RISKworld

issue 17 spring 2010 — *the newsletter of risktec solutions limited*

In This Issue

Welcome to Issue 17 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

The Route to Safe Operations

We are pleased to report that Risktec is weathering the economic climate extremely well. We feel that our determination to provide high quality, affordable services and to work flexibly and closely with our clients is partly responsible. We would like to take the opportunity to thank our clients, old and new, for their loyalty.

Our training business, launched last year, is progressing well and attracting considerable attention. We are pleased to be working with a number of clients to offer tailored training solutions, from full MSc programmes to selected modules.

This 17th edition of RISKworld presents a diverse range of articles, illustrating the continuing challenge to achieve safe operations. The Nimrod review (Page 2) is a hard hitting and sobering investigation into the tragic loss of an RAF Nimrod in September 2006. It contains many salient reminders for those of us who are involved in safety.

Major accidents like this are arguably responsible for the many regulatory bodies in existence today. These organisations have an important role to play in shaping industry practice, as the articles on Safety Performance Indicators (Page 5) and Layers of Protection Analysis (Page 4) illustrate.

Perversely, strong regulatory regimes can mean that industry may over-design engineered systems compared to the overall risk. Our article on nuclear decommissioning (Page 3) explores this theme, where there is a clear trade-off to be made between the short-lived, one-off risk of decommissioning activities and the reduced long-term risk, once decommissioning is completed.

Our last article (Page 6) explains how to get the best out of human factors, a discipline which is receiving more and more attention from the regulators because of the key role the operator plays in preventing accidents.

Whilst it is important to learn from past mistakes, the route to safe operations is all about applying professional foresight in a pragmatic and balanced way, and ensuring that safety is built-in not bolted on.

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

The Folly of 'Paper Safety' – Lessons from the Nimrod Review

On 2nd September 2006, RAF Nimrod XV230 was on a routine mission over Helmand Province in Southern Afghanistan when, only minutes after completing air-to-air refuelling, she suffered a catastrophic mid-air fire which led to the total loss of the aircraft and the death of all 14 on board. Following the initial investigation by the Board of Inquiry which reported on the probable cause of the accident, a broader independent review was instigated in late 2007.

The Nimrod review, led by Charles Haddon-Cave QC, conducted a wide-ranging inquiry over some 20 months. It studied many thousands of documents dating from the 1930s to the present day, interviewed hundreds of witnesses of all ranks and in all relevant organisations, and visited numerous locations [Ref 1].

The review concluded that the most likely cause of the accident was an inadvertent fuel overflow from number one tank during air-to-air refuelling, which ignited on contact with a hot pipe. The review further concluded that design flaws introduced in 1969, 1979 and 1989 all played a crucial part in the loss of XV230. Also, there had been a number of previous incidents and warning signs potentially relevant to XV230, which should have served as a "wake up call".

A Lamentable Job

According to the review, the Nimrod Safety Case, which took 4 years to produce after the introduction of new regulations in 2002, was a "lamentable job from start to finish" and missed the key dangers. The "best opportunity to prevent the accident to XV230 was, tragically, lost".

The Nimrod Safety Case process was "fatally undermined by a general malaise" – a widespread assumption by those involved that the Nimrod was 'safe anyway' because it had successfully flown for 30 years – and the task of drawing up the Safety Case became a paperwork and 'tickbox' exercise. The safety case "was virtually worthless as a safety tool".

The review concludes that the safety case regime in the military environment has led to a culture of 'paper safety' at the expense of real safety. It currently does not represent value for money. The shortcomings of a significant proportion of safety cases are extensive [see Box 1].

Box 1 – Safety Case Shortcomings

- Too long and **bureaucratic** with unnecessary detail, often for 'invoice justification'
- **Obscure**, inaccessible and difficult to understand language
- Failing to see the **'wood for the trees'**
- Routine **outsourcing** to organisations who churn out voluminous quantities of paperwork in back offices
- Lack of vital input from **operators** and maintainers who have the most knowledge and experience of the system
- Written to **comply** with the requirements of regulations, rather than as working documents to improve safety
- Audits which focus on **process** rather than substance
- Languish **'on-the-shelf'** rather than 'living' documents or a tool for keeping abreast of hazards

The purpose of any safety case regime is to encourage people to think as actively as they can to reduce risks [Ref 2]. But, in some instances, the review suggests that safety cases seem to be achieving the opposite effect: "giving people a false sense of security that a safety case is some sort of paper 'vault' into which risks may be safely deposited and forgotten about".

Lessons Learned

The Nimrod review points out that while lessons to be learned from the loss of XV230 are profound and wide-ranging, many of the lessons are not new. The organisational causes echo other major accidents, such as the loss of the space shuttles Challenger and Columbia, and the Piper Alpha disaster and BP Texas City explosion.

The review makes recommendations in eight key areas to improve safety and air worthiness for the future, including a new approach to safety cases. In particular, recommendations are made for best practice for safety cases, which should be brought in-house, and made more focused, proportionate, and relevant.

The review also recommends renaming safety cases 'Risk Cases' to focus attention on the fact that they are about managing risk, not assuming safety. A simple definition of a Risk Case is a "reasonable confirmation that risks are managed to ALARP levels". It is further proposed that Risk Cases should be 'SHAPED' against six principles: Succinct, Home-grown, Accessible, Proportionate, Easy to understand and Document-lite.

Conclusions

The language of the Nimrod review is direct, its criticisms unsparing. In particular, it is outspoken about the military safety case culture of 'paper safety' and recommends a host of solutions.

The military safety case regime is relatively new having only been introduced in 2002. Other high-hazard industries with a longer history of safety cases have similarly wrestled with implementing best practices (for example, see Ref 3). The Nimrod review is a timely reminder that safety cases are worthless unless safety is embedded in engineering and operations.

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

References

1. The Nimrod Review, Charles Haddon-Cave QC, 28th October 2009.
2. Ladbroke Grove Rail Inquiry Part 2 Report, 2001.
3. Ten Good Practices for Oil & Gas Safety Cases, RISKworld, Autumn 2006

Nuclear Decommissioning Demands New Thinking

To achieve the stringent levels of safety required over their lifetime, nuclear power plants rely heavily on engineered safeguards. Other industries, where consequences are less severe, rely more on procedural controls and operator action to manage risks. Understandably, the emphasis has been on designing new operating facilities and upgrading existing facilities to meet improving standards.

However, as industries and countries around the world increase the focus on nuclear decommissioning and clean-up, significant challenges are emerging. There can be considerable political, regulatory and commercial pressure to make progress, yet it is vital that activities are carried out safely and risks are shown to be ALARP. In this respect, much of industry good practice has been developed for operating facilities, and may not be wholly applicable to the specific issues associated with decommissioning and clean-up. For example, the risk stays approximately constant for operating facilities , whereas there is often an increase during decommissioning and clean-up activities with a net reduction in the long-term.

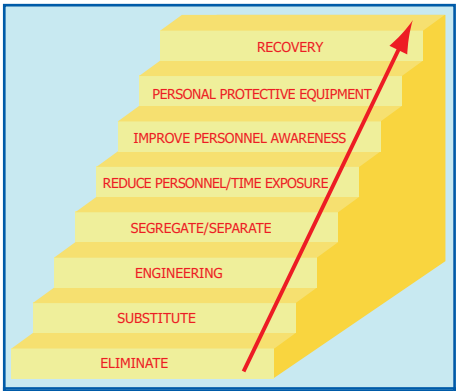


Figure 1 – Risk Control Hierarchy

In a typical risk control hierarchy [see Fig 1], engineered safeguards occur early in the order, and the capital outlay for these controls can be justified over the operating life of the facility. The situation is less clear cut for decommissioning. Whilst it is generally accepted that engineered controls provide greater safety assurance, other factors to consider include:

- The magnitude of unprotected consequences, which may be relatively low
- The required life of the control – one-off versus repeated activity
- The ease (or otherwise) of implementation and any interaction with the existing facility

Courtesy of Simon Ledingham & www.visitcumbria.com

Sellafield in the UK, where decommissioning and clean-up continues

- The time and effort required to design, build and commission new engineering
- Whether the ALARP principle can be satisfied through procedural control, perhaps supplemented by simpler engineered controls

Figure 2 illustrates how there may well be overall risk benefit in making early progress with decommissioning/clean-up activities. In many instances 'doing nothing' invariably leads to an inexorable increase in risk as facilities and other risk controls age. A heavily engineered solution, which may only be required for a limited number of operations, takes time and effort to conceive, design, build, commission and implement.

Serious consideration should thus be given to the greater use of procedural controls to support safe undertaking of decommissioning and clean-up activities. Whilst a safety assessment may not give as much credit to procedural controls as engineered controls, the transitory increase in risk may well be justified in achieving overall risk reduction much earlier.

Procedural controls are not an easy option. It is a sobering reminder that many major incidents can be attributed to undertaking non-routine tasks (e.g. Chernobyl, Texas City, Kleen Energy) where a failure to adhere to procedural controls led to fatalities. It is imperative, therefore, that procedural controls are not simply recorded on paper, but are demonstrated in practice. This will mean thorough training for operational personnel and evidence that they have achieved a prescribed level of competency. Where possible, practical rehearsal of the activity in a non-hazardous environment should be carried out.

Conclusion

Decommissioning and clean-up present considerable challenges to all stakeholders. In many instances bespoke solutions to problems need to be developed, requiring ingenuity and expertise from a great many professionals. Conventional safety assessment and justification methods, which have invariably been developed for operating facilities, may well need to be re-evaluated and adapted to enable hazardous facilities to be safely and efficiently decommissioned.

Contact: : Patrick Wilson (Warrington)
patrick.wilson@risktec.co.uk

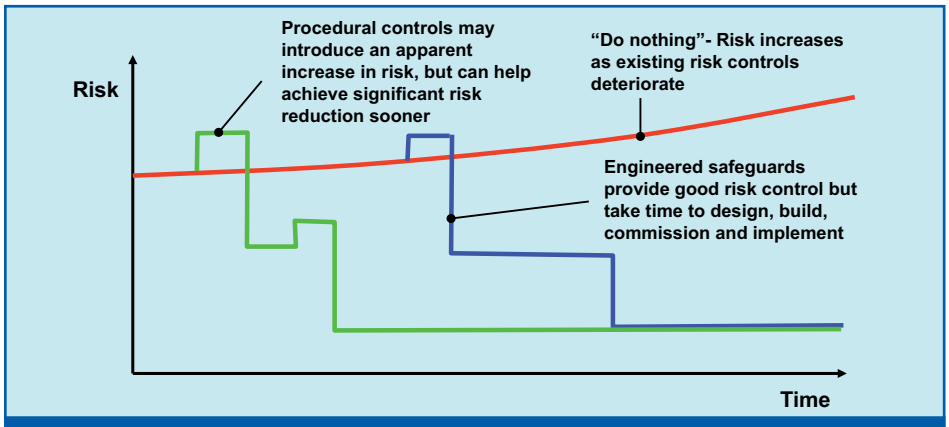


Figure 2 – The Benefits of Earlier Decommissioning

Closing the Safety Gap – Safety Integrity Level Selection Using LOPA

Safety instrumented systems are often used to reduce the risk associated with a potentially hazardous process or plant. It is usual to express the level of risk reduction required as a safety integrity level or 'SIL'. As such, selecting an appropriate SIL is a fundamental step in any safety specification and there are a number of different methods employed, depending on industry. In the oil, gas and process sector, Layers of Protection Analysis (LOPA) is arguably the method of choice. Following the Buncefield incident, for example, the Buncefield Standards Task Group suggested a LOPA study be used to provide a more consistent approach to SIL assessment [Ref 1].

Courtesy of Royal Chiltern Air Support Unit

The Buncefield incident was attributed to tank overfill

Why LOPA?

LOPA is a systematic methodology for examining defence-in-depth and assigning SIL targets. Its careful application can ensure that an organisation achieves a defined and consistent level of safety across all of its processes and plant. The basic LOPA approach is described in Box 1.

Box 1 - LOPA Process

- Define the unwanted outcomes and tolerable risk targets
- Identify initiating events
- Identify independent protection layers
- Quantify the frequency of initiating events
- Quantify the effectiveness of each protection layer
- Evaluate the frequency of unwanted outcomes
- Determine the SIL required to meet each tolerable risk target

When appropriately applied, LOPA can very clearly identify what independent layers of protection are available against each initiating event. It can also use the initiating event frequency and the failure probability assigned to each protection layer in order to determine any gap between the likelihood of each outcome and that which is tolerable [see Fig 1].

One way of closing this gap is to provide a safety instrumented system capable of arresting the accident sequence with an associated SIL target.

LOPA Lessons

When the UK's Health and Safety Executive reviewed a number of LOPAs submitted by sites which store flammable liquids such as petrol (i.e. Buncefield type sites), they identified several areas of concern with many of the assessments [Ref 2]. The main issues were:

- Inadequately defining tolerable risk levels.
- Lack of frequency justification, including compliance with Functional Safety Standard IEC 61511.
- Inadequate substantiation of human error probabilities.
- Too much reliance on generic data without accompanying applicability arguments.
- Dependencies between protection layers claimed as independent.
- An absence of sensitivity analysis to ensure the robustness of LOPA conclusions.

Although these concerns were levelled at LOPAs for fuel storage sites, they can be read across to other LOPA applications. In addressing these concerns, there are a number of other improvements that should also be considered [see Box 2].

Box 2 – Further LOPA Improvements

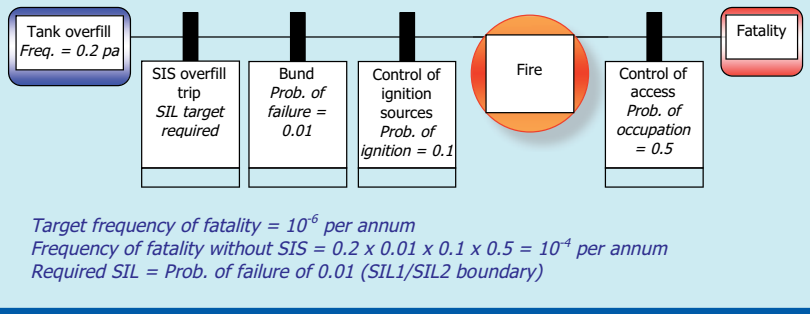
- Ensure appropriate training for LOPA assessors
- Use a systematic and comprehensive approach to identify initiating events
- Ensure a thorough understanding of accident sequences and their consequences, supported by analysis where appropriate
- Consider combining the hazard analysis (HAZOP) workshops, LOPA, and SIL assignment to maximise efficiency

Conclusion

Any SIL selection method, if inappropriately applied, can lead to an insufficient SIL target, with a potentially intolerable level of risk. Conversely, a much too stringent SIL target can divert resources away from other more deserving risk reduction projects.

While LOPA provides a sound framework for deriving representative SIL targets, unsurprisingly, it relies heavily on supporting evidence, as well as the experience and expertise of the assessment team.

Contact: Kevin Charnock (Warrington)
kevin.charnock@risktec.co.uk



Target frequency of fatality = 10^{-6} per annum
Frequency of fatality without SIS = 0.2 x 0.01 x 0.1 x 0.5 = 10^{-4} per annum
Required SIL = Prob. of failure of 0.01 (SIL1/SIL2 boundary)

Figure 1 – SIL Derivation Using Layers of Protection Analysis

References

1. Safety & environmental standards for fuel storage sites, BSTG, 2007.
2. A review of the Layers of Protection Analysis (LOPA) analysis of overfill of fuel storage tanks, HSE, 2009.

Measuring Safety – Safety Related Key Performance Indicators

Many of us are familiar with the concept of Key Performance Indicators (KPIs) as a simple way of indicating how organisations are performing against targets, whether they relate to production, finance or safety. Safety Performance Indicators (SPIs) in particular are notorious for focusing on the negative things that have happened in the workplace, with indicators such as lost time injuries (LTIs). But such measures record outcomes only (they are 'reactive') and provide little or no insight into underlying trends and are very poor indicators of the potential for major accidents.

Guidance galore

Recognising this situation, in 2006 the UK Health and Safety Executive (HSE) issued a guidance note on the subject [Ref 1] following the investigation into the BP Grangemouth incident in 2000 and subsequent research. The US Centre for Chemical Process Safety (CCPS) of the AIChemE published its guidance [Ref 2] in 2007 following the Texas City explosion in 2005. The Organisation for Economic Co-operation and Development (OECD) meanwhile updated its guidance in 2008, building on the experience of the UK HSE [Ref 3]. Furthermore, the UK Fire and Blast Information Group (FABIG) held a Technical Meeting in 2008 on SPIs.

All of this guidance is consistent in approach – the aim is to develop performance indicators that help operators see how well they are managing their major accident risks.

Setting SPIs

As with all KPIs, SPIs fall into two types – leading and lagging. Lagging indicators are in common use and tend to consider things that have gone wrong, while the challenge is to develop meaningful leading indicators – things that give an early warning sign that all is not well. Prof. James Reason's 'Swiss cheese' model of accident causation says major accidents result when a series of failings in risk control systems occur at the same time – the holes in the Swiss cheese slices line up [see Fig 1].

The leading indicators are there to identify the failings through routine checking, to plug the holes before an accident occurs. The lagging indicators reveal the holes through the occurrence of incidents, accidents or defects at which point action can be taken to prevent recurrence.

The HSE describes a 6 step approach to developing and using SPIs [see Box 1].

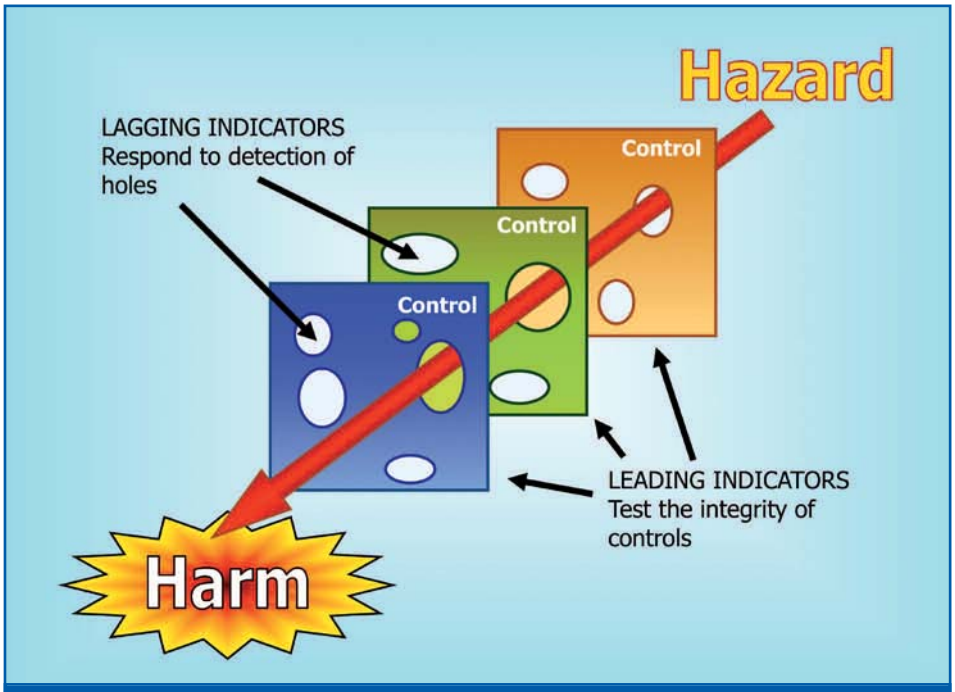


Figure 1 – Safety Performance Indicators and the Swiss cheese model

Box 1 – Six Steps to Effective SPIs

1. Establish the organisational arrangements to prepare and implement SPIs
2. Define the scope of the measurement system
3. Identify the risk control system in place and set a lagging indicator that indicates failure
4. Identify critical elements of the risk control system – actions or processes which must function correctly – and set associated leading indicators
5. Establish a data collection and reporting system
6. Review data and take action

So what does it all mean?

In the UK the HSE has decided to change the way it regulates the control of major hazards [Ref 4]. Now, inspections will focus on the risk control measures claimed by operators and their related SPIs.

It is important to define SPIs that not only demonstrate the hazards are being properly controlled, but are also useful to the operator and not just a 'box ticking' exercise to satisfy the regulator. Moreover, they should not demand so much data collection and complex analysis that they become impractical and fall into disuse. As with most KPIs, simpler is better.

'Bow-tie' or barrier diagrams are one of the best methods for understanding risk control systems, and a powerful approach to identifying leading SPIs would be to ensure every control system on the diagram has a relevant measure. Such indicators might be associated with the completion of equipment checks, proof tests, maintenance, and personnel training within specified timeframes.

Outside the UK the work by the AIChemE and the OECD show that SPIs are being taken seriously internationally. Within the oil and gas industry, for example, it seems likely that SPIs will find a place in the reporting systems of major companies to allow worldwide performance comparisons.

Conclusion

Developing effective SPIs is not necessarily straightforward. Operators should be wary of creating an unwieldy system where counting becomes more important than action. Nevertheless, a more balanced approach to SPIs that considers leading as well as lagging indictors should aid both regulators and operators in identifying and filling holes in the management of major hazards.

Contact: Andy Harding (Warrington)
andy.harding@risktec.co.uk

References

1. HSE, Developing Process Safety Indicators, HSG254, 2006.
2. CCPS, Process Safety Leading and Lagging Metrics, 2007.
3. OECD, Guidance on Developing Safety Performance Indicators, 2008.
4. www.hse.gov.uk/comah/remodelling/index.htm

Breaking Down the Barriers to Human Factors Integration

Human factors (HF) has become relatively well-known as a scientific and engineering discipline that can be used to improve the safety and efficiency of systems, reducing risk and cost [Ref 1]. The list of HF tools available for use by both specialists and lay practitioners is as extensive as the discipline is broad. But how does a project or organisation know which tools to use and when? How do we ensure HF is applied in a cost-effective manner? How much HF is enough and when does it stop adding value?

These questions are answered by human factors integration (HFI), which is a managed process along the lines of project management [see Box 1 and Ref 2]. Like project management, the basics of the HFI process can be taught, but successful HFI is a skill that comes with knowledge, practical experience and innate ability.

Box 1 – Human Factors Integration

HFI is "a systematic process for identifying, tracking and resolving human related issues to ensure a balanced development of both technologies and human aspects of systems" [Ref 3].

Every HFI programme should aim to:

- Ensure a consistent and adequate consideration of all relevant aspects of HF is used during the design and development of systems, equipment and operational practices
- Assist a project or facility in implementing HF activities in a justifiable, cost-beneficial way
- Provide an auditable record of those HF activities
- Provide project teams and organisations with an understanding of the basics of HF, why it is important and how it can be factored into design decisions and safety case arguments

Barriers to HFI success

HFI programmes are often implemented following a set process that, despite having the word "integration" in the title, still sits apart from other project processes. As such these initiatives end up being at best, ineffective and at worst, counter-productive.

Typical barriers to success include [Ref 4]:

- A lack of common understanding between project groups (HF, safety case, engineering, designers, operations) particularly relating to HF data collection and use
- Different mind-sets between project groups for solving the same problem, often expressed in different technical language
- Misalignment of HF processes with those of relevant project areas, hampering coordination
- Mismatch in scope between project disciplines, creating gaps in integration

Sometimes, HFI initiatives fail because they are too ambitious. Under the label HF "best practice", they can cast the HF net too wide, attempting to "tick all the boxes" rather than finding a good balance between HF, cost, timescale and effective implementation. In striving (and invariably failing) to achieve perfection, ironically HF becomes part of the problem.

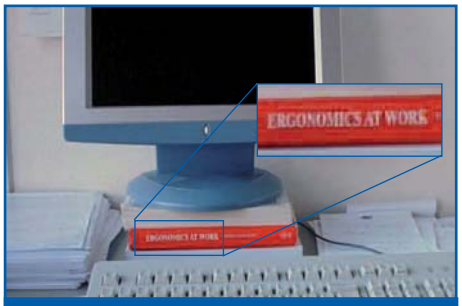
HF throughout life

As HF experience increases, it inevitably means that the integration of HF activities into some stages of a project or system lifecycle is better defined and more likely to be achieved than others. The HF processes within design and operations, for example, are becoming much more effective as organisations and HF specialists deliver more and more programmes that focus primarily on these stages.

HFI in the other lifecycle stages, however, is much less practised. Two clear examples are construction and decommissioning:

HF for Construction

The design has arguably the biggest single influence on constructability, which can crucially depend on human intervention. Poor HFI can affect build quality, lead to re-work, programme delays and safety risks (either during build or operations). Good HFI can also minimise traditional health and safety issues (e.g. manual handling, slips, trips and falls, noise) if it is applied in organisational arrangements (e.g. management structure, safety culture, communications, supply chain management) and job design.



A sceptic's view on the best application of theoretical ergonomics

HF for Decommissioning

Shifting from the operations mode of monitoring highly-automated systems or acting as the "person-in-the-loop" of process control, to the irregular, non-routine, time-limited activities that occur during decommissioning also requires a shift in HF focus. As design solutions become less practical and more costly, the HF emphasis should be on the provision of effective preparation, training (re-skilling as well as task-specific) and pre-job "walk-throughs", as well as optimising organisational arrangements.

Conclusion

HF can add great value to projects when applied in an integrated and intelligent manner throughout a system or facility lifecycle, rather than adopting a piecemeal or bolt-on approach. This requires a project-wide appreciation of HF, as well as access to seasoned HF specialists – not to spout the latest research on the forensic ergonomics of distraction errors, but to work closely with a multi-disciplinary project team to deliver key HFI benefits and add real value.

Contact: Karen King (Warrington)
karen.king@risktec.co.uk

References

1. RISKworld, Issue 15.
2. RISKworld, Issue 14.
3. DEF STAN 00-250 Part 0: Human Factors Integration, UK MoD, May 2008.
4. Bird (2008), Integration is more than a human factors issue, Proceedings of the 2008 UK Ergonomics Society Annual Conference (April 2008, Nottingham, UK).