RISKworld

issue 15 spring 2009 the newsletter of risktec solutions limited

In This Issue

Welcome to Issue 15 of RISKworld, which focuses on practical risk management. 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 suggestions you may have for future editions.

Contact Steve Lewis (Warrington)

Contents

Practical risk management
Alan Hoy comments on the potential effects of the global recession, and advocates a practical approach to risk management.

Rough guide to hydrogen sulphide
Martin Fairclough introduces us to the hazards and challenges of sour gas.

The human condition
It's all too easy to blame the operator when things go wrong. Craig Foley takes a look at why the truth is more interesting.

Risk-based fire protection
Greg Moore examines the benefits of using a risk-based approach for fire protection rather than simply designing to code.

Why is software different?
Why is making a safety justification for software any different to hardware? Kevin Charnock reveals all.

Risk management overkill
With increased oversight in today's 'interesting' times, is there a danger of overdoing risk management? Simon Burtonshaw-Gunn investigates.

Risktec

Practical Risk Management

All clients contacted in our annual client satisfaction survey said they would recommend Risktec to other companies

This edition of RISKworld is published at a time when the world is facing enormous economic challenges and is still coming to terms with historical decisions which, with the benefit of hindsight, are seen as major failings. Blame is rife, inquiries are common and company and personal reputations are under intense scrutiny. There are many lessons to be learned from the past, but the main one is that the risks of the future must be better identified, assessed and managed.

Arguably there has never been a more important time for risk management to help make informed decisions. In the current climate people have become more accustomed to 'thinking the unthinkable' but it remains important that companies and organisations take account of the full spectrum of risks they face.

The Baker report into the Texas City refinery explosion indicated that many companies were focusing on workplace risks at the expense of process risks with potentially catastrophic consequences. Conversely, it is clearly important that the current economic climate doesn't result in a bias towards major risks at the expense of more frequent but nevertheless significant risks.

At Risktec we continue to advocate a practical and cost-effective approach to risk identification and management, utilising a range of qualitative and quantitative techniques, tailored for the specific project.

We also aim to 'practice what we preach' and manage the risks to our business by employing high quality and experienced people to provide a wide range of services to numerous clients in diverse market sectors. Risktec now employs over 100 people and gets further support from a large and established base of associates.

For further information, contact Alan Hoy (Warrington).

A Rough Guide to Hydrogen Sulphide

Around one-third of the world's gas fields contain 'sour gas', contaminated by sulphur compounds including hydrogen sulphide, also known as H_2S. This gas is one of the most deadly hazards in the industry, making the fields more difficult to develop.

As the fields with low levels of contaminants become depleted, the industry has looked to exploit formations of sour gas to meet the demand of the world's growing energy needs. The end result is 'sweet gas', profitably extracted and processed in accordance with increasingly stringent health, safety and environmental requirements.

Safe production from sour gas fields is not new – there are numerous existing facilities such as those in the foothills of the Rocky Mountains of Alberta, Canada, that have many years of safe operation. However, some of the world's largest new projects are developing sour gas reservoirs, such as those in the north east corner of the Caspian Sea and in the deserts of Oman, and they are applying increasingly effective design strategies and technologies to manage the risks.

H_2S hazards

You can detect the presence of H_2S at less than 1 part per million (ppm) – it is easily recognised by its characteristic foul odour similar to rotten eggs. Unfortunately, it may be the last thing you ever smell. If the concentration of the gas is above 100 ppm the sense of smell is quickly deadened, giving a false sense of security that the danger has passed. Concentrations above 500 ppm can lead to breathing difficulties and confusion, and above 700 ppm immediate unconsciousness. 1000 ppm will lead to death unless rescued promptly [see Box 1].

Box 1 – Clear and present danger

Late in the night of 23rd December 2003, a gas-well blowout near the city of Chongqing in central China released a deadly mixture of natural gas and hydrogen sulphide. The toxic cloud killed 243 people (only 2 were site workers), hospitalized more than 9,000 and required the evacuation of more than 64,000 nearby residents.

A government report concluded that the drillers improperly dismantled blowout prevention equipment, misjudged the amount of gas in the well and failed to spot the blowout. The crew failed to immediately ignite the gas as it began to escape, which would have prevented the toxic cloud from spreading [Ref. 1].

H_2S creates another problem – it causes iron to corrode and equipment such as valves and flow lines to malfunction and leak [see Fig 1]. So not only are the effects of an inadvertent release of H_2S far more harmful than conventional gas, H_2S itself makes a leak more likely.

Figure 1 – Signs of hydrogen sulphide corrosion include shallow round pits with etched bottoms

Controlling the H_2S risk

Managing H_2S safely requires design barriers that serve to prevent releases and alert workers should a leak occur, and operational barriers that limit their potential exposure. A selection of design and operational strategies for reducing the risks associated with H_2S are shown in Box 2.

Box 2 – Design and operational strategies for reducing H_2S risks

- Extract H_2S from gas streams
- Use of corrosion resistant materials
- Minimise number of leak paths (simplify the process, reduce instrument tappings, etc.)
- Optimise risk-based asset inspection
- Rapid detection and facility-wide alarm system
- Minimise personnel manning in H_2S areas
- Protection of personnel in transit between work-sites and safe areas
- Larger separation of process trains
- Maintenance of equipment only when shutdown and purged
- Respiratory protective equipment, e.g. self-contained breathing apparatus (SCBA) and fixed air-line systems
- Sheltering provisions in safe locations
- Protected rescue teams
- Reduce concurrent production and construction activities (SIMOPs)

To enclose or not to enclose?

It is common practice in the oil and gas industry for hydrocarbon processing facilities to be situated in the open, exposed to the natural elements. There are some significant safety benefits to this strategy. For example, any gas release may be naturally diluted to below toxic levels or to below the level where it could result in an explosion.

However, many new projects for sour gas fields are also in an extremely cold or hot climate, or both. Some of these projects are considering enclosing the process plant to realise significant operational and maintenance benefits, e.g. easier and faster working for personnel, and less wear and tear of the equipment from the weather. Such enclosures could be heavily engineered modules like those on some offshore platforms.

From a safety perspective, the issue is not clear cut. At first glance it would appear that workers inside an enclosure would be more readily exposed to H_2S should a leak occur, i.e. the gas can't dilute in the open air to below fatal levels. But there are ways of overcoming this, for instance a high specification ventilation system and vent stacks to safely extract and disperse the gas, a requirement for workers to only enter the enclosure when wearing breathing apparatus [see Fig 2], or only allowing maintenance of equipment when plant is shutdown and the gas removed.

Figure 2 – High specification SCBA face mask

Furthermore, a major safety benefit of enclosing the plant is that, with good vent stack design, workers outside of the enclosure would not be exposed at all to any releases inside the enclosures, unlike open plant where all workers downwind of a release could be affected.

There are other safety issues to consider, such as fire and explosion protection, but the industry is tackling every issue head-on to ensure that all risks are reduced and controlled to acceptable levels.

Conclusions

The search for new oil and gas is increasingly requiring the development of sour gas fields. Effective risk management strategies are required to prevent leaks of H_2S and protect workers and the public from its lethal effects. The industry faces many technical challenges, but is rising to meet them with innovative design solutions and new technologies.

For further information, contact Martin Fairclough (Warrington)

References

1. United Nations Environment Programme: [www.unep.fr/scp/sp/disaster/casestudies/china/gaoqiao.htm]

Practical Human Factors: Recognising the Human Condition

The Chernobyl disaster was initially blamed on operator error, before a host of contributing factors, including design flaws, were identified

The human condition

Whilst the aphorism 'To err is human' may well be a truth of the human condition, it is important to recognise that human errors vary in type and likelihood. Since both of these variables are, in principle, predictable, the capacity for human error can also be characterised and managed. For example, the probability of human error is closely related to the complexity of a task, the time available, the usability of equipment, the quality of training and procedures, and the prevailing environmental conditions.

As the architecture of safety related systems changes, so do the demands placed on the human operators that support system safety.

Box 1 – Milford Haven Explosion 1994 Contributing Factors [Ref 1]

- A control valve was shut when the system indicated it was open
- Maintenance of plant and instrumentation was inadequate
- A modification was performed without appropriate assessment of its consequences
- Control panel graphics did not provide necessary process overviews
- Attempts were made to keep the unit operating when it should have been shut down
- Excessive number of alarms in emergency situation
- Concurrent production and construction activities (SIMOPs)

For example, an operator's role may be primarily passive, monitoring changes in system state, and confirming automatic actuation of systems.

Or perhaps the operator is a 'man-in-the-loop' controller, performing actions to control a plant or process, or initiate protective systems.

In most cases the role of the operator will be to support a number of safety related systems, each with differing demands. Clearly then, system safety can be heavily dependent on human factors such as the quality of the plant interfaces used by the operators, and the clarity and user-friendliness of operating and maintenance procedures.

Accidents and operators

Investigation of accidents across disparate industry sectors, such as Three Mile Island, Chernobyl, Ladbroke Grove, Milford Haven [see Box 1] and more recently the Buncefield Oil Storage Depot explosion, add weight to the view that the root cause is rarely as simple as the front line operator.

In a UK HSE study [Ref 2], 34 accidents and incidents due to control system failures were investigated to identify the primary cause and attribute it to a safety lifecycle phase. Only 15% related to the operations and maintenance phase, with more than 60% of failures classed as built into the safety related systems before taken into service. Hence it seems that designers, safety assessors and managers are only human too!

Human factors

The discipline of human factors (also called ergonomics) concerns itself with answering the following questions:

- What are people being asked to do (the job and its characteristics)?
- Who is doing it (the individual and their competence)?
- Where are they working (the organisation and its attributes)?

These issues are more wide ranging than those relating specifically to an operator's role as monitor or controller in the architecture of safety systems, and cover the whole lifecycle. For example, competence clearly applies to those involved in specification, design, manufacture, commissioning, training, operations and maintenance.

The man in the machine

In working to prevent human error, it is essential to keep in mind how important people are to safety. They are proactive and can solve problems; they can make systems and facilities more robust and are irreplaceable in many situations. Unlike automatic safety systems people can learn. With a human as part of the system, the system has the potential to improve.

Active participation of operators in the design, assessment, management and ongoing improvement of safety-related systems should be an essential ingredient towards creating safer working conditions.

Human errors are inevitable – but perhaps Prof. James Reason put it best when he said:

"We cannot change the human condition, but we can change the conditions under which people work."

Contact Craig Foley (Warrington) for further information.

References

1. Health & Safety Executive (1997), The explosion and fires at the Texaco Refinery, Milford Haven, 24th July 1994.
2. Health & Safety Executive (2003), Out of Control: Why control systems go wrong and how to prevent failure (2nd edition).

Practical Fire Protection – A Risk-based Approach

The International Association of Oil and Gas Producers (OGP) recently published a guide to help organizations reduce major incident risks by focusing on asset integrity management [Ref 1]. Derived from good practices in mature regions where operators are required to provide structured evidence of sound risk management practices, the guide applies to new and existing assets at all lifecycle stages.

The guide emphasizes the importance of barriers (safeguards or controls) in minimizing the residual risk so far as reasonably practicable. Recognizing that no barrier is infallible, multiple plant and human intervention barriers are put in place to prevent the occurrence of a significant incident. The bow-tie diagram is arguably the best way of illustrating how barriers prevent a hazardous event (the left hand side) and how they mitigate the potential for the event to escalate to the worst case consequences (the right hand side) [see Fig 1].

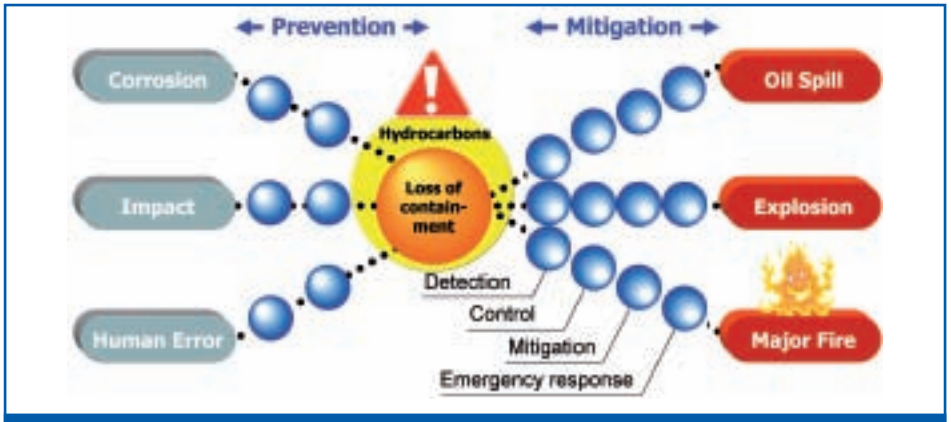


Figure 1 – The 'bow-tie' diagram and the role of fire protection barriers in preventing escalation to a major fire

Fire protection barriers

Much design effort is quite rightly focused on prevention – it is better to reduce the inventory of hazardous materials or reliably maintain the integrity of the containment than deal with the consequences of a release. Nevertheless, fire protection barriers have a very important role in preventing and limiting escalation [see Box 1].

Box 1 – Fire protection barriers

Ignition prevention via hazardous area classification, provision of suitable equipment, control of other sources of ignition and specification of non-flammable materials

Fire and gas detection systems, using flame, heat, smoke and gas detectors to initiate control systems such as emergency shutdown systems (ESD), depressurization systems (blowdown) and activate fire suppression systems

Fire suppression systems, including fire pumps, water deluge, foam systems, sprinklers and fixed extinguishing systems (e.g. dry powder)

Passive fire protection, including hazard separation, structural fireproofing coats, building construction types, heating and ventilation systems

Fire-fighting emergency response, including on-site and off-site fire teams

Designing to codes and standards

Fire protection systems are traditionally designed to well known codes and standards, such as the International Building, Fire & Mechanical (ICC) codes, the NFPA codes, and the API fire standards, coupled with sound engineering practice. This approach works very well where there is nothing new or unusual about the design and the risks are well understood. However, where the design is more novel or challenging, and costs and uncertainty are higher, then the approach is best supplemented by risk-based insights to help avoid over- or under-design.

Risk-based approach and performance standards

Risk assessment leads to an understanding of the magnitude of fire effects, their likely frequency of occurrence, and the effectiveness of the fire protection barriers in reducing risk. This also leads to the operational performance required for the barriers to meet their intended risk reduction function. High level performance standards are set for each barrier, with more detailed performance standards for constituent parts as appropriate.

Performance standards for barriers are typically described in terms of functionality, availability, reliability and survivability. They thus determine equipment design specifications and also set requirements for maintenance and testing throughout the asset's lifecycle.

This risk-based approach typically considers a range of possible performance standards for each component – based on recognized design standards – and then optimizes the overall barrier and combined barriers to give the most cost-effective risk reduction.

For example, options to provide increased protection include active fire protection with high installation and maintenance costs but high risk reduction, and passive fire protection with lower costs but shorter lifespan and less risk reduction.

Once performance standards are defined, assurance processes need to be put in place to confirm that barriers remain fit for purpose [see Box 2].

Box 2 – Typical assurance processes

- Initial testing and commissioning performance tests
- Operational controls and limits
- Maintenance, inspection and testing plans
- Performance records (components and whole system)
- Audit and review

When is fire risk low enough?

The critical step in deciding when risk has been reduced low enough is to identify a wide range of possible risk reduction measures. Tools are available to help assess the risk, such as barrier analysis, layers of protection analysis (LOPA) and quantitative risk assessment (QRA). In practice any decision amounts to taking a balanced view and reaching a defensible consensus. A convincing justification lies in the documented consideration of risk reduction options, both implemented and discounted, at a level of resolution appropriate to the stage of the facility lifecycle and magnitude of risk.

Conclusion

Major fires can have severe consequences for people, the environment, assets and company reputation. The oil & gas industry has been relatively successful in managing these risks, but some high profile major incidents in recent years indicate that the challenge remains. Risk-based fire protection is a powerful but cost-effective way of meeting this challenge.

Contact Greg Moore (Houston) for further information.

An Introduction to Safety-Critical Software

Why Software is Different

Software is often used to implement the functionality of safety systems because it can be designed to handle complex functionality, is accurate and repeatable, and can be cheaper than hardware solutions. However, there are many examples of safety systems which have failed due to software related faults, a small sample of which are presented in Box 1.

Box 1 - Examples of software system failure

Therac-25 (1985 to 1987)
Therac-25 radiation therapy machines delivered radiation overdoses to a number of patients in Canada and the USA which resulted in three fatalities. Most of the Therac-25 safety interlocks were software based, which replaced hardware interlocks that had operated without any recorded patient injuries on earlier versions of these machines.

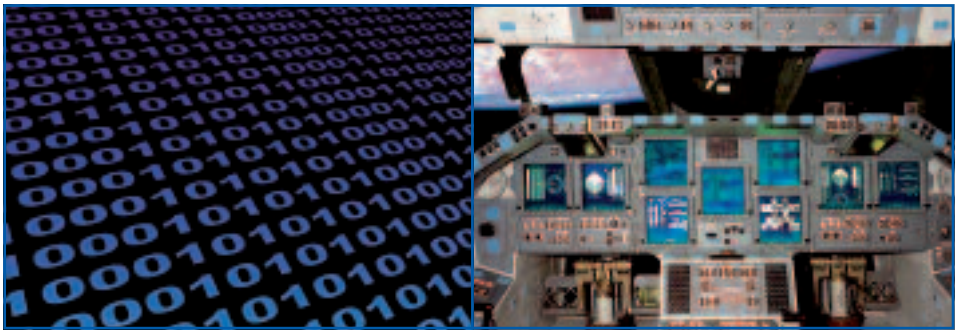
Ariane 5 (1996)
The unmanned Ariane 5 European spacecraft was destroyed less than a minute after launch on its maiden flight, due to a fault with software previously used successfully on earlier versions of the launcher.

Mars Climate Orbiter (1999)
A mismatch between Imperial and SI units on the NASA Mars Climate Orbiter resulted in loss of the spacecraft when it entered the Martian atmosphere too low and too fast.

UK Inland Revenue (2004)
Software errors in the UK Inland Revenue tax credit payment system contributed to a $3.54 billion tax credit overpayment.

How software fails

The failure of a safety system based entirely on "hardwired technology" tends to be dominated by so called random failures, which are typically age or wear related, as opposed to software based systems, which fail predominantly due to systematic errors. This distinction arises because systematic errors can often be identified and removed from a hardwired design, whereas this can be much more difficult with software due to a greater level of design complexity and its abstract nature. Moreover, software does not wear out and so does not fail randomly in the same sense as hardware (although the platform upon which the software runs will be subject to random failure mechanisms).



The factors that can lead to a software error, which if triggered can cause a system level failure, are peculiar to systematic errors, both in terms of their introduction and detection [see Box 2].

Box 2 – Typical factors in software failure

- Poor communication among software developers and end users
- Lack of operational or safety experience in programmers
- Use of inappropriate programming language
- Unwanted functionality supplied as part of commercial-off-the-shelf software
- Inadvertent change to safety functionality during software modification
- Unrepresentative software testing
- Inability to fully test all logic paths due to complexity and number of variables (e.g. timing of inputs)
- High frequency of software updates which may adversely affect safety function

Safety assurance processes

The uniqueness and complexity of software-based safety systems means that there can be a huge array of factors influencing the success or failure of such developments. Fortunately, there are some steps which are generally effective at reducing the risks associated with developing software safety systems.

These steps revolve around safety assurance, i.e. the planning, development, verification and configuration management processes that ensure the software meets its safety objectives. Key steps include:

- Explicitly identify all safety functional and integrity requirements before commencing the software design phase, as mistakes or omissions will be more difficult and expensive to rectify the later they are discovered and significant software modifications can be a major cause of systematic error.
- Identify at the outset the means of generating the evidence to show that each safety requirement has been met, to inform the design process, ensuring that the necessary evidence is produced as the software is developed (since retrospective generation is usually very expensive).
- Confirm the availability of safety assurance evidence when considering integrating previously developed software components, in order to reduce cost and project risk.
- Minimise the number of personnel developing the software system and ensure all interfaces are well defined. Increasing the number of personnel in order to shorten the development timescale will increase the number of interfaces, potentially leading to a greater number of errors.
- Consider the adequacy of generic safety assurance evidence for commercial off-the-shelf components (e.g. electrical protection relays, PLC shutdown systems) in the context of the safety system within which it will be deployed, since for example a system failure causing a valve to close could be safe in one system but may result in a disastrous over-pressurisation event in another.

Conclusion

Identifying software errors in safety systems is not easy, but the application of targeted safety assurance processes should help manage the associated risks to an acceptable level.

For further information, contact Kevin Charnock (Warrington).

Risk Management Overkill

The Hidden Risk for Major Projects

There is an ancient Chinese saying "may you live in interesting times". While purporting to be a blessing, this proverb was originally used as a curse. A high proportion of industrial, commercial and financial sectors across the globe would probably agree. For many, if not all, these times are much too "interesting", not to mention challenging and uncertain, regardless of company reputation, track record or order book size. Now more than ever, with capped resources, limited funding and volatile markets, there is a growing emphasis on risk and financial management, particularly for major capital projects, at all stages of the project life cycle.

Balance of risk

The balance between a willingness to take risks for business purposes and the degree of risk control imposed can strongly influence a project's chances of success, as illustrated by Figure 1. Ideally, the degree of risk control should be proportional to the level of risk exposure. This may take the form of corporate governance, formal risk reviews, and defined project hold points or "toll-gates", for example.

For major capital projects, where there are invariably a number of major parties involved, it can be challenging to agree on the appropriate level of risk control. This can be particularly difficult in times of rapid change or uncertainty, such as those we are experiencing today, where:

- The availability of project finance is severely constrained
- Design & construction costs are falling
- Supply chain businesses are failing
- Commodity prices are volatile

Each party involved in a project may have a different perspective on these areas of uncertainty.

Bad reaction to risk

With this kind of uncertainty, there is a natural tendency to increase the level of risk control and introduce more risk-averse criteria. While this is understandable, there is the potential to overcompensate, which could threaten project viability or introduce unnecessary costs.

The discipline of project risk management is well understood and documented (see inset for example) and much has been written about the pitfalls of leaving risks unidentified and unmanaged. What is less-well documented is the potential for overzealous risk management to suffocate or even terminate projects, a situation that can only be exacerbated in the current credit crisis.

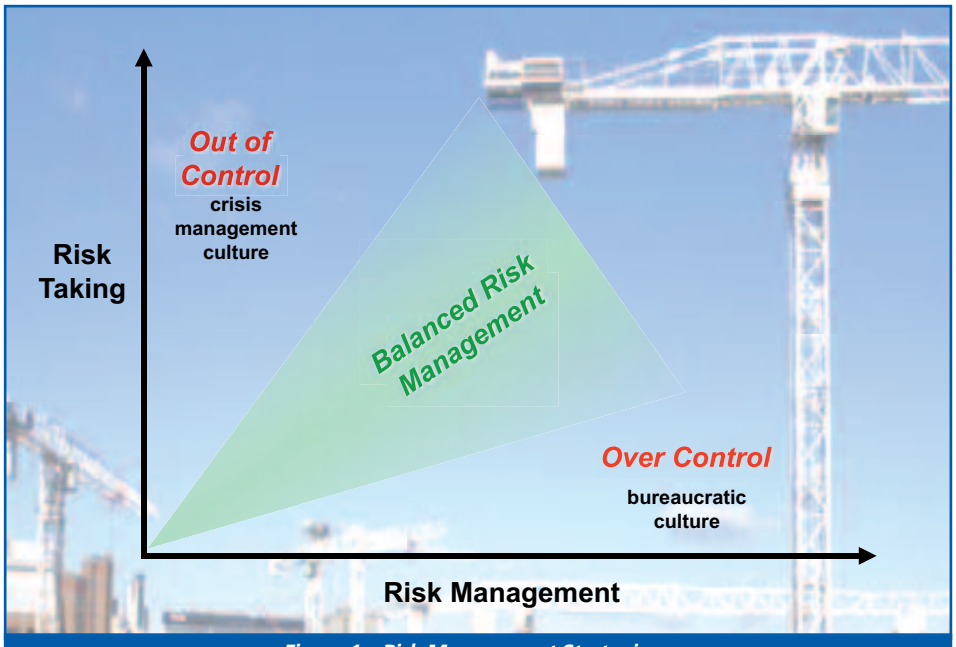


Figure 1 – Risk Management Strategies

Written by Professor Simon Burtonshaw-Gunn of Risktec, *Risk and Financial Management in Construction* aims to assist both practicing project managers and those studying risk and financial management as part of their wider professional studies. This visually powerful reference makes much use of models, charts, tables and figures, including Gantt charts, work breakdown structures, and risk matrices.

A sense of proportion

To counter this, the aim should be to manage risks efficiently and effectively, for example by:

- Actively engaging with major project 'players'
- Systematically identifying risks and assessing them
- Integrating practical risk management controls into day-to-day activities
- Focusing on tangible actions that actually reduce risk
- Imposing a level of scrutiny that is proportional to risk

While this may imply an overhaul of existing arrangements, the emphasis should be on value for money rather than paperwork.

For further information, contact Simon Burtonshaw-Gunn (Warrington).

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

Other UK Offices
Aberdeen
Ashford
Edinburgh
Glasgow
London

Middle East
Dubai
Muscat

North America
Calgary
Houston

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