Issue 33 / Spring 2018

RISKworld

The Newsletter of Risktec Solutions

In this issue

Welcome to Issue 33 of RISKworld. Feel free to pass it on 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
steve.lewis@risktec.tuv.com

Contents

Long-term thinking is key

Image courtesy of Stefan Wernli

Someone is sitting in the shade today because someone planted a tree a long time ago – Warren Buffett

A strong client focus has always been a core value at Risktec and was the highest scoring area in our recent employee survey, underlining its importance to us all. We are therefore very pleased that the results from our latest bi-annual client satisfaction survey show that we continue to perform very well in this area: 97% of clients are satisfied with the service they received and 100% of clients would use us again and would recommend us.

So far this year, we have seen an increase in confidence in most of our markets, especially in the recovering oil and gas sector, with greater demand from clients for our services. Our strategy of taking the long-term view during difficult market conditions and maintaining a strong team means we are well positioned to meet the needs of our clients.

Broadening our service portfolio to reflect client demands is a key strategic objective. A recent example of this is vendor inspection, where purchased equipment is inspected at the manufacturing site to detect any technical issues prior to delivery (page 6). Vendor inspection is an important 'building block' of our asset integrity management offering, as are risk-based inspection (page 2) and reliability, availability and maintainability modelling (page 4).

With the seemingly relentless advances in digital applications it is no surprise that digitalisation is a key strategic area where we are helping clients. Digitalisation provides opportunities to make things more user friendly and accessible, such as safety cases (page 8), but also introduces new challenges which must be managed, like the adoption of commercial off-the-shelf wireless communication for safety-related systems (page 10).

As always we welcome your feedback on this edition and look forward to your continued support.

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

Inspection optimisation: Going beyond risk-based inspection

When was the last time you analysed your risk-based inspection (RBI) strategy? Have you ever asked, "Why are we doing it this way?" and has someone responded, "Because that's the way we've always done it"? If the answer to either of those questions is yes, it may be time for a change.

RISK-BASED INSPECTION (RBI)

At processing facilities, RBI is a risk assessment and management process that focuses on loss of containment of pressurised equipment due to material deterioration. RBI complements process HAZOP studies by focusing on physical integrity-related damage mechanisms and managing risk through methods, coverage and frequency of inspections.

API RP 580 (Ref. 1) provides guidance for developing RBI programmes and API RP 581 (Ref. 2) sets out methods for the calculation of risk by combining the probability of failure with its consequence. This provides the basis for making informed decisions on what to inspect, the inspection frequency, the extent of inspection and the most suitable type of non-destructive testing (NDT). In this way, inspection efforts target the process equipment with the highest risk.

GOING BEYOND RBI

Technological advances in non-intrusive inspection (NII) techniques, where inspections are performed from the outside of the vessel without breaking containment, and the use of robotic equipment for internal inspection, can both realise significant benefits:

- NII significantly reduces turnaround time, leading to greater production availability, because there is no need to shut down a vessel, isolate it and prepare it for entry.
- NII, in conjunction with robotics, can eliminate the occupational safety risks associated with confined space entry.

Improvements such as these can be achieved by going beyond the standard RBI approach and minimising interventions by applying a simple process called inspection optimisation strategy (IOS).

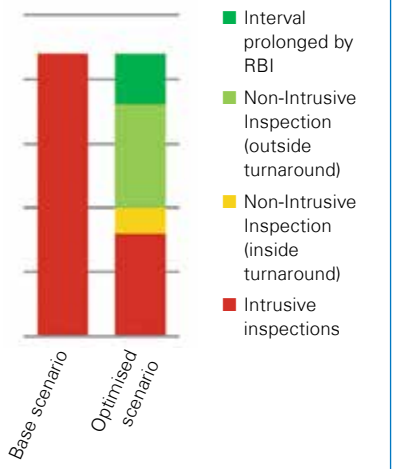
WHAT IS IOS?

The IOS process is a structured, experience-based way of identifying opportunities to mature an asset's RBI strategies and is typically conducted in four steps.

Step 1 – RBI quality review: Using a team comprising individuals experienced in RBI and inspection methods, as well as other subject matter experts, the quality of results from recent rounds of RBIs are reviewed to screen opportunities for extending inspection intervals or changing the scope of the next turnaround.

This is important, as most facilities' RBI programmes are a well run routine process. Inspections are planned, NDT contractors hired, preparations made, inspections conducted and results returned to the company, often without critical owner review. Unless there is an outlier, the information is entered and stored, and the inspection rescheduled according to the original RBI strategy. This means that opportunities for optimisation may be missed.

Figure 1 - Inspection optimisation



Step 2 – Scope optimisation: Next, the team optimises the RBI programme by reducing the scope (amount) of work during the turnaround. This can be achieved by changing from intrusive inspection to NII or remote inspection (robotics),

or prolonging the inspection interval without compromising integrity. With improved confidence in the quality of the data obtained during the previous step, the facility is in a better position to make this distinction. Analysis by experienced reliability engineers, in-house or external, can support the decision to delay an inspection.

Step 3 – Non-intrusive inspection: For vessels, the team should determine if the inspection can be replaced with a NII technique based on knowledge of the potential damage, equipment design and operational parameters. Typically only 5% of the cost of a vessel inspection is for the inspection itself. The remainder of the cost is associated with taking the vessel out of service, preparing it for inspection and placing it back in service. NII removes most of this work from the scope. Where this is an option, the RBI strategy should be modified and the inspection schedule adjusted to reflect the ability to inspect equipment while in-service.

Step 4 – Robotic inspections: Where NII is not a possibility, the team should investigate whether there is the ability to use robots to perform the internal inspections. Choosing robotic inspection eliminates the requirement to prepare equipment for human confined space entry. Not only is this safer, but it can also reduce the number of hours of overall downtime to prepare and conduct the inspection.

Step 5 – Future strategy: The new, optimised scenario is illustrated in Figure 1. It is crucial that the results from the new inspections are themselves reviewed to confirm that the data collected was of sufficient quality and quantity to make an informed decision on the future RBI strategy.

CONCLUSION

Applying the IOS concept for one company realised turnaround scope and cost savings of at least 10%, and up to 50% per asset, the extent depending on the maturity of the RBI strategies in place at the asset. So, the next time you ask, "Why are we doing it this way?" perhaps it's worth a look at the IOS approach.

Contact: Kris Smith
kris.smith@risktec.tuv.com

References:
1. API RP 580, Risk Based Inspection, 2016.
2. API RP 581, Risk Based Inspection Methodology, 2016.

The power of RAM modelling: Optimising facility performance throughout life

Projects in the energy industry often involve the design and build of complex facilities, necessitating upfront capital investment and ongoing operational expenditure. Decisions made during design can carry considerable risk, both in terms of future profitability as well as the impact that incidents may have on health, safety and the environment.

To assist, there are a range of assessment tools and methods available which broadly fall into two categories:

- Production assurance to optimise facility operations and output.
- Risk management to ensure that risks are known and sufficiently managed.

Both must be considered as part of an iterative process to arrive at a balanced solution.

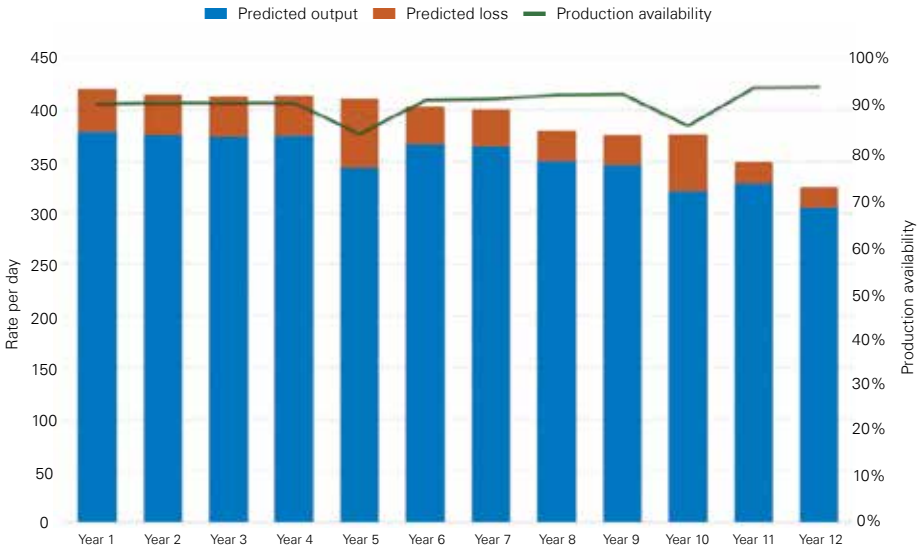


Figure 1 – Typical production profile

WHAT IS PRODUCTION ASSURANCE?

Production assurance activities are those undertaken to achieve and maintain asset performance at its optimum. These activities could be to ensure a system operates at its maximum potential for as much time as possible, or to reliably deliver a product to a customer at a contractually agreed volume and time.

One measure of production assurance, production availability, is calculated by applying the basic techniques of a reliability, availability and maintainability (RAM) study. The critical components and their failure modes are identified (e.g. via failure modes & effects analysis) and a reliability block diagram is developed, building in failure rates and repair times. The design flow rates or relative capacity are also included in the model to assess how failures affect throughput. In this way, the RAM study is no longer limited to determining system 'up' or 'down' time, instead it enables evaluation of the multiple levels of output from a system, from nil to full capacity.

Understanding the varying output from a facility, along with the predicted duration for which the output can be achieved, allows a realistic estimate to be made of the revenue that can be returned over the facility lifetime.

Consider a simple oil and gas production system that consists of two pumps, each required to operate at full capacity to accommodate the input and maximise output. If the simulation predicts failure of a pump in the first year, then the production rate through the system will temporarily halve for a period until the pump is fixed and reinstated. Eventual repair of the faulty pump may have a further impact on production unless it coincides with a planned maintenance outage. The reduction from full capacity in this case represents lost throughput and lost revenue.

MANAGING COMPLEXITY

Extending this concept to the many equipment items that make up a facility, each with their individual capacity, reliability, maintenance and repair strategy, sparing philosophy, delivery times, and ageing mechanisms, creates a relatively complex problem – which is where RAM modelling software can help. Such tools can simulate the varying effect of equipment failures over hundreds of facility lifetimes to provide a statistically relevant prediction of facility throughput.

Figure 1 illustrates a typical production profile for a facility over its lifetime, taking into account the effect of the many variables on overall production. With such a facility model the financial benefits of design and operational enhancement options can be compared with the baseline case. Crucially, the simulation can be used to identify the main bottlenecks to production to help formulate a targeted improvement plan.

A wide range of what-if questions can be considered, such as, "How will another production train affect productivity?" or, "Is it worthwhile holding spare parts in stock to alleviate major bottlenecks?" Once the facility model has been developed, these questions can be answered very quickly with a simple re-run of the simulation.

Such studies can be used to assess the output from any system: be it the lost generation revenue from wind turbine failures, or loss of throughput from a batch manufacturing plant.

CONSIDERING RISK

The method brings clear benefits to production optimisation, but any proposed improvements must also be assessed to determine the impact on risk. For example, more frequent planned maintenance will improve reliability, but will also elevate personnel exposure to hazards. Similarly, adding another live production train will increase the likelihood of a loss of containment, with a commensurate increase in risk levels.

Production assurance and risk assessment often have competing targets, and having the ability to quickly assess proposed changes using both types of study will assist in achieving a balanced solution. In this respect, an iterative process is clearly preferable, with close working between the reliability engineer and the risk assessor.

CONCLUSION

Optimising the resilience of an asset to achieve a strong through-life performance is key to meeting market requirements, achieving customer satisfaction, and building a positive reputation in the long-term. To this end, the traditional RAM study can be extended to assess the expected performance from a complex facility during its lifetime, enabling rapid comparison of design and operational options. When undertaken in tandem with risk analysis, this approach ensures that lifetime performance is optimal and in balance with the associated risks to health, safety and the environment.

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

Precisely right: An introduction to vendor inspection

Procuring new equipment for a large industrial project such as an oil, gas or petrochemical facility inevitably involves a complex supply chain. Manufacturers of equipment like valves, pumps, piping and control systems can be located across many countries and even continents. So what is the most cost-effective way to confirm product quality and compliance with specifications?

Whether the equipment is being bought directly by the operator of the facility or via the engineering contractor, what is required is for it to be delivered to site on-time, to the specified quality and safety performance, while complying with all relevant local and international standards.

It is therefore no surprise that such equipment procurement needs to be managed in a way that minimises both project and operational risk. This is where vendor inspection steps in to help.

WHAT IS VENDOR INSPECTION?

Vendor inspection is used by operators and contractors when purchasing equipment either for a new capital project, which involves buying a lot of equipment, or for maintenance and upgrades of an operational facility where fewer items are required.

Vendor inspection of the equipment can take place along the whole supply chain:

- During the manufacturing process
- Prior to the equipment leaving the manufacturing site ('pre-shipment')
- On arrival at the final site ('post-shipment')
- After installation

Clearly, the earlier the inspection is carried out the greater the opportunity to correct any faults and avoid unnecessary re-work costs and delays.

WHAT IS ACTUALLY INSPECTED?

As there is no statutory requirement to carry out vendor inspection, it is the purchaser who sets the level of the inspection depending upon their strategies for quality and risk control. On occasion, a bank may stipulate that vendor inspection is necessary to meet funding conditions. The requirements are normally captured in the purchaser's quality plan or inspection and test plan (ITP).

Ideally, vendor inspection would cover full inspection of all equipment at the manufacturing site. For a valve, as an example, this might include inspection of the casting, material checks, witnessing of the pressure tests and functional tests, dimensional checks, and review of the painting, packing and shipping arrangements.

Some purchasers will take a risk-based approach to determining what inspections they require, whilst others will request the expertise of an experienced third-party inspection company to advise them of the scope. Operators who are using risk-based inspection (RBI) to optimise inspection schedules for their operational assets will normally take a risk-based approach to procurement as well.

However, some purchasers will simply opt for a final inspection and hope that this will ensure that the equipment will be correct. Others may not undertake any inspection at all, thus saving the cost of inspection, but tacitly living with the downstream operational risk.

Image © TÜV Rheinland

The extent of implementation of vendor inspection across high hazard sectors varies, although most of the larger international operators in the oil and gas sector do have such programmes. There is some vendor inspection in the power, energy and transportation sectors and it is starting to become more prevalent in renewables. On occasion it is found in the chemical and pharmaceutical sectors.

HOW IS THE INSPECTION CARRIED OUT?

Whatever inspection technique is used – visual, witnessing of tests, measurement, etc. – an inspector needs to be present at the manufacturing site, often at short notice. A large capital project might have equipment suppliers located all around the world, which is why most purchasers will use one of the leading, global suppliers of vendor inspection. They will have inspectors in most countries, usually close to suppliers, and the best will have a software system to enable the efficient allocation and coordination of competent inspectors for the inspection assignments.

WHAT ARE THE BENEFITS?

Vendor inspection aims to identify any technical issues prior to the equipment arriving on site. If the equipment arrives and is outside the original specification it can have a significant impact in terms of delay to the construction schedule or shutdown period, and can also have negative safety and environmental implications, ultimately disrupting production output.

The main benefits of vendor inspection may be summarised as:

- Full transparency of the quality of procured equipment
- Documentation of the quality of goods and manufacturing processes
- Confidence in vendor and subcontractor compliance with applicable standards
- Improved reliability and competitiveness by identifying bottlenecks and weaknesses in the supply chain
- Early action to avoid delays and increased project costs

CONCLUSION

The most cost-effective way to confirm product quality and compliance with specifications is to conduct inspections at the site of manufacture. Inspectors verify that the equipment ordered complies with the specification and expectations of the purchaser, taking into consideration industry standards and regulations. A risk-based vendor inspection programme can focus inspections where they are most needed to help mitigate cost, schedule, safety, environment, production and regulatory risks.

Contact: Martin Coles
martin.coles@risktec.tuv.com

E-Safety Cases: More than just a good idea?

The electronic safety case concept has been around for a long time but has struggled to gain widespread traction, perhaps because of its perceived complexity and the implied need for bespoke software. Today, however, e-safety cases can be produced using simple software found on most computers, in ways that make safety information more accessible and engaging.

Figure 1
E-safety case homepage for an offshore windfarm

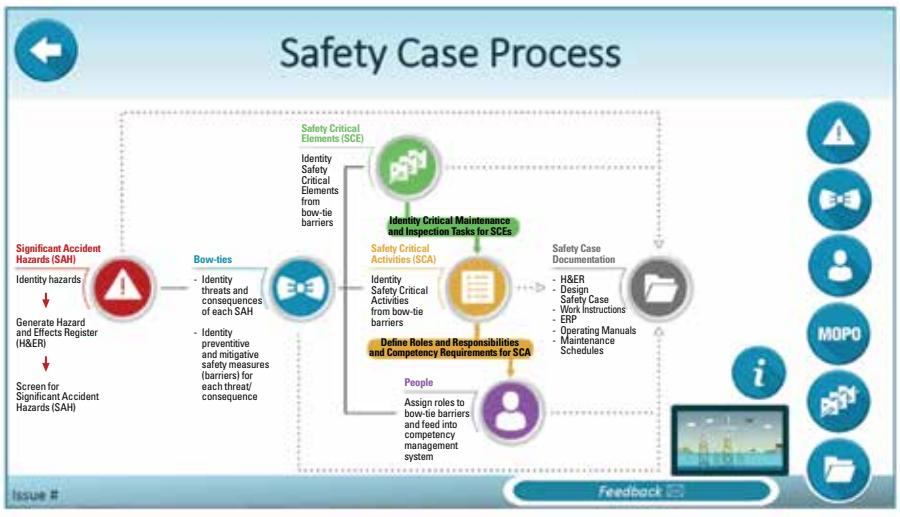


Figure 2
Safety case process

WHAT IS AN E-SAFETY CASE?

The idea behind an e-safety case is to provide a simple, intuitive and more user-friendly tool than a traditional, often impenetrable and lengthy, paper-based safety case, which might depend on hundreds of supporting references. Its purpose and the information presented remains the same as a traditional safety case – i.e. to describe the case for safety, for example, by identifying the most significant hazards and the controls available to ensure risks are acceptably low, including safety critical equipment and human actions. The key difference, though, is that an e-safety case is interactive, using clickable links as a means of connecting and navigating to related information.

DEVELOPMENT

In developing an e-safety case, the first question to be answered is, "Who are the users?" Defining this from the start will determine what information is included, at what level, and how that information is accessed. For example, if the purpose of producing the e-safety case is for submission to the regulator then the presentation will necessarily focus on key hazards, leading the reader through the arguments that risk levels are ALARP; whereas operators may be more interested in understanding the safety critical context of their day-to-day roles.

Figure 3 – Closing the safety-operations gap

The level of sophistication and interactivity can be tailored to suit the organisation and intended use. This can range from including simple hyperlinks within a single PDF document, to creating a web-based portal providing content and access to all supporting components of the safety case, from safety assessment to engineering substantiation to operating procedures and maintenance requirements. There may also be useful links to the live output from ongoing safety management processes, such as safety performance indicators, audit findings and defect reports.

ADVANTAGES

The main advantage of an e-safety case over a traditional safety case is the ease of accessibility to relevant information from multiple entry points, often making use of graphic navigational aids. In the example of a homepage shown in Figure 1, the user can navigate to view major hazards, bowties, safety-critical controls, or job roles. On a separate web page describing the safety case process, shown in Figure 2, the user can navigate to the same places. The power of modern search engines can also be brought to bear, allowing specific information to be tracked down in seconds.

Looking outwards, an e-safety case can be hyperlinked to related documentation such as procedures, method statements, alarm catalogues, job descriptions, risk assessments, etc., thus providing comprehensive and speedy access to the management system. This has the added benefit of highlighting the 'line of sight' from a hazard to its barriers and on to the actual operating controls.

With such a tool in place, users at all levels of an organisation can quickly gain an appreciation of the main hazards, as well as seeing how their role contributes to assuring safety, with many of the key resources needed to do their job at their fingertips. Moreover, this kind of utility naturally lends itself to supporting job induction or awareness training.

Perhaps the greatest benefit of an e-safety case is that it can become a live basis for safety. It can evolve naturally, hand-in-hand with the facility, eliminating the gap between operations and safety (see Figure 3).

DISADVANTAGES

One reason for not developing an e-safety case is the often-daunting prospect of establishing, maintaining and updating such an interlinked set of documents. However, if one accepts the goal of keeping a safety case live, this endeavour should be no more taxing than the paper-based equivalent. In fact, the linked nature of the e-safety case can be used to help identify the potential knock-on effects of change.

Robust processes are needed to control and approve revisions (which may be suggested by users online), albeit sufficiently streamlined to prevent bottlenecks. For simple e-safety cases, these quality processes may be similar to their paper counterparts; whereas for more sophisticated systems, electronic work flow may be employed.

A common pitfall is to allow the e-safety case to grow into a solution-to-all-things, given its potential functionality. Not only can the intended focus on safety be lost, but the initiative (as with any overambitious software project) is more likely to fail. A good e-safety case should not lose sight of its primary objective – to improve understanding, accessibility and relevance.

CONCLUSION

In today's world where answers to most questions can be googled instantaneously, isn't it time the safety world caught up? The development of e-safety cases is no more onerous than conventional safety cases, it's just different. Climbing the learning curve is a small price to pay for the benefits: user-friendly, live safety cases, accessible to all, promoting faster and deeper understanding of the risks to safety.

Taking things further, the e-safety case can be blended with technological innovations such as virtual and augmented reality to bring it to life. This kind of ambitious approach has the potential to change the landscape of safety management in high hazard industries.

Contact: Emily Hilton
emily.hilton@risktec.tuv.com

Wireless communication in major hazard sectors: Challenges and solutions

Many major hazard sectors deploy control and instrumentation (C&I) based safety systems to provide the necessary level of risk reduction for operational plant that would otherwise be unacceptably hazardous. Wireless communication for such systems is more easily installed and maintained than cabling, but what challenges are introduced and can they be solved?

A C&I safety system comprises a number of separate elements which must communicate in order to perform its intended safety function. This communication is traditionally enabled using tried and tested technology based on copper or fibre optic cabling (Figure 1).

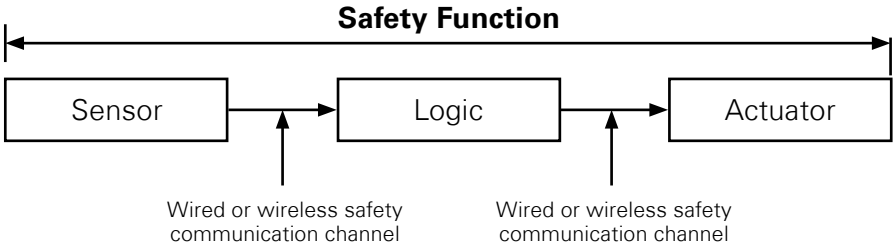


Figure 1 – Safety system elements

The time, trouble and cost of buying and installing communications cabling may be significant and, if disproportionate to the safety benefit, might preclude deployment of risk reduction measures. This is more likely to be the case where the distance between sensors, logic and actuators is significant, or where, as often happens on legacy sites, the installation of additional cabling is potentially hazardous to existing plant.

The continuing advances in commercial off-the-shelf (COTS) wireless communications equipment and the batteries that enable truly wireless operation, has led to use of this technology in non-safety related industrial applications. So far, there has been limited uptake of COTS wireless communications for safety-related systems, except for applications such as crane control and basic data and alarm communications systems.

More widespread use of COTS wireless communications for general safety-related applications is anticipated where the required level of risk reduction is low, as evidenced by the increasing availability of suitable equipment from major C&I equipment vendors, and the development of international standards to facilitate deployment in some major hazard sectors.

NEW CHALLENGES

COTS wireless communication introduces a number of important considerations which are not applicable to safety-related systems using wired communications.

Safety: Wireless communication utilises complex programmable electronic equipment; and demonstrating compliance with functional safety standards such as BS EN 61508 may be challenging.

Security: Wireless communication provides a new attack vector (e.g. eavesdropping, denial of service, hijacking) since it does not require the attacker to gain physical access to the safety related system.

Design: Predicting the reliability of wireless communications during the design phase may be more difficult than for wired communications, as the topology of the site and the presence of temporary obstructions such as scaffolding or vehicles could have a significant detrimental effect.

Maintenance: Routine maintenance of wireless communications equipment could cause spurious data to be sent to the safety-related system, leading to unintended actuation or failure.

Decommissioning: Off-site disposal of a 'failed' wireless device

may provide an attacker with the configuration data necessary to mount an attack on the safety-related system from a location external to the site.

SOME SOLUTIONS

There is a broad range of solutions to these challenges.

White channel / black channel communications: Communications must either be designated as 'white channel' or 'black channel'. White channel communication is characterised by the need to provide a functional safety justification for the associated equipment against standards such as BS EN 61508. However, functional safety justification of communications equipment is not required if the remaining elements of the safety-related system have been designed to detect and appropriately respond to all credible communications failures. In this case, communication may be designated as black channel.

Security measures: A security risk assessment should be completed, with identified threats countered using a defence-in-depth approach where reasonably practicable, to avoid reliance on individual security measures that may be overcome should a threat evolve over time.

Reliability and coexistence: A site specific survey should be completed to correctly locate and configure the COTS wireless equipment in order to ensure adequate communications reliability is achieved, and to ensure adequate separation from any existing equipment that is either sensitive to or emits electromagnetic energy.

Latency: The time taken for the wireless transmission and reception of data may suffer increased latency (i.e. a longer delay) than for equivalent wired communication. The overall system latency is dependent upon the wireless communications system design, which must ensure that the overall safety system achieves its required speed of response.

Network topology: The location of each wireless device and how they are wirelessly interconnected, in either a mesh or star network for example, will generally improve reliability or reduce latency respectively.

Wireless protocol: The standard, policies, procedures and formats which define communication between two or more devices over a network is known as the wireless protocol. Selection of an appropriate protocol is a significant decision, influencing the ability to deliver a number of important factors including security and safety.

Procedural controls: Operating and maintenance procedures must ensure the safety-related system is not compromised by any permitted maintenance activities on the wireless communications equipment. Decommissioning procedures must maintain the security of the system by ensuring the permanent removal of all wireless configuration data when components of the system are decommissioned.

CONCLUSION

When the time, trouble and cost precludes deployment of a safety-related system using wired communications, COTS wireless communications may provide an acceptable alternative if the level of risk reduction required from the system is low. However, the design, safety and security justification of such a system must acknowledge and adequately address the specific challenges that the use of COTS wireless technology introduces.

Contact: Kevin Charnock
kevin.charnock@risktec.tuv.com

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
Crawley
Derby
Edinburgh
Glasgow
London
Rijswijk

Middle East
Abu Dhabi
Dubai
Muscat

North America
Calgary
Houston

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