Issue 42 / Autumn 2022

RISKworld

The Newsletter of Risktec Solutions

In this issue

Welcome to Issue 42 of RISKworld. Feel free to pass this edition on to other people in your organisation. You can also sign up here to make sure you don't miss future issues.

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

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

Contents

"It is not the strongest of the species that survives, not the most intelligent that survives. It is the one that is the most adaptable to change." – Charles Darwin

Thus far, 2022 has been a very encouraging year, which has seen a significant growth in business alongside the recruitment of many new people – all during a period of economic uncertainty and recovery from Covid.

We have seen increases in project activity across all the major hazard industries we support, most notably in the hydrogen, wind and carbon capture sectors.

2MC joined the Risktec Group to provide a range of Governance Risk and Compliance software and consulting services that complement the risk and safety services offered by Risktec.

Our Asset Integrity Management team continues to go from strength to strength. For example, we have now provided inspection or integrity management support to more than a third of all the UK CCGT power stations.

Now that many of the Covid restrictions have been reduced, there has been a welcome return to more face to face meetings and workshops when justified. Building relationships and working closely with our clients, whether in person or remotely, helps to fully understand their current challenges, which is crucial to us providing a valued service.

This year we have also opened a new Risktec office in Bristol that continues our approach of locating offices close to our clients to ensure we can support them locally.

Our client focus is measured by our bi-annual client satisfaction 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 our flexibility and responsiveness to client requirements was 98%, and for the third survey in a row 100% of respondents indicated they would recommend Risktec to others.

This is very much a period of transition, particularly in the energy industry, given the challenge of meeting sustainability objectives while remaining competitive. The articles in this issue provide an illustration of how many of the existing techniques and approaches used for managing risk can be adapted to help meet these and other challenges in cost-effective and insightful ways.

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

CyHAZOP – Bringing cyber to the HAZOP

Cyber-security is one of the fastest growing areas of concern for industrial automation and control systems, otherwise known as Operational Technology (OT). As associated 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.

The HAZOP has been a staple of the safety industry for decades, providing a familiar, repeatable and effective method to identify and assess hazards affecting the safe operation of process equipment.

The cyber-security industry for OT is still growing and learning; this means there is a lack of accepted risk identification and assessment processes, which in turn drives a lack of consistency. The cyber-security industry uses very different language to that of safety or to business, causing further confusion.

Being well known by system managers and engineers alike, the HAZOP methodology provides a perfect bridge for a comfortable and consistent transition to cyber risk assessment. Utilising the basic HAZOP process concept enables cyber-risk to be assessed in a way that is scalable, can be applied to different industries, and is compatible with a range of security standards and regulatory expectations.

WHAT IS DIFFERENT?

A traditional HAZOP utilises a series of guidewords and process parameters that are combined to create deviations – the 'No Flow', 'Less Flow', 'More Pressure', 'Less Pressure' descriptors that all HAZOP attendees will be familiar with.

The Cyber HAZOP (or CyHAZOP) methodology keeps the same basic approach, but with specific tailored guidewords, parameters and deviations designed to target cyber-security needs and enable direct linkage to cyber-security vulnerabilities and controls.

NOVEL NODES

A traditional HAZOP is divided into 'nodes', which generally relate to large sections of the process plant and/or where the process parameters remain the same.

In a CyHAZOP a different approach is taken. The first node is always a contextual view looking at the wider business, to allow the assessor to gain a holistic perspective, incorporating all the security domains shown in Figure 1.

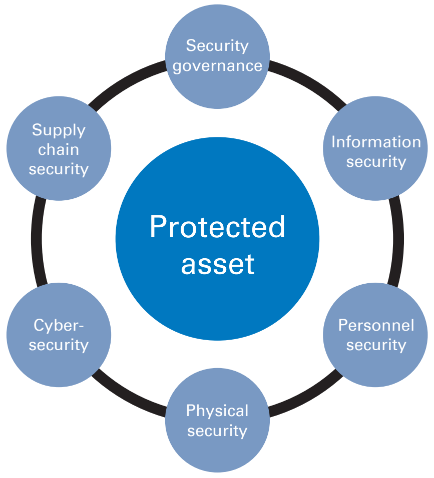


Figure 1 - The Security Domains

Subsequent nodes are based on Zones and Conduits – the definition of which for most purposes is taken from IEC 62443 (Ref 1), which defines:

- A Zone as a logical or physical grouping of assets within, or connecting to, the system in scope.
- A Conduit as a connection between Zones or between Sub-Zones, concentrating on the data that is exchanged between these Zones.

GUIDEWORDS OR CODEWORDS?

For CyHAZOP, not surprisingly, the guidewords and parameters are also specific to cyber-security; and like nodes, the correlation with conventional HAZOP terminology is somewhat alien.

Zone-based nodes use asset-related guidewords, such as 'Engineering Workstation', 'Control Server' and 'Networking Equipment' to direct the discussion around the types of computerised assets that exist within that Zone.

An accompanying attack-chain set of parameters might be:

- Initial access
- Persistence
- Modification
- Execution
- Recovery

These guidewords and parameters are then combined to give deviations such as 'Engineering Workstation - Initial Access', 'Networking Equipment - Modification', which form the basis of the structure for the CyHAZOP Zone assessment.

For Conduits a simple approach is used, the only guideword being 'Data', with a standard information security approach for the parameters:

- Confidentiality
- Integrity
- Availability

This gives the deviations 'Data - Confidentiality', 'Data - Integrity' and 'Data - Availability', which prompt the assessment of what happens if there is a lack of data confidentiality, integrity or availability in the Conduit.

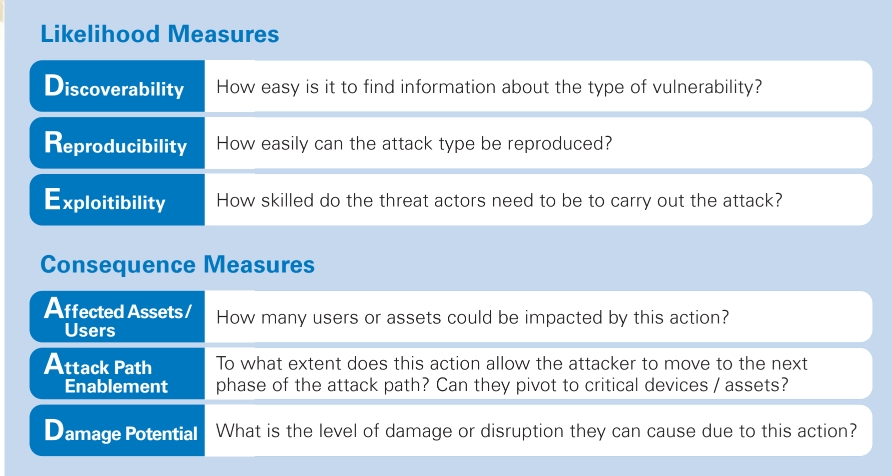
More generally, by stepping through each phase of an attack, the types of vulnerabilities, consequences and controls that are used to combat threat activity typical of these phases can be teased out.

LIKELIHOOD AND CONSEQUENCES ESTIMATION

Estimating 'Risk' is something that is not always considered within a HAZOP, but when it is, this normally involves the use of a Risk Assessment Matrix (RAM) to determine a likelihood-consequence pairing thus giving a risk level for the scenario under consideration.

Determining the likelihood associated with security risk can, however, be very difficult to quantify. To help solve this, a new technique based on an approach initially presented by Knapp and Langill in 2015 (Ref 2) is used. This employs the DREAD method originally developed by Microsoft (Ref 3) for their Security Development Lifecycle.

For the CyHAZOP, the DREAD model is modified by adding an additional criteria 'Attack Path Enablement', to create the DREAAD model (see Figure 2). This ensures that any security factor which enables the attack chain to continue can be captured and allows consideration of the consequences of an attacker achieving their aim in that phase of the attack.



Likelihood Measures

Discoverability	How easy is it to find information about the type of vulnerability?
Reproducibility	How easily can the attack type be reproduced?
Exploitibility	How skilled do the threat actors need to be to carry out the attack?

Consequence Measures

Affected Assets / Users	How many users or assets could be impacted by this action?
Attack Path Enablement	To what extent does this action allow the attacker to move to the next phase of the attack path? Can they pivot to critical devices / assets?
Damage Potential	What is the level of damage or disruption they can cause due to this action?

Figure 2 - The CyHAZOP DREAAD Model

VULNERABILITIES

Vulnerabilities are based around the IEC 62443 Foundational Requirement set, and are kept to a high level, to keep the CyHAZOP efficient and avoid turning it into a detailed vulnerability assessment for each asset. A CyHAZOP will identify areas where more detailed investigations around controls and vulnerabilities should be undertaken.

The CyHAZOP also looks at the consequences of these vulnerabilities being exploited. To do this CyHAZOP takes the MITRE ATT&CK for ICS framework 'impacts' (see Ref 4), linking them to the vulnerabilities.

MITRE ATT&CK for ICS is widely becoming the go to method for considering the tactics, techniques and procedures that threat actors can utilise within the OT space. Linking the impacts in this way allows organisations to embed their findings into various third-party process flows for intelligence feeds and vulnerability scans.

CONTROLS

As for a traditional HAZOP, controls are identified to demonstrate the preventative and mitigative measures in place. In CyHAZOP, these are linked to IEC 62443 Security Requirements, which forms the basis for the CyHAZOP control sets.

CONCLUSION

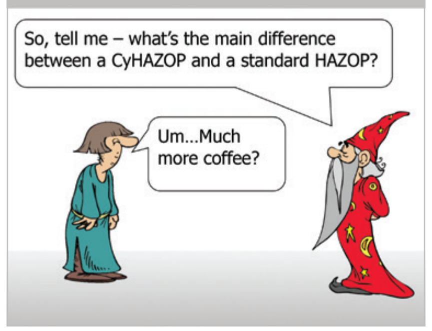
The CyHAZOP methodology is a natural development of the proven HAZOP process and, as such, it offers the same advantages: a systematic and structured technique that actively involves all stakeholders.

In practical applications, CyHAZOP has demonstrated its effectiveness in identifying areas of risk that an organisation is facing within its OT environment. Interestingly, however, one of the biggest benefits seen has been the learning experience that it offers to workshop members.

A Webinar is available on the Risktec YouTube Channel that looks at CyHAZOP in more depth: www.youtube.com/watch?v=2lYE5RUTmK8

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

Legends of Risktec No.42



References:
1. IEC 62443 suite. Industrial Electrotechnical Commission. 2007 - 2020
2. Industrial Cyber-security, Second Edition, Eric D. Knapp and Joel Thomas Langill. Syngress, 2015
3. Threat modelling for drivers - Windows drivers | Microsoft Learn https://learn.microsoft.com/en-us/windows-hardware/drivers/driversecurity/threat-modeling-for-drivers#the-dread-approach-to-threat-assessment
4. MITRE ATT&CK® for Industrial Control Systems: Design and Philosophy, Otis Alexander et al, 2020

Remote Control – Good practice for safety-related virtual audits

With companies grappling with how to achieve sustainability goals and reduce their overall carbon footprint, we look at how remote audits can be conducted effectively and the advantages this can bring.

DEFAULT SETTINGS

Following the changes to our working lives and the lessons learned from social distancing and travel restrictions during the coronavirus pandemic, it has become clear that many tasks can, with a bit of thought, be conducted effectively and efficiently in a virtual environment.

With an increasing focus and desire to achieve sustainability goals and reduce carbon footprints, remote audits can play a part in reducing the need for unnecessary travel, while still delivering an accurate and complete outcome.

So, how can a remote audit be conducted effectively? In order to answer this question, it is worth reflecting on the factors that have made face-to-face audits the default option, despite the presence of ever-improving digital communication tools.

MISSING PIECES?

A major benefit of undertaking audits on-site is that it allows the auditor to see instances of behaviours – both good and bad – and to witness the way people interact with each other and perform their work. In this respect, the on-site observations made by auditors play an important part. When considering a remote audit, the absence of this first-hand interaction is one of the main challenges that must be managed, with the auditor relying on testimonial evidence from the auditees instead of their own, direct experiences. This is where experienced auditors, particularly those who have worked at similar facilities, will add significant value to the remote audit process – building mutual trust with the site team to work towards a common goal.

VIRTUAL REALITY

Irrespective of the subject matter, an audit typically involves:

- Gathering facts and reviewing relevant information; and
- Verifying that the design and effectiveness of a system, programme or procedure is compliant with set standards and expectations.

Usually, these tasks can be achieved through a three-pronged approach – review, verification and interview – and remote audits are no different.

The key to a successful remote audit is preparation, meaning that greater emphasis should be placed on gathering and reviewing information as part of the pre-audit activities, prior to proceeding to interviews with personnel. Pre-audit activities include reviewing relevant procedures, examples of work undertaken, previous non-conformities and corrective actions taken for previously identified deficiencies.

Whilst all these issues can be managed remotely, care must be taken to ensure that adequate, relevant information is shared with the auditors in a timely manner. This will require greater co-operation from the auditee, as they cannot simply point the auditor to a filing cabinet or grant them access to a secure network drive.

IN PRACTICE

If a significant amount of detail needs to be covered during videoconferences, ensure that regular breaks are taken and don't be afraid to split the session over multiple days, to avoid losing people's focus. The auditor may find it useful to have an assistant to take notes and record actions as they arise. These actions should be diligently communicated and tracked to completion.

Conducting site inspections remotely is more challenging, but can be achieved through a variety of means, such as live online broadcasts or pre-recorded videos, if the risks to the personnel recording the video can be safely managed.

The final step in the remote audit process is to interview relevant personnel from all levels of the organisation via videoconference, again to verify that systems are in place and are being adhered to. These calls allow the auditors to gather information about understanding, compliance and training related to the area being audited.

If necessary, a physical follow-up can be recommended. This judgement should be made using the results of the audit and the main risks associated with the topic, e.g. focusing on specific safety-critical items or processes.

Following the completion of an audit, a review of the remote auditing process is recommended, in order to identify any shortcomings and opportunities for improvement.

IS IT WORTH IT?

Remote audits are a practical solution without the time, cost and carbon emissions associated with travel. A carefully considered approach, taking account of the particular circumstances of the auditee, will ensure that there is no impact on the quality of the outcomes for the majority of the process. Where aspects of the audit may be compromised, for example due to the absence of an on-site inspection, don't be afraid to recommend a site visit at a later date to verify the situation first-hand.

Advantages include:

- Uninterrupted surveillance programmes to meet compliance requirements.
- Continued identification of potential safety issues.
- Access to a broader range of expertise on both sides of the table, as geographical and time-based restrictions are more flexible.
- Reduced travel time, emissions and expenses.
- Flexibility of approach, which can be tailored to different companies, technologies and subject matters.

If there is a reluctance to conduct a remote audit, it is worth considering that even if the full effectiveness of a physical audit is not achieved, it will be considerably more effective than doing nothing. Tips for successfully conducting virtual audits are shown in Table 1.

CONCLUSION

The disruption to normal working practices caused by the coronavirus pandemic prompted auditors to innovate and learn how to successfully complete audits remotely.

With careful planning, these lessons learned can be used to help us to reduce carbon emissions and achieve our sustainability goals, while still meeting audit objectives without compromising on quality and accuracy.

Contact: Chris Taylor
chris.taylor@risktec.tuv.com

PREPARATION

- If necessary, hold a pre-meeting to define important preparatory information
- Make as much supporting information as possible available electronically, well in advance (applies to both the auditor and the auditee)
- Plan for the audit to take 25% longer than a face-to-face approach, but you might not need the extra time
- Assign an assistant to support the auditor during the remote session – ideally they will have worked well together previously
- For group sessions, limit attendees to the essential minimum, making clear in the invitation who is required and who is optional
- Test the host platform with the auditee before you start, but accept that there may be interruptions in service, and plan accordingly

AUDITOR

- Undertake introductions methodically and slowly, to allow everyone to capture participants' names and roles
- Keep sessions short (up to one hour with four to six in a day), so that participants remain focused
- Control the session – the subject matter, who's talking, who talks next, what actions are needed, etc.
- Park issues (with an action) that rely on additional information or consideration rather than getting bogged down
- Don't be concerned about awkward silences, but be wary of connectivity issues
- Be careful not to rush through the discussion, to enable space to think and for contributions from others
- Be alert to participants wishing to speak (e.g. by monitoring microphone status or chat room dialogue)
- In the subsequent report, remember to describe the process followed

ETIQUETTE

- Check each caller can hear the auditor (and vice versa) as they enter the call
- To limit background noise, ask everyone to mute their microphone unless they are speaking
- Unless connectivity is poor, request that participants enable video to build up a rapport and enable the auditor to pick up on body language and other visual cues
- Ask everyone to identify themselves before they speak, speak clearly and not over one another
- Ask participants to request screen sharing if they wish to highlight specific issues on documentation to the whole group
- If applicable, notify everyone that you will be recording the meeting
- Schedule breaks in advance so that people don't lose focus

ASSISTANT

- Control the videoconference and screen sharing and record the session
- As an aide memoire, take a screen shot of the list of participants at each session as displayed by the communication platform
- If you miss or cannot understand something, speak up at a suitable break or message the auditor
- If people talk too fast or indistinctly, remind everyone to speak clearly and more slowly
- Take written notes if this is faster and after each day issue draft minutes to all participants
- Review all actions in a separate session with the auditor to ensure they are sufficiently accurate, specific and allocated to the right person
- Circulate actions promptly

AUDITEE

- If necessary, hold a pre-meeting to define important preparatory information
- Make as much supporting information as possible available electronically, well in advance
- Ensure appropriate personnel are invited to and attend the scheduled videoconference sessions
- For group sessions, limit attendees to the essential minimum, making clear in the invitation who is required and who is optional
- Be responsive to the auditor's requests and complete actions promptly, to keep the process moving
- Plan for the audit to take 25% longer than a face-to-face approach, but you might not need the extra time

Table 1 – Tips for successful remote audits

Error Trapping – An introduction to human reliability assessment

Quantitative Human Reliability Assessment (HRA) can improve the safety and reliability of systems that depend on human action. It can also reduce potentially costly redesign of systems and equipment if the opportunities for human error are identified, analysed and designed out or minimised. So what is HRA, where did it come from and what are the main steps for carrying out such an assessment?

WHAT IS HUMAN RELIABILITY ASSESSMENT?

HRA involves the use of qualitative and quantitative methods to assess the human contribution to risk. There are many and varied methods available for HRA, with those first developed focused on predicting and quantifying the likelihood of human error.

The output from these methods is a Human Error Probability (HEP) of the human performance of a task or element of a task (Ref. 1). Some of the tools follow a strict methodology and step-by-step process in order to generate the HEP, while others rely solely on expert judgement.

All methods require knowledge of Human Factors and the ability to make expert judgements in relation to human error likelihood.

WHY DO HUMAN RELIABILITY ASSESSMENT?

As practitioners of these methods will know, HRA is not an exact science. However, it is a useful means of identifying and prioritising plant safety vulnerabilities to human error, and thereby reducing the frequency of associated accidents.

The assessment also identifies and informs system and equipment design features that could be implemented to minimise the likelihood of a human error actually occurring. If such opportunities for human error reduction are considered at an early design stage, the scope for potentially costly redesign can be minimised.

ORIGINS OF HUMAN RELIABILITY ASSESSMENT

Research into HRA started in the 1960s and accelerated following the Three Mile Island accident in 1979 when it became clear that human error was one of the main contributing factors (Ref. 2) that led to the partial meltdown of the reactor core.

Since then, other major accidents including the NASA Challenger disaster and Chernobyl (both in 1986) continue to highlight that human error can be a fundamental contributor to major accidents.

WHAT ARE HUMAN ERROR PROBABILITIES?

HRA techniques all quantify the Human Error Probability (HEP), which is the metric of HRA. The HEP is defined as:

$$\text{HEP} = \frac{\textbf{Number of errors occcured}}{\textbf{Number of opportunities for error to occur}}$$

There is very little HEP data available from studies and accident analysis, most likely due to the perceived sensitivity of publishing data which may imply poor performance, coupled with a lack of appreciation of why it would be useful to collect such data in the first place (Ref. 2). This is why so many of the common HRA methods rely, to a greater or lesser extent, on expert judgement.

HUMAN RELIABILITY ASSESSMENT METHODS

In 2009, the UK Health and Safety Executive (HSE) conducted a review of all known HRA methods (Ref. 3). Of the 35 human reliability tools considered, 17 were deemed to be of potential use in the major hazard sector.

A summary of three of the most well-known and widely used HRA methods is presented in Figure 1. These are:

- Technique for Human Error Rate Prediction (THERP)
- Human Error Assessment and Reduction Technique (HEART)
- Absolute Probability Judgement (APJ)

THERP – Technique for Human Error Rate Prediction

- Developed by Swain and Guttman in 1983 for the US Nuclear Regulatory Commission
- Applied to nuclear and oil and gas, but could be applied to all high hazard industries
- Well known and widely used, stands up to audit, prescriptive methodology detailed within THERP Handbook
- Resource intensive and time consuming

HEART – Human Error Assessment and Reduction Technique

- First outlined by Williams in 1985 in a conference paper whilst working for the Central Electricity Generating Board
- Applicable to all high hazard industries (e.g. rail and nuclear)
- Well known and widely used, relatively quick and simple, requires limited resource
- Relies on detailed task descriptions and judgement

APG – Absolute Probability Judgement

- Based on the work of Seaver and Stillwell (1983)
- Applied to nuclear and oil and gas, but could be applied to all high hazard industries
- Relatively quick to use, freedom to use domain knowledge, facilitates discussion amongst peers
- Prone to bias affecting validity, likened to "guessing", dependent on appropriate expert selection

Figure 1 – Summary of three HRA methods

STEPS FOR COMPLETING A HUMAN RELIABILITY ASSESSMENT

A common approach can be taken for all quantitative HRAs, with the overall method broken down into five high level steps.

Step 1
Task description and information gathering: Speak to the system designers, Subject Matter Experts (SME), operators, and anyone else who knows how the task in question is carried out.

Step 2
Conduct a task analysis: This is perhaps the most important step of a HRA, because it allows the analyst to break down the task into its discrete steps which then highlights where human error could occur. It also allows the analyst to identify possible recovery opportunities.

Step 3
Choose the appropriate HRA methodology, and generate HEPs for the errors being assessed: Based on industry custom and practice and the types of errors being assessed, an appropriate method is chosen (e.g. HEART, THERP or APJ).

Step 4
Identify any means of human error reduction: This can be based on the Performance Shaping Factors (PSF) identified during the HRA (e.g. increased training and supervision, reduction in time pressure).

Step 5
Write up the work done, including all analysis and justification for the resulting HEPs: Being able to justify why a certain HEP is deemed appropriate and accurate is extremely important as it provides an audit trail and traceability, and is often needed to satisfy industry regulators.

QUANTITATIVE VS QUALITATIVE?

As well as quantitative HRA methods, human reliability can also be assessed using methods that don't result in a numerical assessment of human error probability.

One of the most widely used qualitative methods is Safety Critical Task Analysis (SCTA). For SCTA, the analyst systematically reviews the overall task being assessed, anticipates what failures might occur at different task steps, and analyses what factors could increase or decrease the likelihood of those failures.

References:
1. Sanders, M & McCormick, E (1992) Human Factors in Engineering and Design, McGraw-Hill Education, 7th Edition.
2. Kirwan, B (1995) Human Reliability Assessment.
3. Bell, J & Holroyd, J (2009) HSE RR679 Review of human reliability assessment methods.

This essentially follows a similar process as Steps 1 and 2 for a quantitative HRA, but with a checklist-based approach to the analysis of tasks classified as 'high priority'. Suggested additional controls are then identified where needed and may include:

- Improvements in procedures
- Engineering modifications
- Improved access to equipment
- Provision of training or additional checks

Importantly, there isn't a one size fits all approach for human reliability, and the type and depth of the study can be tailored to the application, ranging from high level to detailed and from qualitative to quantitative.

More information on SCTA can be found in Issue 35 of RISKworld (Spring 2019) at https://risktec.tuv.com/knowledge-bank-riskworld-newsletter/

CONCLUSION

Although human error is often identified as a contributing cause to major accidents, there is scant data from operating experience to allow direct evaluation of HEPs. Instead, mature HRA techniques can be used, which can be applied in all high hazard industries including rail, nuclear and oil and gas.

HEPs generated from HRA feed into the safety case (e.g. QRA) and help identify areas in system and equipment design where human failures are most significant and improvements can be made.

Contact: Clare Parker
clare.parker@risktec.tuv.com

DID YOU KNOW?

Risktec offer training in Human Failures and Safety Critical Task Analysis?

Find out more at https://risktec.tuv.com/our-services/learning/modules/human-failures-and-safety-critical-task-analysis/

PEM 101 – An introduction to physical effects modelling

Physical effects modelling is widely used for characterising major hazards and forms a key part of risk-based decision making in the oil, gas, chemical, hydrogen and Carbon Capture, Utilisation and Storage (CCUS) 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.

PHYSICAL EFFECTS

Physical effects can cause serious harm to people and the environment, as well as damage to structures and equipment. In the oil, gas, chemical, hydrogen and CCUS sectors for example, the physical effects arising from the accidental release of hazardous gases, vapours or liquids can include:

- Gas dispersion (which could be flammable, toxic, asphyxiant or all three)
- Jet fires and pool fires
- Flash fires
- Explosions
- Boiling Liquid Expanding Vapour Explosions (BLEVEs)
- Smoke dispersion
- Subsea dispersion
- Dispersion of oil on water
- Tank fires

In order to manage effectively the risks from these phenomena, it is important to first understand their consequences and implications.

Various techniques are available for modelling the physical effects, ranging from simple equations to empirical software tools based on physics that have been correlated against experimental testing data. The most sophisticated models involve 3-dimensional (3D) computational fluid dynamics (CFD) simulation, which is discussed in more detail in the 'Smart CFD' article in this edition of RISKworld.

MODELLING

The three general steps involved in conducting physical effects consequence modelling are illustrated in Figure 1.

Step 1 – Discharge: The plant is divided into isolatable sections using Piping & Instrumentation Diagrams (P&IDs) or Process Flow Diagrams (PFDs) . The location of each potential release within an isolatable section is determined by considering equipment which could provide a release path, e.g. flanges, valves, or vessels.

The process and release parameters for each of the identified scenarios are specified, such as composition of the material, storage pressure and temperature, and the size of the hole through which the release occurs. These act as input parameters for the physical effects model. The composition determines flammability or toxicity (or both), while the temperature and pressure determine if the release is liquid, gas or 2-phase (a combination of liquid and gas), and the hole size determines the release rate and velocity.

The output from the model describes the 'source term', i.e. the physical properties of the release (e.g. phase, release rate, velocity and duration) at the point location of the release. More sophisticated modelling can assess detailed time histories of a release rather than simple duration.

Step 2 – Physical effects: The next step is to input the source term into further physical effects models to determine the extent of the resulting

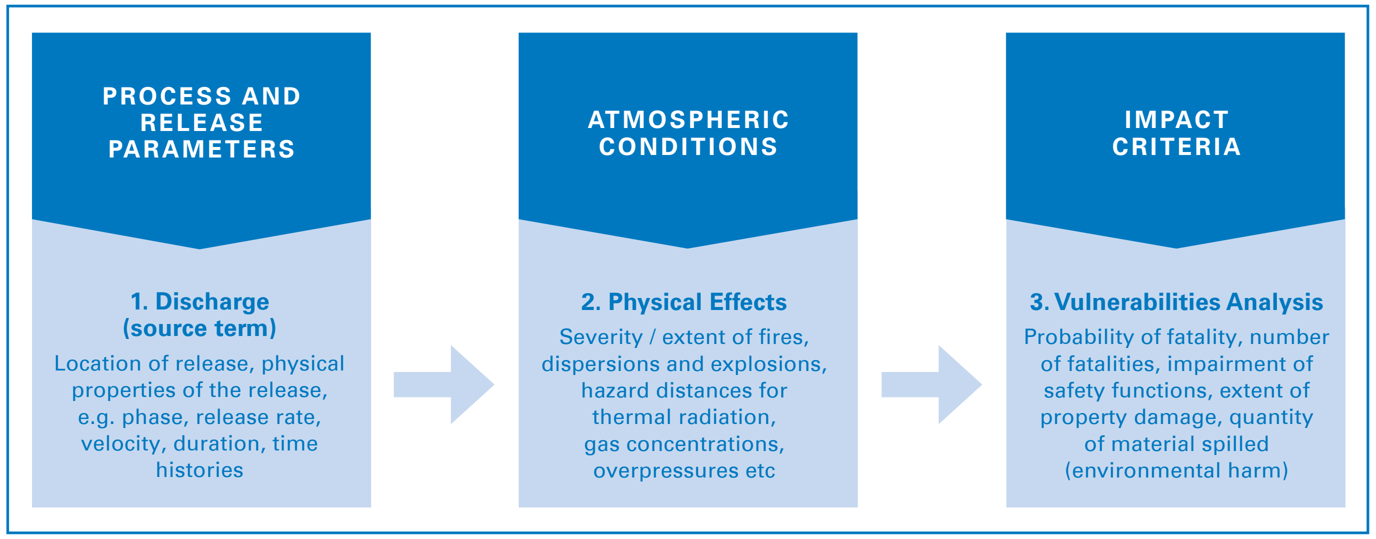


Figure 1 – Three steps to physical effects consequence modelling

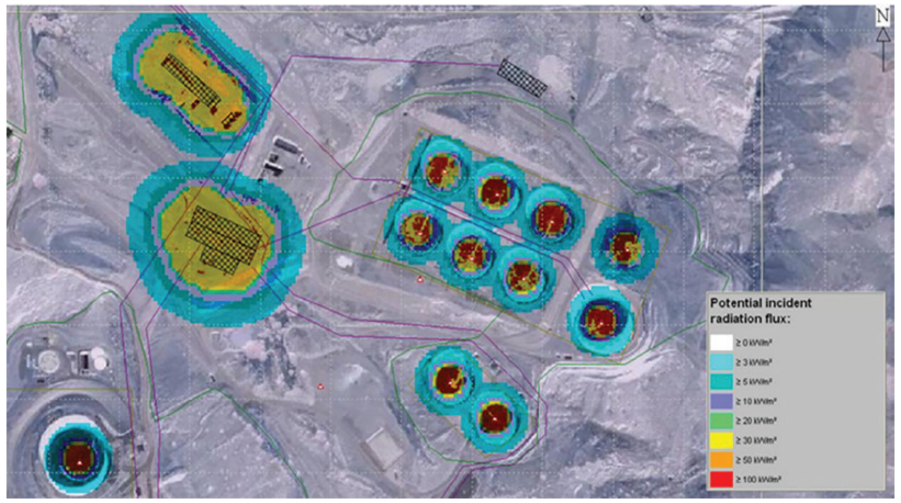


Figure 2 – A plot plan of a tank farm showing thermal radiation levels from hydrocarbon fires

dispersion and potential fires and explosions. The outputs are usually either in the form of distances to specified levels of thermal radiation, gas concentration and explosion overpressure, or in terms of the predicted magnitude of these physical effects at locations of interest; for example, if people are located at a certain place, how much heat will they experience from the fire?

Physical effects can vary greatly depending on the local atmospheric conditions, e.g. wind speed, atmospheric stability, air temperature and solar radiation. In particular, gas dispersion distances are heavily influenced by wind speed and atmospheric stability – the more stable the conditions, the further a gas cloud will disperse. Ambient temperature can affect flashing liquids and the rate of pool evaporation. Atmospheric humidity affects the transmission of heat from fires. It is important, therefore, to choose a set of conditions that are representative of local weather data.

Modelling is often performed using conservative inputs (e.g. worst case pressures and compositions) because if the worst case is acceptable then anything less is also acceptable. However, the cumulative effect of multiple worst case assumptions can be extremely pessimistic, and care must be taken to ensure that each scenario is credible.

Not all of the input data will be well defined and some assumptions will inevitably have to be made. As with any quantitative modelling, all assumptions should be recorded – an 'assumptions register' is a good vehicle for doing this. Whilst physical effects modelling is one of the more accurate risk-related quantitative techniques because the models are based on experimental data from real releases, care must be taken not to use the models outside the limits of their validity.

Sensitivity analysis is an appropriate technique for assessing the impact of uncertainty in the input data and modelling assumptions. It provides an awareness of which inputs and assumptions have the greatest effect on the results and helps to ensure any decisions made are based on a solid understanding of the inherent uncertainties.

Step 3 – Vulnerability analysis: Having determined the severity of a release scenario, impact criteria are used in a vulnerability analysis to translate the physical effect, such as explosion overpressure, into a probability of impact on people, structures/equipment or the environment, e.g. fatality, cost or damage. The vulnerability of people depends on the extent of shelter and protective clothing, and a worst case first estimate would often assume no shelter and no protection.

Impact criteria can be in the form of lookup tables, e.g. someone outdoors exposed to an explosion overpressure greater than 0.5 bar has a 50% chance of fatality, or in terms of mathematical relationships called probit functions. Deriving the impact in this way means it can be combined with frequencies of occurrence to determine numerical risks as part of a Quantitative Risk Assessment (QRA).

USES

Once the consequences of the physical effects have been modelled, validated and understood, the results can be used to help manage facility risks by informing decisions such as:

- Classifying hazardous areas
- Siting buildings and specifying appropriate protection against overpressure, thermal radiation and gas ingress
- Optimising site layouts and separation between units
- Locating vents
- Determining flare heights and assessing flame-out scenarios
- Locating fire and gas detectors
- Providing fire and blast protection and specifying design requirements
- Locating and protecting onsite muster points, temporary refuge and escape, evacuation and rescue equipment
- Impacts on offsite populations and arrangements for offsite evacuation
- Land use planning restrictions on development around facilities
- Emergency response planning

As one example, when planning the location of new tanks or buildings, the plot plan in Figure 2 would help ensure they are located far enough away from potential sources of fire. Or, for existing tanks, the modelling could be used to identify areas where passive fire protection, or cooling water deluges can prevent escalation of fire events from one tank to another.

CONCLUSION

Physical effects modelling techniques range from data correlations and empirical formulae, to complex 3D CFD models (as described in the 'Smart CFD' article in this edition of RISKworld).

Physical effects modelling has a wide range of applications and forms a key input to many risk-related decisions at a facility. As such, it's important that modelling is appropriately applied and validated and that its limitations and uncertainties are well-understood.

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

Smart CFD – Can you get more for less?

Computational Fluid Dynamics (CFD) modelling is a proven tool for the analysis of real-world fluid flow and heat transfer problems, ranging from turbine blade design to fire and explosion assessment. To properly explore potential options or uncertainties may, however, require a large number of simulations, with the associated expansion of costs and timescales. So, is there a smarter way of unleashing the power of CFD?

CFD-BASED OPTIMISATION

Computational Fluid Dynamics (CFD) has gained worldwide popularity due to its proven ability in design optimisation. Unlike physical testing, a large number of numerical simulations can be easily conducted with an arbitrarily low level of error.

However, the ever increasing sophistication and complexity of CFD models has led to higher computational costs, long model run times and the requirement for extensive user expertise. This is compounded by the increasing desire to vary more and more parameters in the search for optimised designs or a greater understanding of the effects of uncertainty, as an input to Quantitative Risk Assessment (QRA) for instance. Thankfully, there are smart methods available that can significantly reduce the CFD effort.

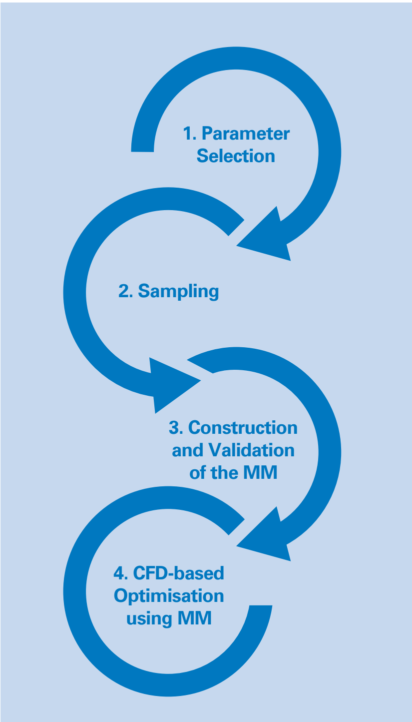


Figure 1 – 4 Stages of Meta Model Application

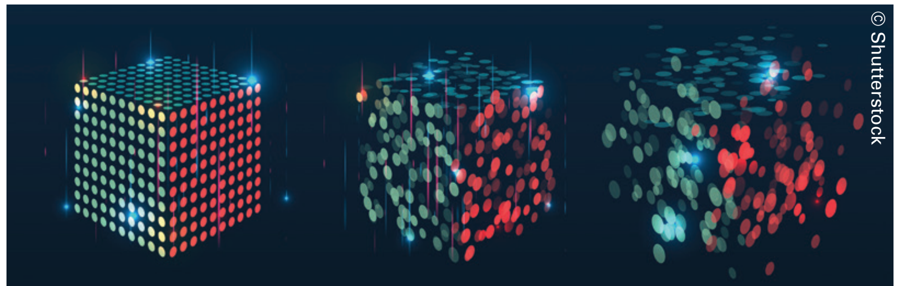


Figure 2 – Potential Sampling Schemes

Over the last 70 years, Meta-Models (MMs) have gained wide adoption as a cost effective alternative to explicit modelling (Ref. 1). MMs (also known as multivariate interpolation / response surface methods) are a powerful tool for substantially reducing computational time and effort through the use of parametric input-output functions.

HOW IT WORKS

MMs allow the estimation of simulation results for a given set of input parameters, thus reducing the number of detailed simulations required. This is achieved through the 4 stage process shown in Figure 1.

MMs make predictions based on pre-prepared data from a limited set of complete CFD simulations. These simulations are chosen to cover variations in the required model parameters, with the parameter values appropriately sampled over the credible range in which they could fall.

Once the MM is trained and validated, the MM can be used in place of the CFD model for generating simulation results across the entire parameter-space (Ref. 3).

DESIGN OF SAMPLING

Unfortunately, as the number of variables (or dimensions) increases, the number of CFD cases required increases exponentially. However, choosing an effective sampling method is a way to reduce the effect of increasing numbers of parameters (see Figure 2).

Available sampling techniques have various benefits and drawbacks, with the most commonly utilised methods being:

1. **Systematic Grid:** This is the most basic sampling method, which utilises a grid of sample points splitting each parameter equally. This is, as it turns out, a very inefficient sampling method (this is clearer when considering 2D projections of the samples, since most of the points line up).
2. **Latin Hypercube Sampling:** Another common sampling technique, which splits the domain into hypercubes and randomly places points. A drawback is that it does not guarantee adequate parameter-space filling.
3. **Quasi-Monte Carlo Sampling:** Methods, such as Hammersley, Halton and Sobol sequences, were designed with efficient parameter-space filling in mind. Sobol sequences are the most efficient of these, and are generated based on primitive polynomials.

TRAINING AND VALIDATION

Prior to training the MM, any scale bias is removed by normalising each of the parameters. The model is trained using the combinations of parameter values generated by sampling and the corresponding CFD results. For testing purposes, a second set of random cases are generated together with CFD results. The magnitude of errors is identified by comparing the MM values against the CFD results. The accuracy of predictions will vary based on a number of factors:

- Number of training data points
- Dimensionality of the data
- Distribution of training data points
- Whether the prediction points are within the domain defined by the training data

Example prediction surfaces and errors are shown in Figure 3.

There are multiple statistical techniques for determining the optimal trained model, such as the Coefficient of Determination (R^2) and Likelihood Function. In practice, more than one technique should be used as there are limitations for each.

APPLICATIONS

MMs have been applied in some form in Explosion Risk Analysis (ERA) for the last 20 years (Ref. 2). Where this involves extensive and complex assets, plant and equipment, there is typically a need for a large number of simulations, given the wide range of possible release scenarios. Combinations of the input parameters can quickly result in thousands of dispersion simulations, simply by varying:

- Release rate, location and orientation
- Representative fluid (composition, temperature and pressure)
- Wind direction and speed

Similarly for explosions, the following variables might be considered:

- Gas cloud location, size and shape
- Representative fluid composition
- Ignition location

The use of MMs in this case can reduce the number of CFD simulations, but predictions can suffer from a loss of accuracy where consequences are especially sensitive to the parameters in question.

MMs can, however, be applied much more widely. Some known applications are listed below, along with the technique often used:

- **Wind turbine blade design optimisation –** Neural Networks, Genetic Aggregation Response Surface (GARS) algorithm
- **Modelling CO2 leakage from a storage complex for CCS –** Neural Networks, Gaussian Process Regression
- **Reliability Analysis of Nuclear Passive Safety Systems –** Genetic Aggregation Response Surface (GARS) algorithm, Neural Networks

TOOLS

There are several commercially available tools for creating bespoke MMs; three of the most commonly used off the shelf include:

- Ansys Inc. Design Xplorer
- Stat-ease Inc. Design-Expert ®
- Mathworks Inc. Matlab

Choosing the correct MM has to consider:

- Accuracy of the results obtained
- Quality of the training database
- Volume of CFD calculations necessary to sufficiently train the model
- Extent to which the accuracy of predictions can be improved

COMPUTATIONAL POWER

Over the past two decades, microchip evolution has very closely followed Moore's Law – the number of transistors on a microchip doubles every two years. Alongside the 1000-fold increase over this period, we have seen a significant increase in affordable computational power. This, in tandem with the ability to utilise high performance computing systems to run large numbers of simulations in a matter of days translates to greater accuracy and coverage of MMs. Conversely, we should not lose sight of the original motives for using MMs, and be aware that this same increase in computing power may dilute the benefits over explicit modelling in scenarios where the analysis cases are well defined.

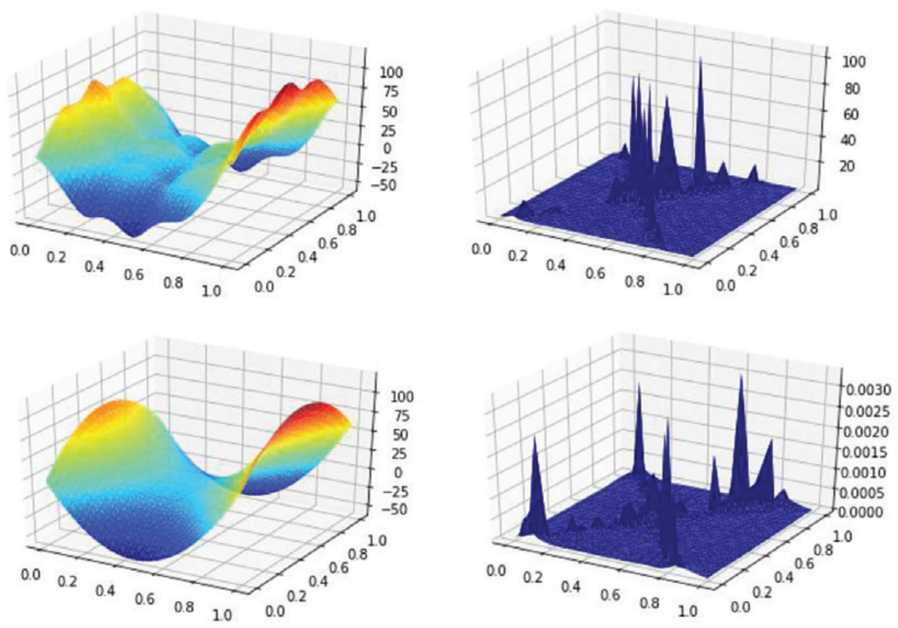


Figure 3 – Validation of Meta-Model

CONCLUSION

MMs can substantially reduce computational time and effort when conducting CFD analysis with multiple variables, although some studies (such as ERA) are inherently less suited than others. This notwithstanding, the accuracy of the predictions are dependent on the sampling method, quality of the training data and choice of statistical validation techniques.

Current applications of MMs range from physical effect modelling to reliability analysis. As computing power and speed continue their upward trajectory, the potential uses of MMs are probably only limited by our imagination.

Contact:
Connor Bloodworth or Michael Kupoluyi
Connor.Bloodworth@risktec.tuv.com
Michael.Kupoluyi@risktec.tuv.com

References:
1. Box, G.E.P., 1951. Wilson. KB [1951] On the Experimental Attainment of Optimum Conditions. Journal of the Royal Statistical Society, Series B, 13(1), pp.1-45.
2. Huser, A., Eknes, M.L., Foyn, T.E., Selmer-Olsen, S. and Thevik, H.J., 2000. Express: Cost effective explosion risk management. In Major hazards offshore (London, 27-28 November 2000) (pp. 3-4).
3. Rößger, P. and Richter, A., 2018. Performance of different optimization concepts for reactive flow systems based on combined CFD and response surface methods. Computers & Chemical Engineering, 108, pp.232-239.

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

CYBER-SECURITY OF OPERATIONAL TECHNOLOGY

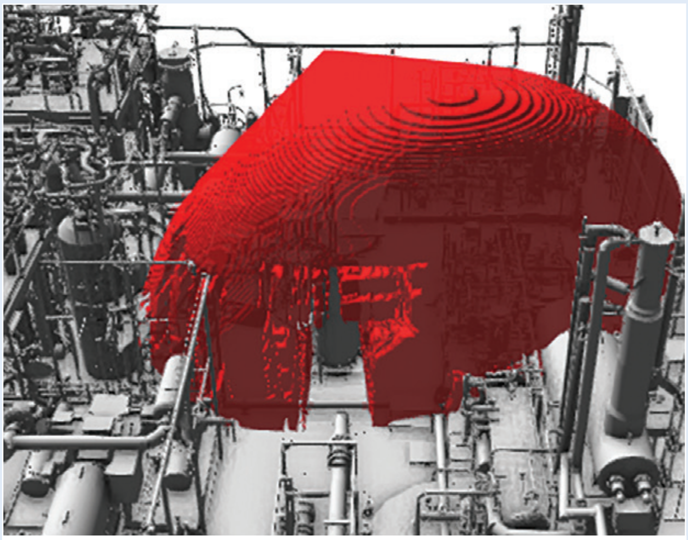
Discussing the cyber threat to industrial automation and control systems.

DELIVERING SUCCESSFUL TECHNICAL WORKSHOPS REMOTELY

The art of conducting remote technical workshops, for example HAZID, HAZOP or LOPA.

COST-EFFECTIVE SAFETY CRITICAL TASK ANALYSIS

Challenging the perception that assessing the enormous number of tasks at an industrial facility would be too time consuming, practical methods have been developed for cost-effective analysis of safety critical tasks.



MAKING THE MOST OF FIRE AND GAS DETECTOR MAPPING

Using fire and gas detector mapping studies to support the design process and optimise the number of detectors needed to meet coverage targets.

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