RISKworld

issue 27 spring 2015

the newsletter of risktec solutions limited

In This Issue

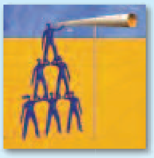
Welcome to Issue 27 of RISKworld. If you would like additional copies please contact us, and feel free to pass on RISKworld to other people in your organisation. We would also be pleased to hear any feedback you may have on this issue or suggestions for future editions.

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

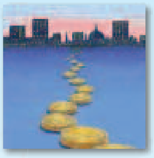
Contents

Risktec
TÜV Rheinland Group®

Satisfaction (almost) guaranteed

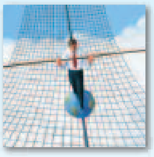


96% of clients rate the technical knowledge of our personnel as very good or good



97% of clients believe they have received good value from us compared to other consultants

96% of clients view us as easy to do business with



99.6% of clients would recommend us

Statistics are average over last three years from about 500 responses to Risktec's twice yearly customer satisfaction survey

It is over a year since Risktec joined the TÜV Rheinland Group (TRG) and in addition to the Risktec core business continuing to grow and develop, a number of the benefits of being part of TRG are being realised. New Risktec offices in Abu Dhabi and the Houston energy corridor have recently opened, utilising shared office space with group companies. Moreover, a steady flow of work has passed between group companies, extending the range of services provided to our clients.

Risktec's Managing Director, Alan Hoy, commented, "Our priority is to deliver our high standard of services to our established clients, and it is very pleasing to see that our regular client surveys are confirming that our standards are being maintained at a very high level. We have also worked closely with colleagues across TRG to respond to enquiries and explore how Risktec can contribute to the development of the group. These interactions have confirmed the close alignment in business values and we are confident that the decision to join TRG was the right one".

We hope you find the articles in this latest edition of RISKworld to be interesting and thought provoking. We are particularly pleased that Lee Allford, from the European Process Safety Centre, has contributed an article based on his MSc research project. Lee was recently awarded an MSc with Distinction in Risk and Safety Management[1] and won the Risktec best student prize in 2012.

The wide range of topics in this edition illustrates the ever growing challenges of demonstrating and assuring safe operation. To achieve this requires expertise across a wide spectrum, from a detailed understanding of highly complex technical systems through to the critical importance of effective safety leadership. The increased focus on security brings new and evolving challenges and the possible conflict with safety requirements. Rigorous, yet proportionate, assessment of risk is invaluable to help operators of potentially hazardous facilities operate safely and remain constantly vigilant to changing circumstances.

A thorough understanding of risks, which are well managed by competent organisations, will help ensure "it will never happen here".

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

Note

[1] Awarded by Liverpool John Moores University in partnership with Risktec

The Integral Safety Leader: Thinking about the Whole

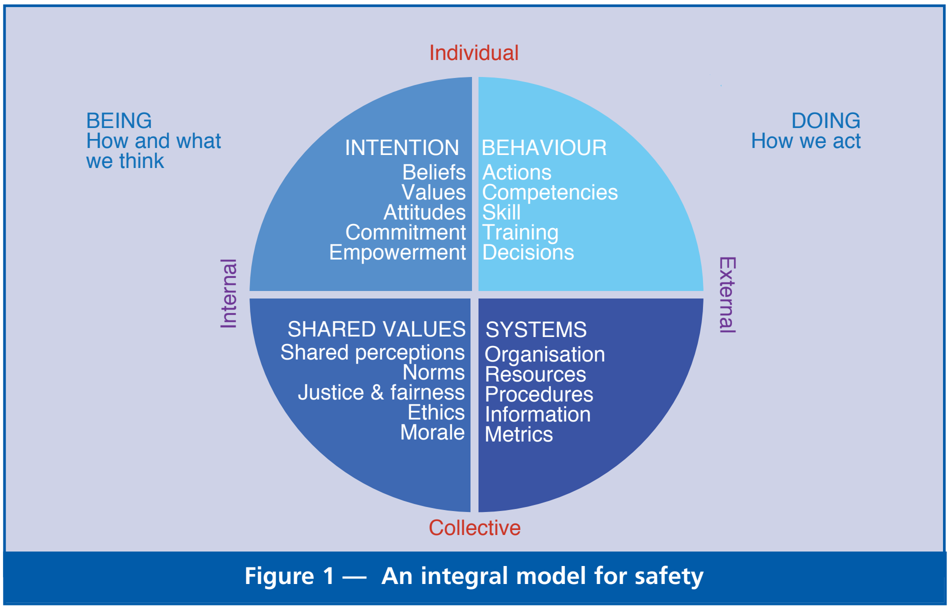


Figure 1 — An integral model for safety

Put yourself in the mind of a line manager responsible for the safety of personnel. You have been warned of many deficiencies in a part of the business, including a strong indication that a significant accident has a worryingly high potential. How do you begin to think about this problem?

It is not easy, the problem is complex. There is a great deal to think about – technology, procedures, competency and cost, just to start. Einstein once said, "You cannot solve a problem from the same thinking that created it." But how can you learn to see the world anew? Would an 'integral theory' of safety leadership help?

Integral theory

Ken Wilber, an American philosopher and writer, published the Integral Theory in 1997 (Ref. 1). He asserted that each of the dozen most influential schools of consciousness, such as cognitive science, neuropsychology and eastern traditions, has something irreplaceably important to offer our understanding of consciousness. What he created was a general 'whole' model sophisticated enough to incorporate the essentials of each of them.

Integral simply means comprehensive, balanced and inclusive. It helps make sure that nothing gets left out. A useful theory will change perspectives, which will then lead to the implementation of new strategies, actions and behaviours. Integral theory helps those who are ready to use it. It would be a mistake to force it on anyone.

An integral model for safety

An integral model for safety, based on Wilber's integral theory, focuses on the four perspectives of safety performance, or 'quadrants', as shown in Figure 1. The four quadrants – which are the four basic ways of looking at anything – turn out to be fairly simple: they are the inside and the outside of the individual and the collective.

The right side is the objective, outside, external view. It is observable and measurable. It is how we act, our 'doing'. Most organisations in the high hazard industries are dominated by technical people such as engineers, scientists and accountants, and so it is not surprising that they understand this side of the model. However, they sometimes struggle to understand the left side because it is the subjective, internal view – you cannot reliably observe or measure what is in the minds of people. It is how and what we think, our 'being'. Arguably the greatest opportunity for improvement in safety performance would appear to stem from this left side…but let's take a closer look.

The upper right quadrant is the domain of **behaviour**. It is all the things that you see the individual doing or working with. Improvements in this area come from working with individuals to modify their behaviour. Having a well developed behavioural-based safety programme is crucial to success in this domain.

The lower right quadrant is the domain of **systems**. It includes organisational structures, procedures, formal and informal processes, metrics and rewards. A robust and effective safety management system is critical here. Change in this domain is driven by good management.

The upper left quadrant is the domain of **intention**, the view from the 'interior' of the individual, their consciousness, their self. It is the language of "I" and includes the values and commitment the individual brings to all situations. Improvements in this area come from working with individuals, through leadership and coaching. Change in this area is typically perceived as difficult and requiring time. In reality a change in intention, such as commitment to safety, can happen in an instance – the "aha" light-bulb moment.

The lower left quadrant is the domain of **shared values**, the view from the interior of the group. It is the language of "we" and includes the shared perceptions, norms and standards of the group. It is here we find the ethics, morale and sense of justice that is commonly held by the group. Positive change in this domain, such as creating a 'just' safety culture, has its origin in leadership. This quadrant is itself often labelled as 'culture', but a broader interpretation is that culture embodies all four quadrants – the whole.

The integral leader

Our overall safety performance will only be as good as our least developed quadrant and how well all four quadrants work together. Any solution that does not genuinely succeed across all four worlds will be inherently lacking. When the line manager we introduced earlier starts to look through the integral lens, thinking about issues in each quadrant, everything has the potential to come into focus. With focus comes clarity and with clarity comes better decisions. The intent is to be as all-inclusive and caring as possible.

Conclusion

Being receptive and open minded to an integral approach presents many possibilities for improvement in safety performance and, ultimately, transformation – for you and your organisation. If you feel it has some potential, just try it and see.

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

References

1. An Integral Theory of Consciousness, Ken Wilber, February 1997.

Internal auditing of process safety – a false sense of security?

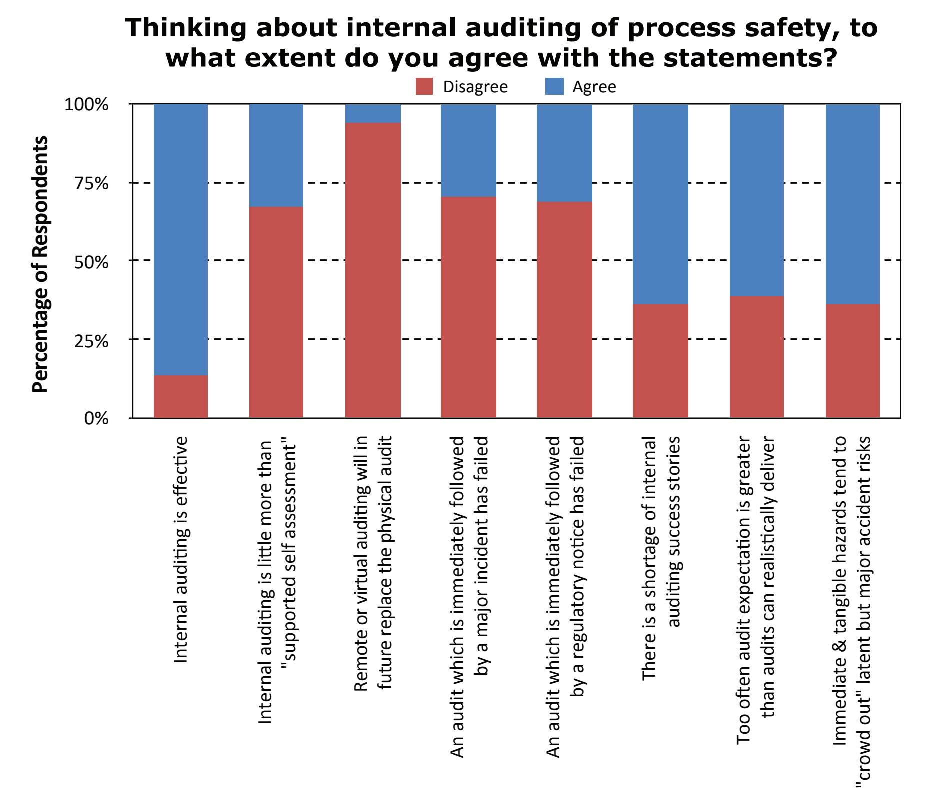


Figure 1 – Process safety internal auditing survey results

In the wake of recent major accidents, several investigation reports have publically criticised the effectiveness of internal auditing of process safety. Recent research (Ref. 1) sheds light on whether process safety practitioners and those individuals at the front line of auditing share the view that internal process safety audits provide a false sense of security.

The research was conducted in 2014 as part of an MSc in Risk and Safety Management offered by Risktec, and canvassed facts and opinion, unattributed, using online survey software. It targeted about 70 process safety professionals working for operators of major hazard facilities who are also company members of the European Process Safety Centre (EPSC), which sponsored the research.

One of the later sections of the survey invited responses to statements related to process safety auditing which speak to commonly voiced criticisms or are simply contentious (see Figure 1).

Highlights

The headline survey finding is that around 86% of respondents believed internal auditing to be effective. A less emphatic but still sizeable majority of respondents believed that audits did offer more than supported self-assessment, underpinned by the view that audits provide a level of probing which uncovers major hazard risks that the site has hitherto been unaware.

Greater polarisation was seen to the suggestion that there was too high an expectation of process safety auditing, that there were too few success stories related to auditing (e.g. risk reduction actions as a result of auditing) and that immediate, tangible hazards crowded out latent, multi-causal process safety risks.

The survey contained a couple of questions related to hypothetical scenarios following an audit. The first was an audit followed by a major accident. About 30% of respondents agreed that this was an audit failure. The flip side is that about 70% of respondents disagreed that this scenario amounted to audit failure. An audit by its nature is both a sample and snapshot and offers no guarantee of avoiding major accidents. However, an audit programme should reduce the likelihood of a major accident occurring. That this view is not necessarily shared universally outside the process safety community is in part corroborated by about 60% of respondents who believe that audit expectation is too often higher than the audit can realistically deliver.

One question which looked to the future proposed that virtual or remote auditing would replace an on-site audit. In other words, the auditor would be distant to the plant under audit and modern technology would present the plant and its people and processes to a remotely located audit team. Almost 95% of respondents disagreed with this notion.

Conclusions

The research highlighted auditor competence and senior management commitment to the audit process as areas for improvement.

Practitioners believe internal auditing by competent auditors is effective and reduces the potential for a major accident, but also feel that too often the expectation of what an audit can realistically deliver is too high. Just because an audit shows good process safety results yesterday, it is no guarantee that a major accident cannot happen tomorrow. This reinforces the need for managers not to be complacent when receiving positive audit reports but to maintain a sense of chronic unease and ask, "Is there anything we're overlooking and what else do we need to do?"

References

1. Internal auditing of process safety – a false sense of security? MSc dissertation, Lee Allford, 2014

Contact: Lee Allford (Rugby, UK)
LAllford@icheme.org

Prescriptive safety: Have we gone too far?

In NASA's heyday, the safety of the space shuttle was assured by a strict adherence to 'Flight Rules'. These were black and white rules that identified precisely what action should be taken under specific circumstances. For example, if instrumentation suggested a fuel cell had failed, the launch was cancelled. No argument, even if instrumentation malfunction was suspected. Their purpose was "to protect against the temptation to take risks" (Ref. 1).

Continuous improvement?

Flight Rules were developed over the course of the shuttle programme, and took into account lessons learned from both real and simulated failures. As such, they grew in number steadily, and whilst they undoubtedly saved lives they were also responsible for an increasing rate of aborted missions. Although it seems churlish to argue with such an approach in the context of the hazards of space flight, as evidenced by the Challenger and Columbia disasters, it illustrates nicely one of the potential pitfalls of black and white safety improvement.

Black and white safety

Coming back to earth, the major hazard industries face a somewhat parallel situation as standards mature. Lessons learnt are continuously reflected in updated or new regulations, codes and standards, both from recognised professional institutions and operators, for everything from nuts and bolts, to cranes, to blowout preventers. The majority, like Flight Rules, are black and white – there are no shades of grey for circumstances where the consequences of failure are limited or infrequent (or both). Inevitably, compliance ratchets the costs throughout the life cycle and for each new project.

In the nuclear industry, which is arguably the most mature (and most expensive), this vicious circle is broken to some extent by classifying equipment according to its importance to safety and tailoring requirements to avoid gold-plating.

Maritime classification societies and the IMO, on the other hand, have introduced risk-based rules and goal-based standards respectively in recent years, which in principle provide more flexibility and steer away from blind compliance.

ALARP thinking

In the UK, the principle of reducing risks ALARP (As Low As Reasonably Practicable) adds into the mix a legal imperative for continuous improvement. In a nutshell, for new equipment the ALARP principle requires compliance with relevant codes and standards and adoption of good practice elsewhere as a minimum, together with consideration of options for improvement, which can only be discounted if the time, trouble and cost are grossly disproportionate to the benefit. If these improvements are subsequently enshrined in updated standards or deemed to be relevant good practice, this becomes the new baseline.

The problem is compounded when more and more preferential requirements are added into standards by well intentioned technical authorities – something that is quite common in large operators with their own engineering standards. The standards can become complex, difficult to comply with and may even lead to design solutions where the associated safety risk is actually higher than a simpler, cheaper design based on inherent safety thinking. Moreover, it is difficult to see how raising standards ad infinitum is sustainable, economically speaking.

Quite clearly, the solution to this conundrum is to think hard about the potential applicability of standards and make clear the distinction between essential and nice-to-have requirements in varying circumstances. At a high level this could take the form of specifying when certain standards as a whole apply (and when they don't). At a more detailed level, within standards themselves, there is plenty of scope for spelling out any relaxations or offering alternative risk-based avenues of compliance.

Conclusion

In a world where spiralling costs in the name of safety are a recipe for project cancellations, the clear message to operators and professional bodies is to build risk-based flexibility into otherwise black and white standards.

References

1. Chris Hadfield, An Astronaut's Guide to Life on Earth.

Contact: Steve Pearson (Warrington)
steve.pearson@risktec.co.uk

Cyber Risk for the Rail Engineer

Cyber security issues have pervaded almost all aspects of life as daily data breaches and hacked websites testify. In the rail sector, where previously isolated control systems have become connected to the internet, we have seen a new challenge emerge for engineers tasked with ensuring system reliability, availability, maintainability, safety and now security (RAMSS).

There are very good reasons for connecting control systems to the internet. Operating costs can be kept lower and reliability and performance can be greatly improved by providing more timely information and instruction for maintenance. There is also a safety benefit from a reduction in human error.

Unfortunately the commercial drive for internet protocol (IP) enabled systems has brought in security risks, with systems now being exposed to hackers across the internet. Hacking control systems is the new and growing pursuit of hobbyist hackers, those with malicious intent and nation states alike. As more and more IP enabled and connected, commoditised hardware is used, cyber related risk needs to be considered; it is now a given that any current or future rail system may use products vulnerable to cyber attack.

Box 1 - Managing Control System Cyber Risk

- **Accept that cyber risk is now a part of everyday rail engineering activity**
- **Become cyber aware and take an interest in cyber related security issues**
- **Get a thorough understanding of the control systems in your domain and ensure that they have been cyber security risk-assessed and incorporated in the safety case**
- **Ensure control system vendors are able to provide evidence of a detailed third-party cyber security evaluation of their products**

The reality of cyber risk

Probably the first time the public was made aware of control system hacking was in 2010 when the Stuxnet computer worm was widely reported to have infected nuclear facilities in Iran. A technician plugged a worm infected USB stick into a control system PC. This adversely impacted the site's centrifuges and their ability to enrich uranium. Over the past year other control systems have been hacked due to weak system passwords or simply because control system administration interfaces had no firewall or authentication mechanism in place.

Cyber risk and rail systems

Those responsible for infrastructure are taking cyber risk seriously: the UK Government's 2010 National Security Strategy rated cyber attacks a 'Tier One' threat alongside terrorism, war and pandemic disease. Rail engineers need to take an equally serious approach to cyber risk.

In the UK, with the move to unified control systems and regional operational centres, the impact of a successful cyber attack can have national implications. How might cyber security affect other systems such as power, passenger information, asset condition monitoring, train door control, ticketing barriers and escalators for example?

Managing system risk

RAMSS rail engineers have a key part to play in managing cyber security risk, see Box 1. They need to ensure that the advantages delivered by new technology and networks are not outweighed by cyber risk. Engineers should know enough about cyber security issues to ask pertinent questions of system suppliers and implementers, and in turn seek expert advice if they have any doubt over the safety and reliability of a system.

As such, cyber security is becoming an ever increasing requirement for inclusion in engineering safety cases. A safety justification for a technical system should consider the impact of cyber security risk and demonstrate that safeguards are in place to control this to an acceptable level. Safety cases lacking in this area are incomplete.

Conclusion

With many rail networks across the world undergoing a transformation by introducing IP enabled systems, cyber risk has become a reality. Control systems across these rail networks are potentially exposed to cyber attack. To counter this, RAMSS rail engineers need to ensure that such systems are security risk-assessed and any weaknesses are mitigated proportionately, alongside other traditional risks. After all, who wants to be headline news in the next hacking scandal?

Contact: Anna Holloway (London)
anna.holloway@risktec.co.uk

Nigel Stanley, OpenSky,
a TÜV Rheinland company
nstanley@openskyuk.com

Functional Safety: A Proportional Approach to Legacy Safety Systems

The requirement for identification, specification and maintenance of Safety Instrumented Systems (SIS) is contained throughout legislation, with the industry-wide good practice standard being IEC 61508, Functional safety of electrical/ electronic/ programmable electronic safety related systems. SIS are specific electrical or electronic systems that prevent or mitigate the effect of a hazard.

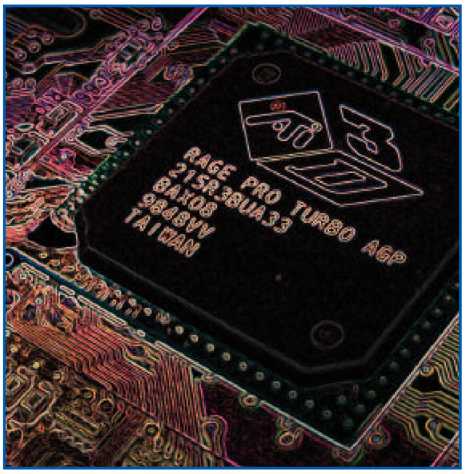
Practical problems

For sites with legacy SIS in place there is a burden of responsibility on the site operator to demonstrate these systems are being managed actively and are fit for purpose. However, there are a number of practical difficulties:

1. Requirement for quantitative or semi-quantitative assessment – previous assessments may have been qualitative only, therefore the additional data requirements and techniques involved may be unfamiliar.
2. How to assess all the relevant faults for each system? The list of potential faults leading to the hazardous event can be extensive.
3. Some requirements of IEC 61508 may be difficult and expensive to retrofit to existing systems or to demonstrate retrospectively.

A proportional approach

These difficulties may be overcome by adopting the proportional approach described in Box 1. Using this high level, order of magnitude methodology allows a result to be obtained using a relatively simple methodology. The first and second stages are applied to screen out low risk hazards, leaving only the significant risks. These are assessed using Layers of Protection Analysis (LOPA) to reveal whether the existing SIS is required to provide a Safety Integrity Level (SIL) rated safety function. The assessment can be largely based upon existing documentation and can quickly identify any weaknesses in protection.



The fifth step is a review of whether the overall risk can be regarded As Low As Reasonably Practicable (ALARP), or if there are further, or alternative safeguards that could be put in place.

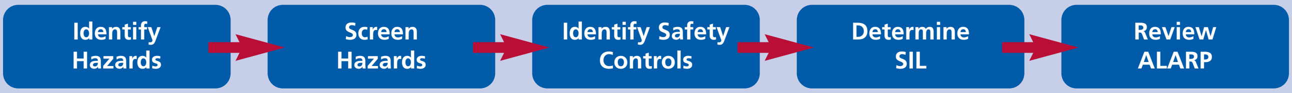
Conclusion

A high level approach is often sufficient to identify any weaknesses in legacy safety instrumented systems. Where weaknesses are identified through LOPA, applying an ALARP review can often highlight simple procedural or non-electrical/electronic engineering controls, thus avoiding unnecessarily onerous SIL requirements altogether.

Contact: Katy Skipworth (Edinburgh)
katy.skipworth@risktec.co.uk

Box 1 – Case study: Assessment of legacy plant

The client company operates sites with multiple legacy Safety Instrumented Systems (SIS) that required assessment to demonstrate that they are fit for purpose. Risktec developed a simple, high level order of magnitude assessment to determine whether these systems were required to provide a SIL rated safety function, and whether other simple, non-SIS safeguards would be more appropriate. The stages of the methodology are:


Identify Hazards → Screen Hazards → Identify Safety Controls → Determine SIL → Review ALARP

Stage 1 - Identify Hazards
A hazard identification exercise was carried out, utilising existing documentation including HAZOPs, HAZIDs, safety reports, etc.

Stage 2 – Screen Hazards
A simple risk matrix was applied to the identified hazards to assign likelihood and consequence scores. Where possible, existing hazard assessment documents were used to facilitate this stage. A screening exercise was then used to identify major accident hazards to be carried forward for further assessment. The majority of hazards were discounted at this stage.

Stage 3 - Identify Safety Controls
For each major accident hazard, all existing prevention and mitigation safety measures were identified, not just the legacy SIS. Key data were derived from existing information sources, operational procedures and site walkdowns.

Stage 4 - Determine SIL Requirement
The LOPA desktop technique was used to identify any risk shortfalls and the associated SIL requirements to address those shortfalls. This also identified the reliability and integrity requirements of the legacy SIS.

Stage 5 – Review ALARP
Each shortfall was reviewed using a 'Hierarchy of Protection' strategy to identify additional risk reduction measures to be implemented. This avoided the use of a complex SIL-rated system in favour of a more appropriate or simpler technology option.

UK Principal Office
Wilderspool Park
Greenall's Avenue
Warrington WA4 6HL
United Kingdom
Tel +44 (0)1925 611200
Fax +44 (0)1925 611232

Europe
Aberdeen
Alderley Edge
Ashford
Bristol
Crawley
Derby
Edinburgh
Glasgow
London
The Hague

Middle East
Abu Dhabi
Dubai
Muscat

North America
Calgary
Houston (South East)
Houston (Energy Corridor)

For further information, including office contact details, visit:
risktec.com
or email:
enquiries@risktec.com

6