effectively. If tackled in a traditional siloed approach, the outcome will be duplicated GRC activities which increase operational costs, or incomplete GRC leading to unknown risk exposures.

In contrast, a GRC technology solution helps organisations to operate more efficiently, communicate more quickly and readily share information. When implementing a technology platform, the opportunity should be taken to create robust, standardised GRC processes to help future proof the solution.

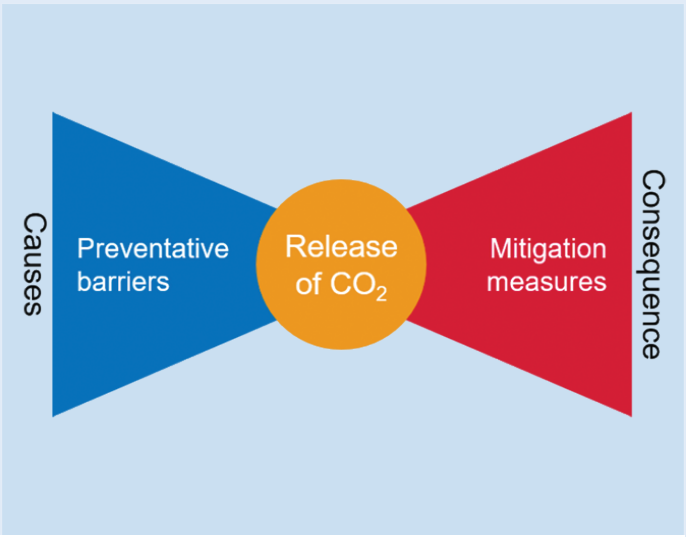
Contact: Dev O'Nion
donion@2mc.co

2MC is a sister company of Risktec and a leading provider of GRC services.

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

THE LEADING EDGE

The essence of good HAZOP leaders

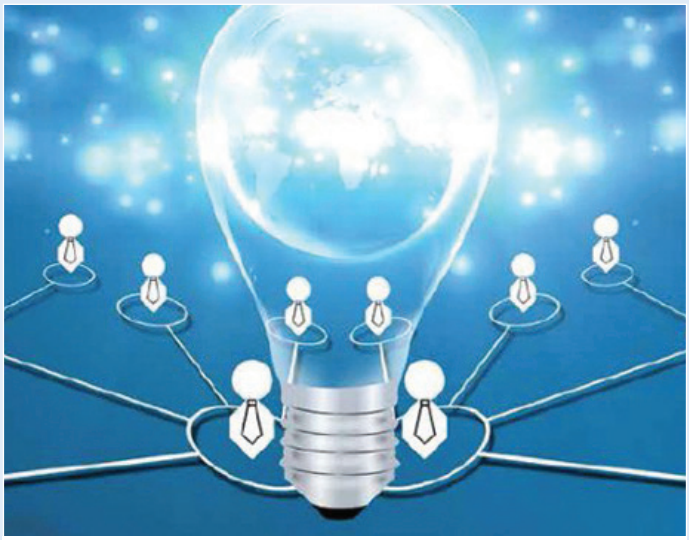


BOWTIE BY NUMBERS

Quantifying bowtie diagrams for carbon capture

THE PRICE OF (SINGLE POINT) FAILURE

Two Boeing 737 MAX aircraft crashed within six months, with the tragic loss of 346 lives



ENTERPRISE RISK MANAGEMENT

How to prevent losses and create value

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