RISKworld

issue 22 autumn 2012 — *the newsletter of risktec solutions limited*

In This Issue

Welcome to Issue 22 of RISKworld. If you would like additional copies please contact us or download from www.risktec.co.uk. Feel free to pass on RISKworld to other people in your organisation. We would also be pleased to hear any feedback you may have on this issue or suggestions for future editions.

Contact: Steve Lewis (Warrington)
steve.lewis@risktec.co.uk

Contents

Risktec

Safety Leadership in Action

"Every day you may make progress. Every step may be fruitful. Yet there will stretch out before you an ever-lengthening, ever-ascending path. But this only adds to the joy and glory of the climb." Sir Winston Churchill

We are pleased to bring you some updates from Risktec and welcome you to the latest edition of RISKworld, which also marks over 11 years of successful operations.

Our new office in Bristol, which opened in August, continues our commitment to deliver services close to our clients, and provide a platform for local recruitment. We now have a total of 13 offices globally, where our 190+ staff operate from, plus over 70 associates actively supporting projects and clients in many countries around the world.

ASTEC, our Resource Solutions business, which joined the Risktec group last year, is developing well, providing a flexible technical support service to a wide range of clients.

Our collaborative partnership with Liverpool John Moores University is flourishing, with more postgraduate awards being made during the summer graduation ceremonies. In addition, more than 50 students from around the world are now working towards their awards on our Distance Learning programmes.

We would like to thank client personnel who completed our recent survey on our performance; your feedback and comments are very important to us. We were pleased that the response was overwhelmingly positive and we will remain committed to delivering the highest possible standard of service in the years ahead.

The diversity of the articles published in this edition of RISKWorld is a reminder of the wide range of responsibilities associated with operating hazardous facilities, from detailed numerical analysis to leadership. The words of Winston Churchill are a reminder that safety improvement is a continuous and challenging, but rewarding endeavour.

Contact: Alan Hoy (Warrington)
alan.hoy@risktec.co.uk

Balancing Personal and System Safety

Holding the handrail and putting lids on cups of hot coffee will not prevent major accidents. That is the message coming through loud and clear in the aftermath of recent disasters such as the Texas City refinery explosion in 2005, the Gulf of Mexico oil well blowout in 2010 and the Fukushima nuclear meltdown in 2011. Disasters don't happen because someone slips down the stairs or bumps their head. They result from flawed ways of doing business that allow inappropriate risk control.

Many organisations implement initiatives and campaigns aimed at promoting personal safety in the workplace, both in attempts to achieve a measurable step change in safety performance and to demonstrate corporate commitment to good safety culture. This is very important, but don't expect those actions to lead directly to improved system safety, which concerns the integrity of the process or operations. Indeed, the year before the Texas City explosion the refinery had its lowest injury rate in history, nearly one-third of the oil refinery sector average.

Different approaches

The traditional 'accident pyramid' model mixes together personal safety and system safety. This is not very helpful because it implies "holding the handrail" will prevent an explosion. Today it is a far more useful concept to view the situation as two separate pyramids with some overlap (see Figure 1).

The role of incorrect mental models that don't reflect what actually happens is well documented in major incidents, e.g. Three Mile Island, where operators believed a coolant leak could not lead to a rising coolant level (although this was well understood scientifically). So if management's mental model is that personal safety initiatives will prevent major accidents, is there a blindness to major risk? Moreover, what message is really being sent to staff by rolling out an occupational safety initiative at a facility with a history of leaking pipes?

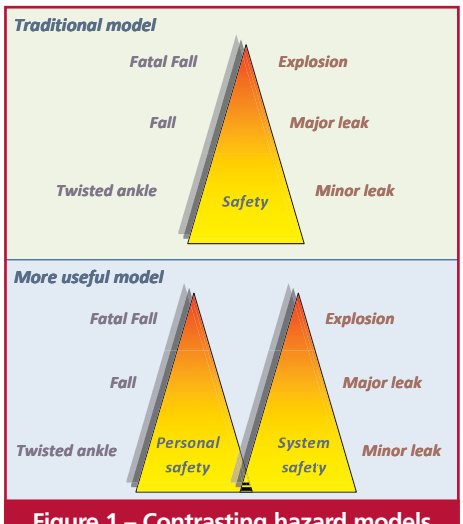

Figure 1 – Contrasting hazard models

Furthermore, what works for one company or location in achieving safe operations may not be applicable to another. For example, the portfolio of risks present for a major hazard site such as a refinery will be very different to a manpower intensive, low hazard environment like an office, as will the way in which those risks are managed. It would be reasonable to suggest that the former will require both occupational and system safety approaches, whereas the latter will be primarily focused on occupational issues.

Different mindsets

With occupational safety there is a direct and visible link between the action (holding the handrail) and the benefit (avoiding a fall). As such it is generally easier to make improvements by bringing about changes in safe behaviours, and its traditional lagging metrics, e.g. loss time injuries, are familiar and easy to measure.

> Creating the right mindset is not an effective strategy for dealing with hazards about which workers have no knowledge...

System safety on the other hand is less visible and more complex because it focuses on the integrity of the design, operation and maintenance to prevent major incidents. Its metrics, particularly proactive ones (e.g. percentage of safety-critical equipment that performs within specification when inspected) are harder to define, measure and interpret. Although there is some overlap, believing that improvements in one means that the other is also improving is at best misleading, and at worst, dangerous.

Having a mindset to hold a handrail is not in itself a bad thing – it's simple, costs nothing and may prevent a fall, but is it really rational to assume that this will prevent a pipeline leak? Yes, the mindset may mean that personnel are more proactive in major accident safety, but what really matters is top down leadership – that leaders have a focus on system safety when allocating resources and making decisions, that any cost-cutting is managed effectively, that bonuses are not solely tied to personal-injury metrics – and that the plant is properly designed, operated and maintained by competent personnel.

Understanding risk

While, globally, occupational hazards kill and injure more people than major accidents events, a single catastrophic event can wreak widespread harm and jeopardise the survival of an entire organisation. So where should an organisation focus its efforts? This comes back to the very crux of the issue – an organisation that does not clearly understand its full spectrum of risks will not be able to manage those that are important.

Conclusion

The benefits of personal safety based initiatives are clear; properly conceived and implemented they will minimise injuries and save lives. But they should be viewed as one part of a balanced approach to risk management, based on a clear understanding of the wide landscape of risks faced by an organisation, and its leadership practices, culture and approach for assuring safety across the whole business.

Contact: Andy Lidstone (Warrington)
andy.lidstone@risktec.co.uk

Applying Modified HAZOPs to Well Testing

Hazard and Operability studies (HAZOPs) are widely used in the oil and gas industry to examine process systems, but less so for drilling, completion and well testing activities. This is typically because the traditional HAZOP applies process-based guidewords to Process & Instrumentation Diagrams (P&IDs), whereas drilling, completion and well testing activities are more procedurally-based and also use Well Test String Diagrams.

However, well testing is widely recognised as a higher risk activity since temporary equipment is brought onto the drill site, hydrocarbons are deliberately brought to the surface and personnel from several companies are required to work together during the campaign. Not surprisingly, applying the rigorous and systematic method of HAZOPs – suitably modified to reflect the differences between well testing and process plant – has been found to help reduce and manage the associated risks.

Well testing 101

Well testing is carried out to better understand an oil or gas well's performance and the reservoir's characteristics. Well tests incorporate many aspects of operations from the worlds of drilling and process plant production.

A basic well test system consists of a subsurface string, incorporating down-hole tools such as gauges, check valves, flow switching valves, isolation valves and packer assemblies, together with a surface system for separating, sampling and metering the fluids flowing from the well.

A typical well test has a number of distinct stages: running a test string, setting packers inside the production tubing, perforating the reservoir, displacement of kill weight fluids in the well, flow and pressure build-up periods, bullheading of fluids, reservoir stimulation, well suspension, and flow between rig pits, tote tanks and well test surge tanks.

HAZOP coverage

In addition to considering the surface package built from a number of modules that are assembled for each well test, a HAZOP would also consider services such as coil tubing, nitrogen and acid injection equipment.

By converting Well Test String Diagrams to P&IDs, it is possible to extend the HAZOP to the downhole systems and thus consider all stages of the well test programme individually.

The benefits

The HAZOP approach enables a thorough examination of what may go wrong and the sufficiency of the preventive and mitigation controls in place. Moreover, it can be used to examine the interaction between the well test systems and the rig systems, particularly the rig manifold and standpipe arrangements, rig pits and rig pumps and emergency response systems.

The HAZOP technique is interactive and enables all parties involved in a well test to improve their understanding of the well testing process as a whole and how the different systems and organisations interact. This is a crucial benefit given that, unlike process plants, well testing systems are largely manually operated and successful operations require personnel from the oil company, the drilling rig provider and various service providers to work together effectively. Hazards are highlighted as a matter of course, but the HAZOP can also be used to identify the role played by each party in assuring safety, and highlight any holes in responsibility or potentially conflicting activities.

Conclusion

While most of us are familiar with the utility of HAZOP as a tool for hazard identification for process plant, in the right hands the technique can be applied successfully to well testing and, as well as determining the adequacy of the safeguards. It can also help clarify organisational interfaces and responsibilities for safety, and build ownership of controls for an activity that is considered to be higher risk compared to production activities.

Contact: Mark Taylor (Aberdeen)
mark.taylor@risktec.co.uk

Stakeholder Management and the Engineering Change Process

Changing times

Whether it is a simple decision to replace an obsolete piece of equipment or a more involved deliberation of the options available to address an emergent safety or production issue, many industries adopt an 'Engineering Change' process (or equivalent). Its purpose is to control the transition from the existing to the desired condition in a manner whereby safety, the environment, and operating efficiency are not adversely affected.

For the most part, Engineering Change is used for implementing solutions to technical problems (such as obsolescence or poor reliability, efficiency, or maintainability) or for enhancing operations (e.g. a production upgrade). On the face of it, identifying a technical solution which is aimed at maintaining, or even improving safety or operating efficiency is a rewarding aspect of an engineer's role. However, it would be unusual and potentially undesirable for a sole individual to recognise the problem, identify the solution and implement it. As a fundamental control measure within the Engineering Change process, other stakeholders will invariably, and quite correctly, become involved.

Balanced decision-making

Whilst perhaps it is a reasonable expectation that all stakeholders will hold a similar set of values regarding safety, other drivers come into play depending on the specialist role of each stakeholder. Taking a simple example of installing a new cabinet containing a safety-related control function: the operator may expect it to be positioned where it does not present an obstruction, the maintenance department may ask for it to be positioned such that access for calibration and testing will be gained without the need for ladders or scaffolding, whereas the safety case engineer may request that the cabinet be positioned in an area remote from recognised hazards. Satisfying these constraints could mean that the cabinet would be positioned 200 metres from the nearest available power supply, in which case the budget holder may have something to say about cable costs!

Stakeholder management

One solution is to appoint an Engineering Change 'champion' (or similar) to drive the change through and manage the expectations of all stakeholders. Impartiality is vital; that is, recognising that the influences underpinning each stakeholder's expectations are equally valid. The ability, and indeed willingness, to analyse and explain each stakeholder's requirements in a measured manner is often crucial in reducing the risk of differences of opinion turning into conflict.

Maintaining good relationships with the stakeholders is pivotal to success. Interpersonal conflict is not only unpleasant, it can also be costly, in terms of time, resource and money, and has the genuine potential for decisions to be made that may ultimately result in an adverse affect on operating safety.

Conclusion

Controlling engineering change is an important part of assuring the safety and operational efficiency of major hazard facilities, but can become bogged down or ineffective without active stakeholder management.

Contact: Dave Fiddler (Warrington)
dave.fiddler@risktec.co.uk

No Need for Alarm? The Art of Alarm Management

The design philosophy of any alarm system is to alert the operator to a plant condition that has reached or exceeded a pre-defined limit, so that he or she can take action or monitor any automatic response.

Too much information

Historically, as organisations have begun to make formal claims upon alarms within safety cases as a line of protection against a specific fault condition, they have gained a much higher prominence. At the same time, the growing capability of modern alarm systems (both hardware and software) has made the provision of alarms relatively simple, leading to a proliferation in the number and diversity of alarms. Coupled with increasing plant complexity, the control room operator is often faced with a huge array of alarms, covering many scenarios. This can make it challenging to differentiate between the alarms that are important and those that are not, and to diagnose the root cause of the problem.

To compound the issue, as the plant ages and is modified, alarms can be rendered redundant or may be replaced with alternative indication.

Incorrectly configured alarms can cause frequent spurious alarms which can introduce a culture of complacency where a real alarm could fail to prompt a timely operator response.

Modern alarm management

A modern plant requires a robust alarm management philosophy. This identifies the purpose, importance and priority of each alarm, action to be taken on alarm failure, operator training and a robust management of change process (see Box 1).

Where operator response is claimed in a safety case, the alarm should be unambiguous and directly traceable to the hazard. Techniques such as Bowtie analysis can provide a visible link between the hazard and the alarm condition and clearly highlight the requirement for operator training, procedures and maintenance arrangements. This helps ensure that the safety integrity claimed for the alarm can be achieved, and supports any justification required of the Human Error Probability associated with operator response (e.g. for use in PSA/QRA – see Page 6).

The presentation of the alarms should be carefully considered and reflect the operating conditions. In this regard, human factors assessment is an integral and important part of system design and aims to ensure that alarms cannot be missed, masked or mistaken.

The number of configured alarms should be rationalised and minimised, with each alarm configured to minimise spurious activation and provide clear information to the operator, supported by procedures and training.

Ongoing performance monitoring is essential to ensure that frequent alarms are identified and the root cause investigated. Changes to the plant may require re-assessment of alarm systems.

Conclusion

Failure to manage alarms properly undermines the operator, the safety case and plant safety. By having a robust alarm management system in place, the operator has the best chance of taking the correct action when required.

Contact: Grant Reekie (Edinburgh)
grant.reekie@risktec.co.uk

Box 1 - Alarm management philosophy

- Specify required alarm integrity (operator response and alarm design)
- Design alarm system (e.g. alarm presentation, alarm levels, operating environment, etc.)
- Assess, demonstrate and justify the integrity of the alarm hardware / software
- Specify required operator action on receipt of alarm and on alarm failure
- Provide training and assessment to underpin claims made on operator integrity
- Provide adequate routine maintenance and proof testing to demonstrate integrity
- Implement robust change management to identify any changes that could affect integrity

What's in a Number? Myths and Realities of PSA and QRA

In many major hazard industries there is a regulatory requirement that the risk posed to people by operation of a facility is shown to be tolerable and as low as reasonably practicable.

But, how do you measure risk? There are several techniques available to estimate risk, ranging from simple, qualitative frequency-consequence matrices through to use of complex quantitative event tree, fault tree and consequence models. The precise technique used depends on the stage in the facility lifecycle, the complexity of its design and operation, and the potential consequences of any postulated accidents. In certain industries (such as nuclear, rail, oil & gas), acronyms like PSA (Probabilistic Safety Analysis) and QRA (Quantitative Risk Assessment) have become synonymous with the use of complex risk models and computer codes, accessible to a limited number of practitioners who often use mystifying language, but are able to generate seemingly authoritative risk numbers. As a consequence, a number of PSA/QRA myths have flourished.

Myth #1 – I can believe the numerical answer without question

Reality #1 – PSA/QRA provides an estimate of risk based on a large number of assumptions and input data, some of which may be uncertain

Paraphrasing the old saying - there are lies, damn lies and PSA! The numerical risk evaluated by a PSA/QRA can be meaningless without an understanding of the purpose for which it was intended and the underpinning assumptions and uncertainties. Often data will be taken from other facilities, or even generic databases, which may or may not be directly applicable. Some of the phenomena considered in the analysis may not be well understood and, although PSA/QRA is expected to be best-estimate, a bounding assessment may need to be adopted.

Myth #2 – PSA/QRA is only required to comply with the requirements of the Regulator

Reality #2 – If properly conducted, PSA/QRA can provide valuable insights into the strengths and weaknesses of a design and the way it is operated

At different stages of facility development PSA/QRA can be used to identify important design or operational issues, and can help focus or prioritise their resolution, as well as looking at potential solutions. It can be used to optimise maintenance activities and therefore minimise plant outages. Ultimately, PSA/QRA provides an input into demonstrating that the risk posed by planned operations is as low as reasonably practicable.

Myth #3 – There is only one accepted method for calculating risk

Reality #3 – There are several valid methods available to assess risk

Given the potential expense, it is important to ensure that the intended purposes of a PSA/QRA are well understood so that the right level and type of analysis is undertaken. The quantitative method used at the preliminary design stage may not be what is appropriate or necessary to support detailed design or, for that matter, operations. For relatively low hazard facilities, a simple evaluation of risk may well suffice.

Myth #4 – The PSA/QRA is my safety case

Reality #4 – PSA/QRA forms part of the overall safety case and is not a catch-all that will ensure your design is acceptable

PSA/QRA complements, but is not a replacement for, good qualitative studies such as bowties, deterministic safety assessment or similar conservative, non-quantitative techniques that are used to assess faults and hazards and the suitability and sufficiency of controls. Neither should PSA/QRA be used to justify non-compliance with legal requirements.

Key to success

The key messages to take away are that PSA/QRA should:

- Be viewed as tools to aid in managing risk at all stages in a plant lifecycle.
- Be integrated with the design and operating processes.
- Be underpinned by an appropriate level of data.
- Not be considered an exact science.

Results should be used with a degree of caution and should be supported by qualitative understanding before informing decision-making, such as a design change.

The more complex the project, the more sophisticated the PSA/QRA is likely to be, involving a larger number of potentially affected stakeholders. Equally, the higher the associated risk, or sensitivity to an increase in risk, the more robust and comprehensive the supporting evidence should be.

Conclusion

To some, PSA/QRA may seem like another legislative or corporate hurdle. However, in the right hands, it provides a very powerful tool that can be used to aid understanding and support the decision-making process during the design and operation of a facility.

Contact: Steve Hendrie (Warrington)
steve.hendrie@risktec.co.uk