Issue 38 / Autumn 2020

RISKworld

The Newsletter of Risktec Solutions

In this issue

Welcome to Issue 38 of RISKworld. Feel free to pass it on to other people in your organisation. We would also be delighted to hear any feedback you may have on this issue or suggestions for future editions.

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

Contents

Thriving in Adversity

"When it is dark enough, you can see the stars."
Ralph Waldo Emerson

Coronavirus continues to have a significant impact on all our daily lives, transforming the way we work and interact with our colleagues and clients. Remote working and online meetings have become the 'new normal' for many of us. We are extremely proud of our achievements in maintaining an uninterrupted service, while ensuring the wellbeing of our employees, their families and our clients. We continue to put our clients first and learn all possible lessons to help us provide an even more effective service.

The changes in the way we work have resulted in many fantastic examples of our teams developing new innovative and collaborative solutions to support our clients – some of which are featured in this edition of RISKworld. The articles highlight the importance of managing the full range of risks that businesses face, and adapting to fluid situations.

Our client focus is measured by our bi-annual client satisfaction survey. It is pleasing that despite the impact of coronavirus we have been able to maintain very high levels of client satisfaction. During the first half of the year, 98% of clients rated our flexibility and responsiveness as very good or good and 97% said they would recommend us to other organisations. We would like to take this opportunity to thank all of our clients for their continued trust in us.

We have benefited from our diversified business model – across industry sectors, geographic presence and services. All of our sectors, except oil and gas, have continued to grow during 2020. However, the outlook for the rest of the year continues to remain uncertain; no one knows how long the impact of coronavirus will last or how quickly the global economy will take to recover. Our ability to be flexible and responsive will be more important than ever during these challenging times.

We hope you enjoy all the articles, which are intended to spotlight our forward thinking approach. As always, we welcome your feedback and look forward to your continued support. And please stay safe!

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

Harnessing Chaos – The antifragile approach to Business Continuity Management

Resilient businesses are able to recover effectively from disruption. When the business is also agile it can recover quickly. But what if the business actually harnesses the uncertainty created by the disruption and grows stronger as a result? This is the defining characteristic of the 'antifragile' business model.

THE EVOLUTION AND REVOLUTION OF BUSINESS AS USUAL

We live in a chaotic world, and the realm of business is no exception. Every organisation faces unexpected fluctuations in business conditions from time to time. These deviations from 'business as usual' are often outside an organisation's influence, and can emerge slowly and apparently (e.g. market trends), or strike at random with little warning (e.g. natural disasters or epidemics).

The fact is that businesses, by necessity, must adapt if they wish to survive; either by continual evolution to gradual change, or by immediate revolution when the unexpected occurs.

Succumbing to the hidden forces of entropy which bid constantly to derail business plans is plainly not an attractive option. So business leaders turn to the practices of Business Continuity Management (BCM) to offer a route map towards building resilience to disruptions.

Resilience in this context means that business risks are eliminated or mitigated to a low level; that there is a built-in tolerance to disruptions, and that the business is able to recover. But there is an important facet of resilience in BCM which is often overlooked – agility.

AGILITY: A KEY INGREDIENT IN THE RECIPE FOR SURVIVAL

By agility we mean that the business is quick to mobilise and respond, and flexible enough to adapt, and does this decisively with high conviction. The ability to rapidly understand and react to an evolving scenario sets up a business to minimise both the magnitude and the duration of the disruption. Moreover, a truly agile response can enable a business to extract value out of the disarray.

Inspiration can be drawn from General Sun Tzu's 5th century BC treatise on military strategy and tactics "The Art of War" (Ref. 1), in which he submits that "in the midst of chaos, there is also opportunity". Whilst the modern commercial environment may at first seem worlds apart from ancient Chinese warfare, BCM leaders today can still take motivation from Sun Tzu's fundamental messages on tactical operations and management strategy.

Take the COVID-19 pandemic for example. It has forced companies to adapt to change and redesign their products or services – or even create new ones – to respond to the developing demands of millions of people around the world. While some businesses shut down or suspended their activities, others forged opportunities from the pandemic through transformation and innovation – the 'pandemic pivot'.

When dark clouds form, search for the silver linings

Restaurants moved towards take-out, delivery and catering rather than an eat-in service. Textile and apparel manufacturers switched to producing face masks. Fast-moving consumer goods companies transferred focus from products where demand had fallen (like skincare) towards surface cleaners and personal hygiene products. Breweries even repurposed distilling equipment to produce hand sanitiser.

These are all examples of businesses which, despite the disruptions and impending hardship, have been agile enough to pivot in new directions conducive to survival.

BEYOND RESILIENCE AND AGILITY

Nassim Nicholas Taleb coined the term 'antifragile' as an alternative to resilience (Ref. 2). He argues that if fragility is the quality of being damaged by stressors, then resilience

cannot be the opposite of fragility. Resilience is more geared towards a neutral outcome, whereas to be truly antifragile the result must be a positive one. Although resilient businesses have an ability to resist shocks and remain unchanged, antifragile businesses are able to leverage an unpredictable environment and actually grow stronger from the knocks they receive (see Figure 1).

Antifragility is a nice notion, but how can it be translated into practice through BCM? In short, antifragility must be implemented throughout the business via a BCM approach which includes:

- Strategies that recognise potential **upside** as well as downside
- Risk and impact analyses that identify and categorise **opportunities** arising from disruptions
- Implementation of business continuity measures geared towards **agility**
- Business continuity plans which ramp up quickly from 'survive mode' to **'thrive mode'**
- Embedding a business continuity culture which accelerates decision making and innovates at **pace**

Simply having a business continuity plan which promotes antifragile responses is not sufficient. The value of business continuity planning lies not in the plan itself, but in the organisational capabilities developed through the planning process. Only when an antifragile approach is baked into the BCM process, can it create a collective mindset which is embedded throughout the organisation.

An antifragile business culture decentralises control and empowers individual business units and employees with the autonomy to embrace risk, innovate, and – crucially – to make mistakes and learn from them. An antifragile approach actually requires failures in the short term in order for it to succeed in the long term (see Figure 2). As long as failures are on a manageable scale, acting on feedback is what enables the business to learn lessons, fortifying it for the future.

TO THE VICTOR BELONG THE SPOILS

Antifragile businesses will be the first movers into new arenas, and will gain a competitive advantage by being the first to market. Being first enables the business to establish strong brand recognition and customer loyalty before competitors enter the fray, some of which may whither and fold in an analogous way to natural selection.

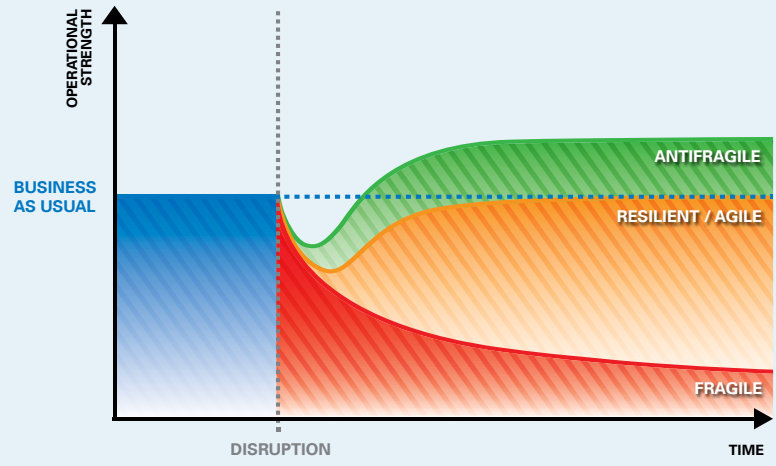


Figure 2 – Antifragile businesses benefit from disruptions

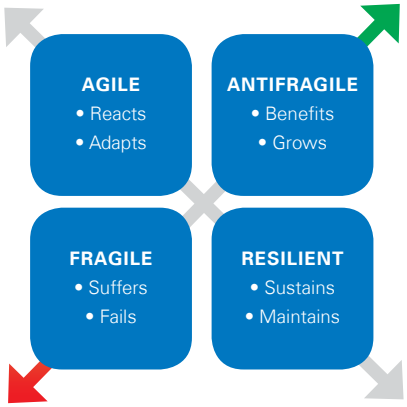


Figure 1 – Beyond resilience and agility, towards antifragility

Consider, also, that disruptions naturally trigger customers to seek alternatives for currently unavailable products and services. If the alternatives prove more convenient, the customers may never return. So the antifragile approach yields twin benefits – securing the existing customer base through innovation, as well as capturing market share from competitors.

CONTINUOUS RECALIBRATION

All adaptations or transformations of a business's operating model come with changes to that business's risk landscape. BCM – and enterprise risk management in general – therefore needs to evolve in step with the business to ensure that emerging risks are identified and managed. This makes the continuous review and improvement step of the BCM system all the more important for agile businesses.

CONCLUSION

Change is inevitable, and business leaders can't afford to treat BCM as an afterthought. A reliance on organisational resilience may suffice for short-term interruptions, but to thrive following major disruptions requires an antifragile mindset which is most effectively implemented through BCM.

References: 1. The Art of War, Sun Tzu, circa -500 BC
2. Antifragile: Things That Gain from Disorder, Nassim Nicholas Taleb, 2012

Contact: Matt Baggaley
matt.baggaley@risktec.tuv.com

Cyber Essentials – A holistic approach to reducing the risk of cyber-attacks

It may be surprising to learn that a well-designed computer system that is not connected to the internet can still be compromised by a cyber-attack. For example, 'sleeper' malware implanted during the design of a digital system can manifest itself many years later. The damage caused by such cyber-attacks can be significant and has been well documented following high profile incidents in recent years. As cyber-attacks become more sophisticated and continue to evolve, how can we best reduce the risk and assure ongoing cyber security?

WHAT IS CYBER SECURITY?

Cyber security is a collective term used to describe the measures put in place to reduce the risk associated with cyber-attacks. It has been around for about half a century since the advent of computers and the invention of the internet. Initially focused on the protection of Information Technology (IT), cyber security has evolved to embrace Operational Technology (OT) as digitalised industrial automation and control systems have become prevalent.

Over the years considerable effort has been expended in managing the cyber threat via design measures, such as air gaps and fire walls, but with the ever changing landscape of cyber-threats, which are evidently able to infiltrate IT and OT, it is essential to widen the focus if we are to effectively manage the risk.

The holistic approach incorporates the three complementary cyber security risk reduction enablers illustrated in Figure 1, namely design, management systems and culture, applied throughout the IT or OT lifecycle; and integrates with physical aspects of security.

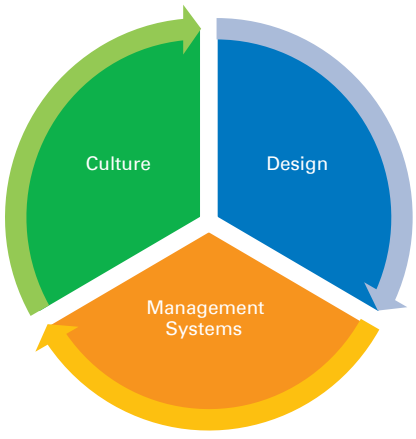


Figure 1 – Cyber security risk reduction enablers

SECURE BY DESIGN

Design is potentially the most effective of the three enablers. It is best considered alongside a cyber security hierarchy of controls (see Figure 2) to help prioritise possible cyber security measures.

The preferred option during design is to eliminate the potential for a cyber-attack (e.g. design analogue or passive OT systems) or eliminate paths for cyber-attacks (e.g. system not connected to the internet or other IT systems). Next, consideration should be given to reducing cyber-attack paths in the design of the system (e.g. reduced number of logical entry points).

Design robustness is crucial. It includes the design of a defensive system architecture as well as software programming measures to ensure system confidentiality, integrity and availability. A Cyber

Security Risk Assessment (CSRA) of the system design against a broad range of threat actors and sources, including blended cyber and physical attacks, will identify the need for any additional requirements.

These may lead to active systems (e.g. system monitoring) and/or control measures (e.g. procedural security measures or applying the principle of least privilege) and/ or physical security measures (e.g. hardened cabinet for digital equipment or physical port blockers for connection points).

MANAGEMENT SYSTEMS

Effective cyber security requires cyber security processes and procedures to complement the design measures. These need to be in place and followed not only during the use of the OT/ IT system but throughout its entire lifecycle, from initial concept, design and manufacture, right through to operation, upgrade and eventual removal.

Furthermore, the procedures should be embedded not just within the organisation operating the system but also its associated supply chain. During the system design or build, for example, a latent cyber threat introduced into the system by a supplier may remain undetected and can be exploited years later as the basis for a cyber-attack during operations. During maintenance or upgrade, portable devices used to upgrade software can provide a convenient path for a cyber-attack on systems that have been air-gapped from the internet.

The management system specifies when the CSRA should be carried out. Typically, this would be periodically at set intervals but should also be considered in response to known developments in the cyber threat, any internal or external cyber security incidents, or system upgrades and modifications.

Informed by the CSRA, a broad range of cyber security processes and procedures will be required. These will cover the use of the digital OT system, the use of the IT platforms on which the design, maintenance or upgrade of the digital system is carried out, as well as personnel vetting and aftercare, and regular testing of the system. Particular attention needs to be given during the development of these processes to address the insider intent on causing harm, either directly via a cyber-attack or via a combined cyber and physical attack.

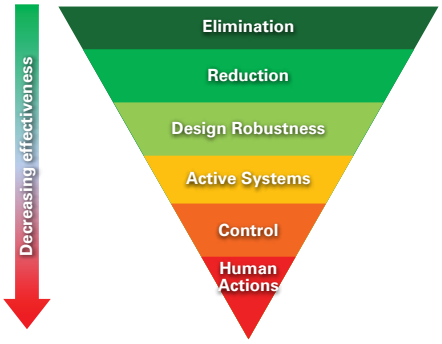


Figure 2 – Cyber security hierarchy of risk controls

CULTURE

The effectiveness of a robust system design and management system in reducing the risk of cyber-attacks can be compromised by the actions of people interfacing with the system, whether intentional or not. This could include inadvertently opening up a phishing email or connecting an infected USB stick to an IT or OT system, or simply not adhering to logical access control procedures.

A proactive security culture will drive the desired behaviours within the operating organisation and associated supply chain. Effective security requires motivating people to comply with well-defined procedures. Crucial to success here is the visible commitment of leaders to security, as well as providing cyber security awareness and refresher training for all personnel. Developing a mature security culture does not happen overnight; it takes time and continuous effort, but is as important as the other elements of the holistic approach.

INTEGRATION WITH PHYSICAL SECURITY

Overall security against the many potential cyber threats will depend to differing degrees on both cyber security and physical security. For instance, a knowledgeable insider (e.g. a disgruntled, radicalised or coerced employee), can present a specific challenge to cyber security which may only be effectively countered by non-cyber security measures. These could include physical security measures (e.g. hardened buildings or rooms, and access control), procedural measures (e.g. two-person rule), or may involve the deployment of the site security force.

More generally, understanding the defence in depth offered jointly by cyber security and physical security against specific threats and the trade-offs available can help optimise the overall solution.

CONCLUSION

Cyber-attacks on digital systems have the potential to cause significant loss. Rapidly changing and sophisticated cyber-attacks present an increasing challenge against which robust cyber security design and testing of digital systems is no longer sufficient.

A holistic approach which considers the three risk reduction enablers of design, management systems and culture throughout the different stages of the system lifecycle, in a way that also integrates physical security, is required to effectively reduce the risk of today's evolving cyber-threats.

Contact: John Llambias
john.llambias@risktec.tuv.com

Simplifying Complexity – The challenges of fire and gas detection

Fire and gas detection enables the early detection of loss of containment incidents, which then demands automated or manual actions capable of significantly reducing the magnitude of consequences. For a long time, however, the performance of associated systems has been poor, with incident databases revealing that 36% of major and 69% of significant gas releases go undetected (Ref. 1). So what can be done to improve this situation?

THE PROBLEM

Ideally, a fire and gas detection system would detect all potential releases as soon as they occur. The reality, however, is that the diversity of release outcomes does not make this practicable. The range of influencing factors that affect hazard behaviour, such as release direction, wind speed, wind direction and ignition sources leads to a seemingly unlimited number of scenarios against which to design our detection system.

The problem is not limited to just choosing the most reliable equipment, we must also choose an appropriate layout. We could spend much effort procuring the most reliable equipment, but such efforts will be wasted if we do not support the design with an appropriate number and layout of detectors. Since the availability of the fire and gas system is dependent on both the equipment and the detector layout, traditional approaches to availability assessment, which do not consider the location (or coverage), are not sufficient for demonstrating fire and gas detection performance.

OTHER CHALLENGES

These issues are aggravated by the wealth of fire and gas detection equipment available on the market, each with their own supporting guidance, data sheets and manuals. Rather than helping, the range of options and information can serve to hinder the designer.

Not only do we have a large range of release scenarios to design against, we also have to consider detectors (and their varying capabilities) from competing vendors. All this comes together to form a potentially complex, multivariate design and analysis problem.

SIMPLIFYING COMPLEXITY

Like all other safety related systems, the requirements of the fire and gas detection system should be defined with an understanding of the hazards for each area of a facility. The hazards and associated risks then drive the specific performance requirements for the detection system (as well as the mitigative actions to be taken).

For fire and gas detection, it is actually helpful if we accept the assertion that not all potential release outcomes will be detected and instead, tailor our design solutions towards the most dominant risk contributors.

For example, in a highly congested volume the dominant hazard may be explosion (and subsequent escalation). In this case we need to provide a sufficient density of detectors to detect a flammable gas cloud before it could result in a damaging explosion. The detector layout for explosions will also likely be required to trigger automatic shutdown, placing further demand on our system to ensure there is a reliable signal for shutdown (e.g. by using a voting logic from multiple detectors).

For an open facility the main hazard may be migration of a gas to a public area, Here, perimeter monitoring achieved by line of sight detection may be more beneficial.

These two simple examples show us how understanding the risks and vulnerabilities of our facility provides valuable input to the fire and gas detection design philosophy, in particular the technology of choice and layout strategy.

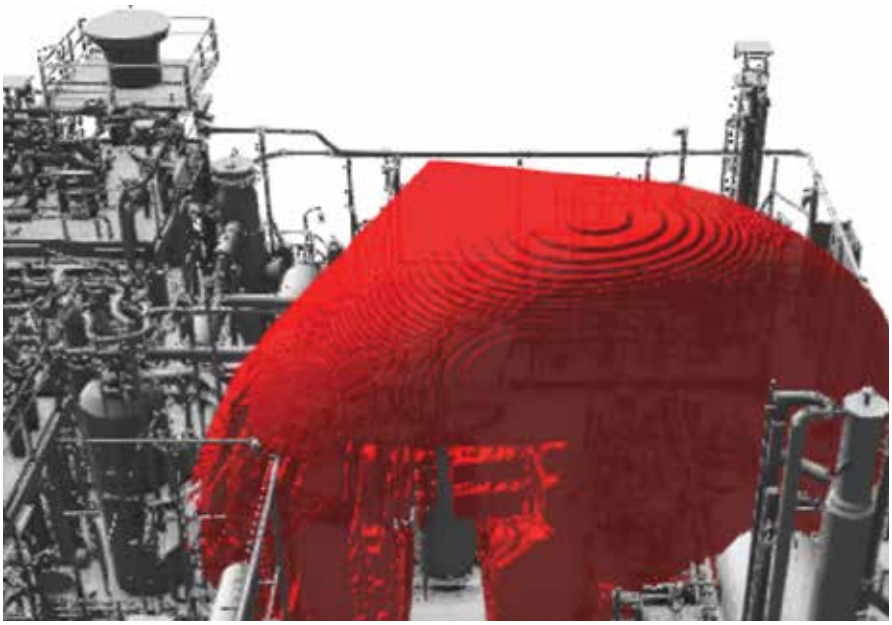
GUIDANCE

When we consider the range of facility types (e.g. offshore and onshore), and hazardous outcomes (e.g. toxic dispersion, jet fire, explosion) the benefits of a publicly available and versatile standard methodology are clear.

To fill this void, the UK's Energy Institute is in the process of producing guidance which provides a recommended approach to developing fire and gas detection philosophies. It is intended to be flexible, and equally relevant to small and large facilities, in both the onshore and offshore industries. The guidance promotes the requirement to assess hazards and risks by practicable means, utilising existing or planned studies (e.g. fire and explosion risk assessment and quantitative risk assessment) where possible. From this we can design our system against the dominant risks, and select an appropriate layout strategy and technology that can fulfil the performance requirements.

FIRE AND GAS MAPPING

So where does fire and gas mapping sit in all this? Fire and gas mapping has gained much traction in recent years, and provides a means to measure the coverage performance of our detector arrangement. It no doubt provides confidence and consistency (both within a facility and across industry) in proposed fire and gas detector layouts. The latest



methods allow detailed assessment of thousands of release cases and automate the analysis of resultant data to 'optimise' our detector layout.

It is important, however, not to get too engrossed in mapping analysis and assume that with more analysis, comes greater risk reduction. No matter how sophisticated the approach to mapping, ultimately it should be treated as a verification exercise and applied only if appropriate for the detection strategy. For example, perimeter detection or dedicated spot detection are not ideal strategies for verification by fire and gas mapping.

Greater risk reduction benefits are likely to be realised if we apply equivalent effort in choosing the right technology and layout in the first place. For example, in some situations, it might be better to adopt acoustic detection technology, or consider infra-red gas cameras. These technologies are becoming more reliable and more cost-effective; and we should understand the benefits these could bring to detection performance, rather than defaulting to the standard type of detectors and assuming that mapping will bring the optimum solution.

CONCLUSION

Designing a fire and gas detection system is a significant challenge – the range of scenarios, detector positions, technologies and minimal industry guidance leave the whole process ill-defined, leading to poor potential detection performance in practice.

First and foremost our design should be informed by risk assessment, from which we can define the specific detection requirements, choose appropriate technology and select the best layout strategy. Performing these activities initially will yield the greatest risk reduction benefits and only once these are completed are we in a position to decide whether mapping is needed. Crucially, this pragmatic approach will be reflected in the forthcoming Energy Institute guidance on fire and gas detection design.

Contact: Jon Wiseman
jon.wiseman@risktec.tuv.com

References: 1. RR1123, Fixed flammable gas detector systems on offshore installations: optimisation and assessment of effectiveness, HSE, 2017.

Breaking it Down – A brief guide to creating effective operating procedures

Ensuring that all operating and maintenance procedures are easy to follow, accurate and up to date can be a challenge, but it is essential for accomplishing safety critical tasks and meeting corporate and regulatory expectations. To meet this challenge, human factors best practice can be boiled down to help improve the usability of procedures, resulting in fewer human errors and violations, and greater compliance.

COMMON PROBLEMS WITH PROCEDURES

Although operating and maintenance procedures may be developed by operators with extensive experience, the way in which procedures are written may not always make them easy to follow without error, particularly in the case of new operators. A common failing is that as things change (e.g. new equipment is introduced, roles and responsibilities are re-assigned, etc.), the procedure isn't updated. In contrast, sometimes procedures may be modified piece-meal over time by various individuals until they no longer accurately reflect the tasks in question. Other commonly observed issues include:

- Procedural steps are written as lengthy paragraphs, containing a mixture of instruction and information
- Safety critical tasks are not clearly identified
- The operator responsible for carrying out each step is not clear
- Poor document control

Poorly written procedures increase the potential for operators to make errors. Even worse, if a procedure is out of date and cannot be correctly followed then shortcuts may be taken.

ESTABLISHING AN EFFECTIVE PROCESS

It is important that there is a robust corporate procedure that lays out the process to be followed for the development and ongoing control of operating procedures and work instructions.

Key considerations include:

- Assigning responsibilities for procedure development and management
- Establishing a robust process for determining whether the procedure is safety critical or not
- Setting and enforcing requirements for procedure checking, approval and periodic review

DESIGNING FOR USABILITY

When deciding procedure structure and content, established human factors guidance on usability should be applied. Taking account of best practice will reduce the potential for human errors and procedural violations and encourage compliant use. Some examples of key points are:

- State the criticality level of the activities covered by the procedure, and summarise any key risks at the front of the document
- List any equipment or Personal Protective Equipment (PPE) that is required
- Limit each step to a single operator action
- Use short, simple sentences, in the present tense
- Number all steps and make appropriate use of check boxes to help operators keep track of their place in the task sequence

- Clearly differentiate between task instructions, warnings, cautions and additional information
- Consider additional sign-offs for safety critical tasks

Once a procedure has been drafted, it is important to pilot it with operators who will be using it. Indeed, a key requirement for the production of effective procedures is to ensure the involvement of all end-users throughout the process.

THE BENEFITS OF HIERARCHICAL TASK ANALYSIS

Another crucial requirement is that the procedure's steps must accurately reflect the task as performed in practice.

Hierarchical Task Analysis (HTA) is a proven method for capturing and describing a task or activity down to a detailed level. Typically, HTA is based on task observation or a talk-through with the operator, and involves systematically identifying and sequencing task steps to enable the accurate update of an existing procedure or development of a new one.

Software may be used by non-specialists to support this, enabling complex activities to be broken down into their constituent steps (see Figure 1). Safety critical steps can be identified and warnings or cautions assigned. Task steps can then be transposed electronically into procedure format (Figure 2). Once agreed, the new or revised procedure provides the ideal starting point for Safety Critical Task Analysis (SCTA) or Human Error Assessment (HEA).

Method Statement

Procedure: Make a cup of tea

Background: Follow these steps to make a perfect cup of tea safely.

⚠ **CAUTION HOLD POINT:**
Time for a pause and check.
(Examples: Verify adequate storage for scrap material; or stop to allow scaffold access to be adjusted).

⚠ **WARNING CRITICAL STEP:**
Failure to adhere to instruction could result in catastrophic failure, a major accident, serious injury or death.

Step		Instruction	Signature
1		Boil water	
1.1		Fill kettle with water	
1.2		Put kettle on stove	
1.3		Turn gas and light stove	
1.4		Wait for kettle to boil	
1.5	⚠	**CAUTION HOLD POINT** Turn off gas	
2		Empty teapot Information: Make sure the teapot is empty before continuing	
3		Put tea leaves in pot Information: One teaspoon of leaves per person	
4	⚠	**WARNING CRITICAL STEP:** Take care, the water will be hot Pour in boiling water	
5		Wait 4 or 5 minutes	
6	⚠	**WARNING CRITICAL STEP:** Take care, the tea will be hot Pour tea into cups	

Figure 2 – Example operating procedure format

Using such a tool has a number of benefits, including:

- Helping operators gain a clear understanding of task steps and sequencing, encouraging 'buy in' to the development process
- Facilitating the involvement of operators in developing accurate, user-friendly procedures, quickly and efficiently, providing the starting point from which further refinement can take place
- Standardising the procedure development process, structure and format
- Enabling details of tasks, sequencing and supporting information to be easily modified

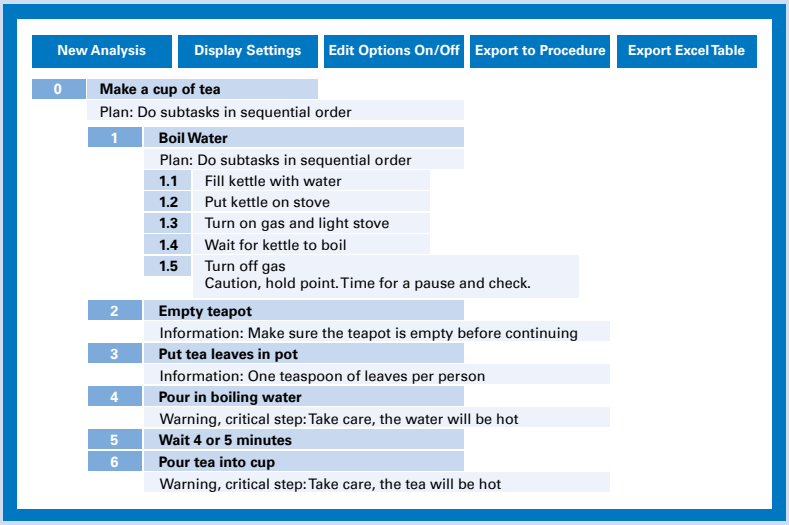


Figure 1 – Example Hierarchical Task Analysis

CONCLUSION

Ensuring that procedures are easy to follow, accurate and up to date is essential for safe working and more generally minimising the potential for error or non-compliance.

Applying human factors knowledge, including the use of HTA and associated tools, can help ensure that procedures are optimised and effective, and that corporate and regulatory expectations are met.

Contact: Derek Porter
derek.porter@risktec.tuv.com

Workshops – More than the sum of their parts?

Everyone who works in risk management and safety engineering knows that facilitated workshops are an essential part of our toolkit. They bring together diverse and often disparate technical disciplines, skillsets and perspectives, and are capable of identifying and solving problems beyond the ability of any single individual.

THE WORKSHOP IDEAL VERSUS REALITY

A multi-disciplinary workshop, uniting engineering with operations and management provides confidence in the output of the risk management process. Facilitators look for a quorate team of participants, whose knowledge and experience can encapsulate the full context of the risk or safety issue being considered. At least, that's the theory or the ideal and generally it's mostly true in practice.

Notwithstanding the best of intentions, there will always be hurdles to overcome that prevent workshops from running as smoothly as we would like. There are nearly always the attendees who sit quietly, seemingly contributing nothing but a page or two of beautifully crafted doodles. Sometimes there are strong characters who want to run the meeting without actually running the meeting, or who want to close down discussions that go beyond some arbitrary time limit. Often, despite all preparation and testing, the IT fails or glitches or assumes a mind of its own. Workshops can be frustrating, stressful, expensive and sometimes painstaking for many of the people involved; so why bother?

COMPLEXITY, ANXIETY AND EXPEDIENCY

Part of the answer to that question is that there is little practical alternative. Modern engineering projects can be so complex it is arguably impossible (and certainly inadvisable) for one individual, no matter how talented, to undertake

risk identification or optioneering (for example) in isolation. We need input and understanding that only comes from the relevant engineers, operators and maintainers. Similarly, engineers and operators need safety and risk management specialists – professionals in their own right – who simultaneously possess the perversity of mindset to continually question what can go wrong, as well as keeping the big picture in mind when deciding whether it matters. Formats can range from short half-day, free-form brainstorming sessions to highly structured multi-week workshops. Each has its own characteristics and requires very different facilitating and recording skills.

One of the beauties of the structured, systematic, guideword-driven approach led by an independent professional facilitator is that it resolves many of the internal challenges organisations face, such as office politics and the imposition of individual, preferential views rather than an evidence-based consensus.

We provide a technical antidote to the nagging anxiety that the operations or engineering manager feels when they think they might have missed something or could do more. We'll never be able to fully mitigate the chronic unease, but as well as a workshop we can often facilitate the occasional decent night's sleep.

There's also definitely something to be said for the lifecycle 'set-piece' that a workshop provides. Get in, manage risk, and get out again; thanks for the free lunch. While the person-hours can add up, from the perspective of calendar days there can't be any doubting the expediency to the project schedule. The alternative is a correspondence-based, iterative approach, which relies on the goodwill and availability of correspondents, who all have a day-job. Not surprisingly, few are tempted down this route, which risks incompleteness and delays.

THE EXTRAS

It turns out that safety professionals and risk management experts are often engineers, scientists, human factors experts, or former operators or managers. Although we're not practicing designers, operators, maintainers or research scientists, at heart we're a little bit of all of those things. The more experienced we get, the more languages we learn to speak. We stand at the front of the room knowing something about each of the participant's field of interest and expertise. Most of us will never be experts in geomechanics, nor will we be oil well engineers, but we can learn enough to discuss the issues and solutions with experts and synthesise a risk analysis for geological carbon storage, for instance.

Then there's the roomful of discipline engineers and operators embedded in the detail and the managers holding the project together (and the purse strings) with no time for the detail but plenty of accountability for making sure it's right. In this scenario, the workshop facilitator is the integrator that helps make sense of the detail, challenges it, and catalyses a balanced and positive transformation into something cohesive that moves things forward.

Busy, large engineering projects seldom afford many occasions for project teams to assemble. A workshop can do just that, allowing people from different parts of the world to meet over coffee and snacks during the breaks, forging new relationships. Project discussions unrelated to the ostensible goals of the workshop can suddenly take shape and come to life when taken out of the day-job context, creating innovative solutions to problems no-one had even thought about. Facilitating a workshop can be just as much about facilitating the development of a team as obtaining the primary output.

Remember our doodler? He might well be a graduate or new to the project, learning by osmosis about the engineering or the process itself, as are all of the participants to greater or lesser extent. Workshops always include implicit training – learning and understanding more about the project, the issues faced by each discipline and the associated technicalities – they have to if you want to achieve the end result.

REMOTE WORKING

In our post-Covid-19 era, remote workshops are increasingly the norm and their effectiveness is proven, at least in terms of meeting their immediate aims. Concerning the fringe benefits, the jury's out but there's certainly promise being shown. As we become more used to life in the virtual meeting, the people we meet begin to feel almost as close as face to face and the benefits appear to remain largely unthreatened… even if we do have to make our own coffee.

CONCLUSION

Workshops *are* more than the sum of their parts. Whilst intended as a vehicle to identify and solve specific, multi-disciplinary problems, they bring with them a host of extras, including innovation, team building and learning…and sometimes good coffee.

Contact: Matt Beeson
matt.beeson@risktec.tuv.com

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

MANAGING THE SAFETY RISK OF NUCLEAR DECOMMISSIONING

Assuring safe, cost-effective and timely decommissioning of legacy plants.

REMOTE INSPECTION – THE ARRIVAL OF THE VIRTUAL EXPERT

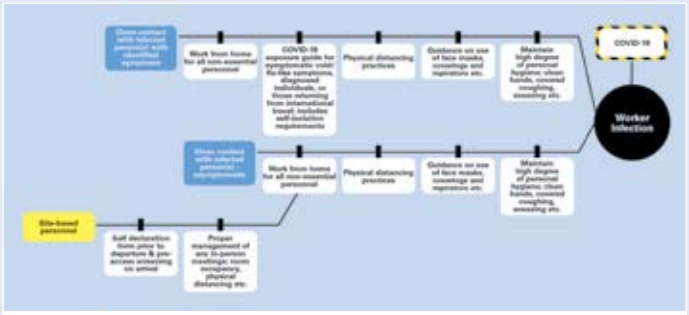
Quicker, easier and cheaper surveys and diagnoses.

CHALLENGING TIMES IN THE DISTILLERY SECTOR

Carefully improving production efficiency and process safety.

GOOD PRACTICE FOR SAFETY-RELATED VIRTUAL AUDITS

Tips for successful remote audits.



PANDEMIC MANAGEMENT USING BOWTIE ANALYSIS

Ensuring safe operations during the COVID-19 crisis.

SAFETY CRITICAL TASK ANALYSIS

A pragmatic approach to identifying human failures.

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
Derby
Edinburgh
Glasgow
London
Nottingham
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