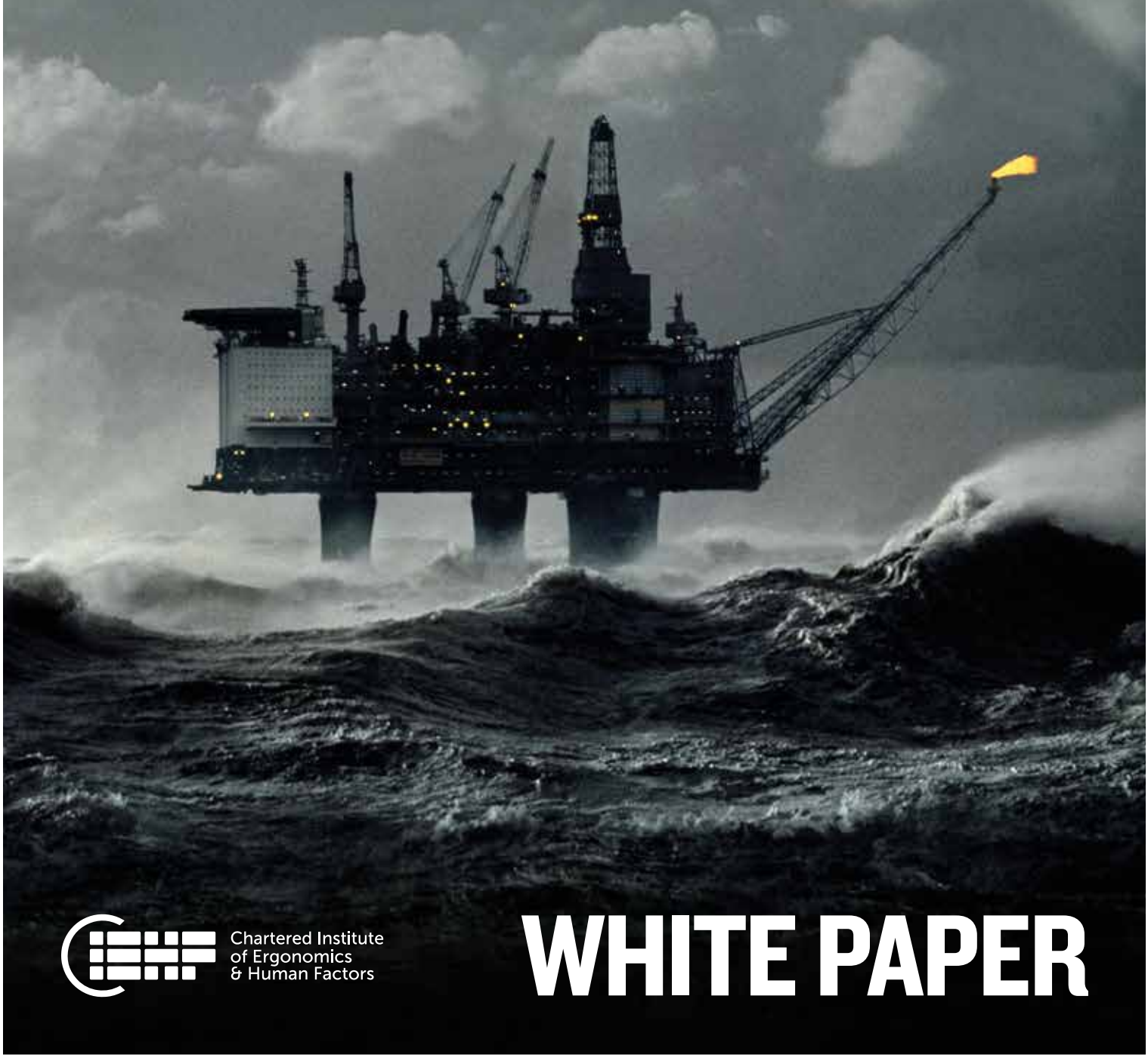
HUMAN FACTORS
IN BARRIER MANAGEMENT

For those with corporate or asset-level responsibility for the development, implementation and assurance of safety and environmental management systems



Chartered Institute of Ergonomics & Human Factors

WHITE PAPER

HUMAN FACTORS IN BARRIER MANAGEMENT

A White Paper by the Chartered Institute of Ergonomics & Human Factors

Prepared by a CIEHF Working Group comprising: Ron McLeod, Ian Randle, Rob Miles, Ian Hamilton, John Wilkinson, Christine Tomlinson, Gyuchan Thomas Jun, Tony Wynn.

December 2016

www.ergonomics.org.uk

ciehf@ergonomics.org.uk

FOREWORD

The Chartered Institute of Ergonomics & Human Factors (CIEHF) is a UK-based professional body which raises awareness of the discipline, sets and maintains professional standards and promotes communication among those who have an interest in ergonomics, human factors and related fields.

Part of our remit as an organisation with a Royal Charter includes the dissemination of information on ergonomics and human factors research and good practice. This includes the publication of conference proceedings, case studies and white papers.

A white paper is an authoritative report or guide that informs readers concisely about a complex issue and presents the issuing body's philosophy on the matter. It is meant to help readers understand an issue, solve a problem, or make a decision.

This white paper on Human Factors in Barrier Management is the first in a series on key current and emerging issues in ergonomics and human factors. It was prepared by a technical steering group of practitioners and academics with a professional interest in human factors and barrier management. It was reviewed by a wider group of members from CIEHF. The work was led by Professor Ron McLeod.

Dr Ian Randle

President of the Chartered Institute of Ergonomics & Human Factors (2016-2107)

Barrier management refers to the process of ensuring that the controls an organisation intends and expects to have in place to protect against losses are actually capable of doing the job, are properly implemented, and are supported and maintained such that they will function as expected when needed.

Whatever the industry sector, the single most frequent, and arguably the most important, factor in any approach to barrier management is people: whether they are relied on to perform some barrier function or to ensure other barriers are in place and effective, or if they are viewed as a risk factor that can degrade or defeat barriers.

The traditional high-hazard industries – oil and gas, nuclear, rail, aviation, mining – apply a variety of more or less formal approaches to identifying, analysing and assuring barriers. The technique of Bowtie Analysis however is becoming increasingly popular. There is as yet little standardisation or recognised best practice about how to conduct and implement Bowtie Analysis either within or across sectors. Because of this, practices have developed and been shared across businesses and industries that are not consistent with good practice in human factors and ergonomics.

Many organisations struggle to know how to ensure: a) that the human performance they need and expect can reasonably be relied upon to be delivered when and where it is needed, and; b) that the controls they intend to have in place are as robust as they reasonably can be to the loss of the expected standards of human reliability.

With a membership drawn from 43 countries, one of CIEHF's strategic priorities is to promote best practice in ergonomics and human factors. CIEHF members have become concerned at how human performance is being addressed in some current approaches to barrier management, and in Bowtie Analysis in particular. A significant gap has developed between:

- What is known from research and experience as well as from innumerable incident investigations about the role of people in socio-technical systems, the nature of human performance and factors that contribute to loss of human reliability; and
- The expectations and assumptions about human performance – especially of those working at the operational front line – that are actually being embedded in many operational barrier models.

Recognising both the rapid growth in the use of Bowtie Analysis, and the lack of current standardisation or established good practice, CIEHF has prepared this white paper providing recommendations on how human factors issues should be treated in barrier management in general, and in Bowtie Analysis in particular. Specific objectives are:

i. to bring clarity to some areas where there is ambiguity or confusion in the way human performance is treated, and

ii. to set out recommendations for good practice in developing and managing those elements of barrier systems that either rely on, or can be defeated or degraded by, human performance.

The white paper is intended mainly for those with corporate or asset-level responsibility for the development, implementation, and assurance of safety and environmental management systems. Typical users will include HSSE professionals, regulators and technical and operational managers.

Structured into four major sections, the white paper provides background information and context for the role of people in barrier systems and sets out concerns about the way human and organisational factors are currently treated in some approaches to barrier management. The paper sets out 33 recommendations to improve the development, implementation and management of the human performance aspects of barrier management systems.

Developing the paper drew on experience from safety-critical industries including oil and gas, mining, nuclear, rail, healthcare and air traffic management. While recognising the need for care in cross-industry applications, the material contained in it should be of value in many sectors.

6

CONTENTS

8

The concept of barrier management – implementing and assuring a range of controls[1] to protect against the risk of major losses – is widely used across many industries[2]. While it is currently applied with most rigour in industrial processes, and particularly the traditional 'high-hazard industries' (nuclear, oil and gas, rail, etc) the concept applies to virtually every industry with the potential for significant losses. Industries such as healthcare, banking, the public services (police, fire, ambulance), and public utilities (water, electricity and gas distribution) all place heavy reliance on barriers to guard against losses.

In 1995, Lord Bruce of Donnington spoke in the House of Lords in a debate on the Chancellor of the Exchequer's investigation into the collapse of Barings Bank. Commenting on the number of measures that were thought to have been in place to prevent the collapse of a major bank, and on how all of those measures were defeated, Lord Bruce remarked:

> *It seems to me that the Bank of England ought never to have authorised this concern without verifying that all of these conditions were in place.*

His challenge was precisely the same one many organisations and regulators face in seeking to have confidence in the controls they believe and expect to be in place to protect against losses; are they actually in place and will they perform as intended and expected when they are needed? And in the case of Barings Bank, as in virtually every other industry, those defences rely predominantly on people.

Achieving and maintaining reliable human performance is a major concern in organisations that rely on barrier management. On the one hand, the performance of people continues to be relied upon for controls to function as expected: this is true whether the vigilance, decision making and actions of people act as controls in their own right, or whether they are relied on to ensure physical, hardware or electronic controls are effective. On the other hand, the inherent variability of human performance – 'human error' – is widely regarded as one of the principal threats that need to be guarded against through the use of barrier models.

Most organisations, however, struggle to know how to ensure: a) that the human performance they need and expect can reasonably be relied on to be delivered when and where it is needed, and; b) that the controls they intend to have in place are as robust as they reasonably can be against the loss of the expected standards of human reliability.

1. A variety of terms are used to convey the same idea most commonly 'layers-of-defences', and 'protection layers', as well as terms such as 'protective measures'. These terms sometimes have very specific meanings: such as in Layers-of-Protection-Analysis (LOPA) and 'Control' in the STAMP (Leveson, 2011) and FRAM (Hollnagel, 2012) techniques. See the definition of 'control' as used here in section 6.

2. CIEHF is aware of the potentially negative psychological connotation of the term 'barrier'. Despite the specific meaning of the term in the context of preventing unsafe events, the term can be interpreted as having a role that is counter-productive to efficient operations – this in itself could act to limit the willingness of some individuals to fully accept their role as a 'barrier' – in a layer-of-defences strategy. Many CIEHF members prefer the use of the terms 'control' or 'defence', which have more psychologically positive connotations. However, due to its very widespread take-up, this paper will adopt the use of 'barrier' and related terminology.

Box 1: Over-prescription of a toxic drug

An elderly female patient, who had been taking a drug called Methotrexate for rheumatoid arthritis, died from her immune system failure due to Methotrexate overdose (ref: Cambridgeshire Health Authority 2000).

Her General Practitioner had increased a prescription from the patient's usual single weekly dose of 17.5 mg Methotrexate up to 10 mg daily (a total weekly dose of 70 mg). The intention had been to prescribe 10mg "as directed", though the wrong frequency was selected in the computerised prescription system. The community pharmacist interpreted the prescription as Methotrexate 10mg once per day and entered the detail into the computerised patient records system. The patient dutifully took one 10mg tablet daily following the directions printed on the medicine bottle.

While preparing a repeat prescription, a second GP identified the frequency error and crossed it off from the written prescription. The error however remained unrectified on the patient's computer record, and was consequently repeated.

The patient began to feel unwell and deteriorated. She was admitted to an ENT ward under the care of a third doctor. The patient's GP faxed the patient information but it was not received by the third doctor.

Blood tests were ordered, but two successive samples were inadequate to obtain blood counts. The ward doctor phoned the patient's surgery and received confirmation from a non-medical member of staff that 10mg daily was the correct prescription. Methotrexate 10mg was therefore continued to be administered daily.

A nurse eventually suggested to a fourth doctor that Methotrexate could be the cause of the problem. This doctor pursued the need for blood tests and obtained the blood count results. The results confirmed Methotrexate overdose but it was too late. The patient died.

What barriers might have been expected to have been in place that should have prevented this accident?

- Care and attention to detail in writing the original prescription?
- Cross-checking of prescriptions?
- Computer-based warnings of high dosage?
- Procedures for rectifying known prescription errors?
- Communication of critical information?
- Management of critical data?
- Persistence in checking data and completing critical checks?
- Ownership of responsibility for patient care?
- Medical discipline?

1.1. IMPLICIT CONTROLS

The controls organisations believe they have in place to protect against incidents are frequently only made explicit after incidents occur. One way to approach the concept of barrier management is therefore to look at incidents that have occurred, and to consider what controls the organisations involved intended and believed they had in place that should have ensured those incidents did not occur.

Boxes 1 and 2 summarise two incidents, one involving a fatality in healthcare due to an overdose of a prescription drug and the other involving fatalities at sea. The boxes illustrate a number of examples of the kind of controls that are often implicitly relied upon to prevent such incidents – from signage, the use of checklists and alarms through risk assessment and hazard analyses, to training, supervision, risk awareness and even care and attention on the part of individuals[3].

3. The Methotrexate overdose incident is explored in more detail in section 5.3.

The purpose of barrier management is to make the kind of implicit controls illustrated in boxes 1 and 2 explicit: to be clear about exactly what controls are relied on to prevent incidents, to understand their characteristics, to have an understanding of how reliable they can be expected to be, and to know what needs to be done to ensure the controls are implemented and continue to function throughout their expected operational lifetime.

Box 2: Two fatalities at sea

A seaman collapsed during a routine operation to secure a rattling anchor chain within the chain locker on board a vessel. The supervising 'leading hand' raised the alarm and put on an emergency escape breathing device (EEBD) to enter the chain locker in an attempt to rescue his shipmate. However, he too collapsed when he removed his EEBD.

With the assistance of a rescue team from a nearby drilling rig, the victims were recovered from the chain locker and evacuated ashore by helicopter. Both men were dead on arrival, having died as a result of the oxygen-deficient atmosphere inside the chain locker, due to on-going corrosion of the steel structure and anchor chain.

The victims, the master and some others on board had failed to recognise that the chain locker was a dangerous enclosed/confined space and the likelihood that the atmosphere could become lethal during routine shipboard operations. Casual entry to the chain locker had become routine for this crew; the job had been done in a similar fashion many times before, so that poor hazard recognition was likely to have been reinforced by regular operational practices on board.

What barriers might have been expected to have been in place that should have prevented this incident?

- Safety management system (SMS) encompassing:
  - Risk assessment e.g. JSA?
  - Training, drills and rescue procedures?
  - Command and control of the rescue team?
  - Permit to work?
  - Use of PPE/EEBD?
  - Hazard recognition training?
- Risk awareness from experience?
- Safety culture?
- Audit process to detect deficiencies in training, equipment and drills?

1.2 THE CASE FOR A WHITE PAPER

Any strategy that aspires to a degree of formality and rigour in the way it identifies, assures and manages barriers needs to be able to deal with the many human and organisational (HOF) factors that inevitably arise in a way that is both rigorous and technically sound while being realistic and pragmatic. It also needs to be adequately grounded in what is known of the psychology of human behaviour and performance.

With a membership drawn from more than 40 countries, one of CIEHF's strategic priorities is to promote best practice in ergonomics and human factors. For over 65 years, CIEHF members and associates have been prominent in the research, development and implementation of many of the techniques and regulatory approaches that are now considered global best practices in implementing human factors in safety-critical industries. Examples include: safety management systems; safety-critical task analysis; safety culture assessment; human factors in incident investigation; integration of human factors engineering into capital projects; and human reliability analysis (quantitative and qualitative approaches to demonstrating the risk of human error has been reduced to a level that can be shown to be as low as reasonably practicable (ALARP)).

Through their professional activities, CIEHF members are aware of the cross-sector importance of barrier management. In particular, the technique of Bowtie Analysis is increasingly prominent in supporting the development and operational management of barrier models. This rapid growth in Bowtie Analysis has been driven largely by the conceptual simplicity of the approach and the visual representation of the analysis, together with access to easy-to-use software tools.

While there is some published literature on the topic, there is, as yet, little standardisation or recognised best practice about how to conduct and implement Bowtie Analysis either within or across sectors[4]. The guidance that is available says little or nothing about what represents good practice in dealing with human factors aspects of barriers[5]. Consequently, practices have developed and been shared across businesses and industries that are inconsistent with good practice in human factors and ergonomics.

There are of course other ways of modelling hazard and risk, which do not use Bowties. For example, while some COMAH operators in the UK used Bowties for their initial safety report submissions from 2000 onwards, this approach fell out of fashion for a time before later returning. Companies typically followed basic HAZID/HAZOP approaches with some use of other methods such as Failure Mode and Effects Analysis (FMEA). The resulting tables were then often used to try and link hazards and risks to control measures.

The purpose of this white paper is to set out a CIEHF position on the treatment of human factors issues in barrier management in general, and in Bowtie Analysis in particular.

1.3 TARGET AUDIENCE

This white paper is intended mainly for those with corporate or asset-level responsibility for the development, implementation, and assurance of safety and environmental management systems. Typical users will include HSSE professionals, regulators and technical and operational managers.

Developing the background and recommendations drew on experience from safety-critical industries including oil and gas (upstream as well as downstream), mining, nuclear, rail, healthcare and air traffic management. While recognising the need for care in cross-industry applications, the material contained in this white paper should be of value in many sectors.

4. Though there are exceptions. For example, the Norwegian Petroleum Safety Authority has set out broad principles for barrier management in the petroleum industry (PSA, 2013). The International Council on Minerals and Mining, has also issued a guide to good practice in managing what it refers to as "critical controls" (ICMM, 2015) in the mining and metals industry. Neither however say much about human factors.

5. Though the Center for Chemical Process Safety is currently preparing guidance on how to carry out Bowtie Analysis that includes some material (sponsored jointly by the Energy Institute) on human factors (CCPS, 2017).

1.4 STRUCTURE

The document has four sections;

Section 2 defines the scope of the document.

Section 3 provides important background information and context for the role of people in barrier management systems.

Section 4 discusses some concerns about the way human and organisational factors are treated in the development and implementation of some barrier models.

Section 5 identifies 33 recommendations to improve the development, implementation and management of the human performance aspects of barrier management systems.

Specific objectives are:

i. To bring clarity to some areas where there is ambiguity or confusion in the way human performance is treated, and

ii. To set out some recommendations for good practice in developing and managing those elements of barrier systems that either rely on, or can be defeated or degraded by, human performance.

14

2.1 BASIC CONCEPTS

The core ideas behind barrier management are captured in Reason's famous 'Swiss cheese' model of accident causation (though see Leveson, 2012 for a broad perspective of the history of barrier approaches):

1. Organisations aim to avoid serious unwanted events by having a number of layers of protection in place between hazards and undesirable consequences or losses.
2. Layers of protection are recognised as being imperfect: which is why they are visualised as being analogous to slices of Swiss cheese – solid bodies with holes in them.
3. The holes in each layer represent weaknesses in the protection afforded by that layer. In Reason's model, weaknesses can be of four types: organisational influences; supervision; pre-conditions; and specific acts.
4. The size and position of the holes within any layer can continually change.
5. Accidents happen when the holes in all of the layers are in alignment, allowing the release of a hazard to the point where undesirable consequences occur.

The Swiss cheese model has found widespread application and is still used globally as a means of thinking about safety management. It has however been developed and elaborated in many directions: while the core ideas continue to have great value and are easily understood, variations of the model are now in widespread use. For example, figure 1 illustrates a related conceptualisation of barrier management.

The model shown on figure 1 distinguishes between threats, events and losses. At the centre of the Bowtie (the 'knot') is an event: a gas release, a fire, a child left unprotected from domestic abuse, a crowd of people forced into too small a space, or whatever the event of concern is. The left-hand side represents all of the threats that could lead to the event, while the right-hand side represents the development of the event to the point where losses are incurred (injury, damage, loss of life, reputational damage, etc).

On both sides of the bowtie, the model shows three generic types of barriers against the threats[6]. The figure shows the barriers in their order of importance, or expected strength, from left to right:

- Engineered.
- Organisational.
- Human.

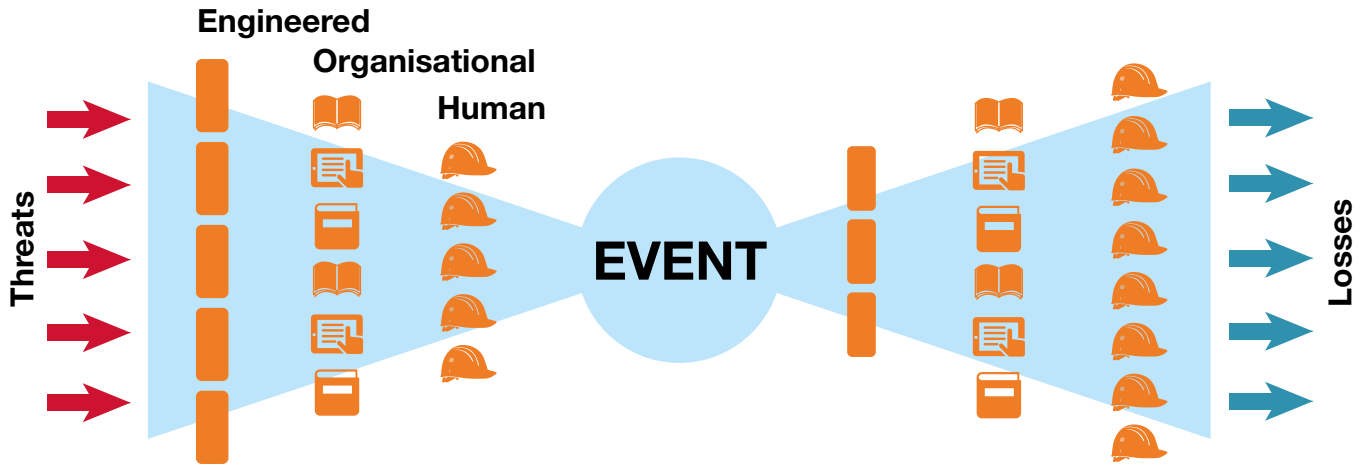


Figure 1: Conceptual model of barrier management

6. Note that there can be multiple controls of the same type.

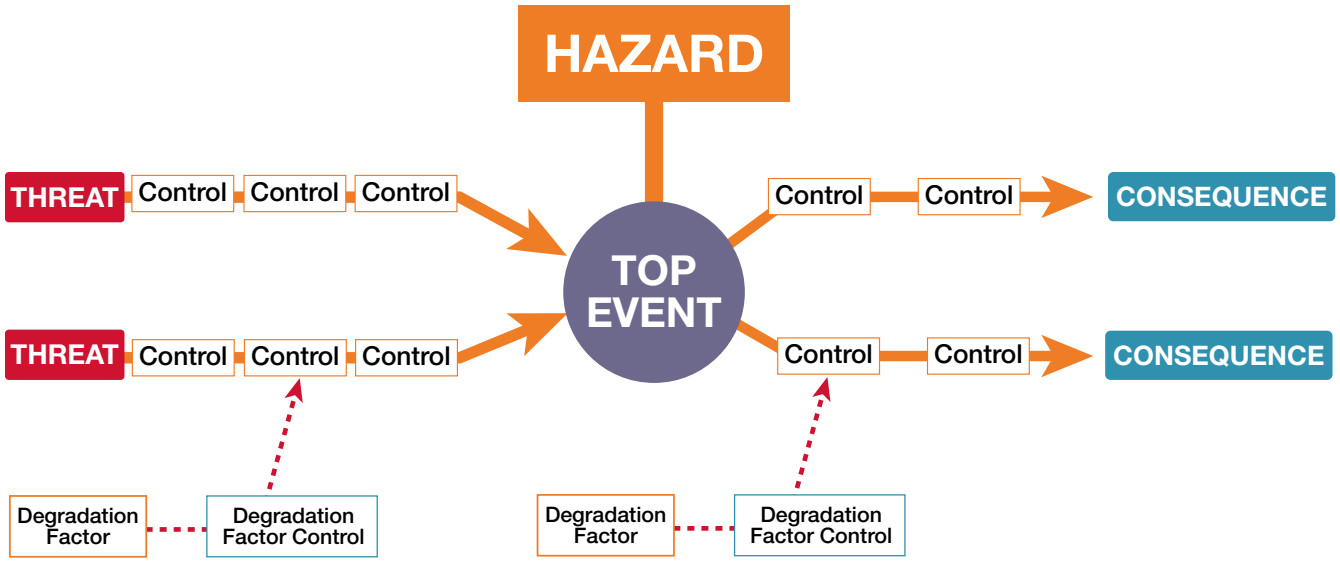


Figure 2: Elements of a Bowtie Analysis

In combination, these three types of generic barriers, with potentially multiple instances of each type, provide 'layers of defences' against threats. Human factors can defeat all three types of barrier.

2.2 BOWTIE ANALYSIS

Some techniques for analysing barrier strategies, most notably Layers of Protection Analysis (LOPA) are formalised and implemented rigorously in compliance with standards and accepted sources of industry best practice (see for example IEC, 2003, 2010; HSE 2009, 2010; CCPS, 2001, 2015). LOPA probably has the most specific guidance on how to deal with the role of people both as threats and as barriers (or protection-layers).

An alternative to LOPA that is in widespread, and growing use across safety-critical industries, is the technique of Bowtie Analysis. The Centre for Chemical Process Safety (CCPS, 2017) is publishing guidance on good practice in conducting and using Bowtie analysis. Lewis and Smith, 2010, also provide an introduction to the Bowtie Analysis method, and summarise their experience in its application to a range of safety-critical operations.

The diagrams prepared to represent the results of a Bowtie Analysis comprise a number of elements, as illustrated in figure 2.

- Each diagram is associated with a specific hazard and a single top event – one of the ways in which the hazard could be released. There can be multiple top events for a single hazard.
- Threats are events that, if they are not prevented from doing so, are likely to lead to the top event occurring.
- Controls are the defences against the threat: on the left-hand side of the Bowtie, they reduce the likelihood of the threat leading to the top event. On the right hand side, they prevent a top event, if it did occur, from leading to the consequences[7]. Controls can be technical (i.e. engineered), organisational systems or human.
- Degradation factors are things that could cause a control to fail to do its intended job.
- Degradation factor controls are things that are intended to prevent the degradation factors from interfering with the functioning of the control.

7. Sometimes controls on the left-hand side are referred to as 'control measures', while those on the right-hand side are referred to as 'recovery measures'.

In combination, the controls included in a LOPA or Bowtie Analysis are expected to be sufficient to reduce the risk to a level that the organisation – with, in some countries, influence from a regulator – is prepared to accept: i.e. to reduce the risk associated with a hazard to a level that is considered to be 'As Low As Reasonably Practicable' (ALARP); where the cost and effort needed to reduce the risk further is considered grossly disproportionate to the reduction in risk that would be achieved. When they are done rigorously, both LOPA and Bowtie Analysis provide a rich understanding of the controls that are expected to be in place and how they need to be implemented, supported and managed.

The guidance set out in this document is intended to build on, and to be compatible with, existing formal techniques. There are however some differences. For example, the necessary conditions for effective barriers defined in section 2.5 (specific, independent, effective and auditable) are consistent with existing LOPA guidance (IEC, 2003, 2010; CCPS 2001, 2015).

However, LOPA relies on quantifying the likelihood of human error[8] whereas Bowtie analysis is an essentially qualitative technique.

2.3 CONTROLS, BARRIERS AND SAFEGUARDS

Governments and organisations put in place a wide range of human and organisational measures to seek to prevent the possibility of major unplanned and unwanted events and to mitigate the consequences if they do happen. Examples include:

- Legal requirement for organisations with the potential for major accident hazards to produce a formal demonstration that they can operate safely and to ensure they comply with the measures contained in that demonstration (often referred to as a safety case, or safety demonstration).
- Development of organisational cultures where there is strong safety leadership and where everyone involved places a high value on safety and environmental performance.
- Engineering and other technical standards controlling how equipment and facilities are to be designed, manufactured and constructed.
- Operating standards and regulations setting out how operations are to be conducted.
- Contractor management and procurement standards defining how contractors and other procured items are to be selected and managed.
- HSE management systems defining the measures an organisation intends to implement to control risks to their workforce, to others affected by their activities, and to the environment.
- Procedures, work instructions, Permits to Work, etc, prescribing at a detailed level how specific operations and activities are to be carried out in the workplace.
- Emergency response procedures, defining how the organisation intends to respond in the event that an emergency occurs.
- Competence standards, defining the skills, knowledge and experience considered necessary for an individual to be appointed to a role, and how that competence is to be demonstrated, assured and maintained.
- Systems for recognising and managing the risks associated with change.

> *Controls are the defences against the threat*

- Systems for investigating incidents and ensuring that lessons are learned and fed back for continuous improvement.

As important as these measures are, most of them could not hope to meet the criteria to be considered as barriers (section 2.5 sets out criteria for effective barriers). They are nevertheless clearly important in

8. Or more accurately, failure-on-demand of human performance when it is relied upon as an Independent Protection Layer (IPL).

mitigating and managing risk, and the role they play needs to be capable of being recognised in a barrier management system. Weaknesses in any of these areas can lead both to failing to achieve the levels of human reliability that are expected and needed (i.e. for failure of the role of human performance as a barrier), as well as increasing the chances that human performance will lead to a weakening or complete failure of other controls (i.e. for human performance to act as a degradation factor).

To accommodate the role of organisational measures such as those listed above, it is necessary to distinguish between two types of controls: barriers and safeguards.

The term '**controls**' means all of the measures expected to be in place to prevent incidents. Controls comprise barriers and safeguards.

The term '**barriers**' means controls that are assessed as being sufficiently robust and reliable that they are relied on as primary control measures against incidents (See **section 5**).

The term '**safeguards**' means controls that support and underpin the availability and performance of barriers but that cannot meet the standards of robustness or reliability to be relied on as primary measure (i.e. as a barrier).

Barriers are controls that can be assured to meet minimum criteria (specific, independent, effective, and capable of being assured, see section 2.5). Safeguards, by contrast, are any form of control an organisation seeks to have in place with the intention and expectation that it will play a role in preventing incidents, but that cannot meet the same standards as barriers. Safeguards intended to mitigate against the risk of human error can range from local warnings and signs, the design and implementation of alarms and the human machine-interface to control systems, through job design, operating procedures and cross-checking practices, to the willingness of front-line personnel to stop work if they have any concerns over safety. Generally, the role of these organisational safeguards is to ensure that the barriers that are expected to be in place are not degraded or defeated by other factors – including human error.

Safeguards cannot, and do not need to, provide the same level of risk reduction as barriers (section 2.5 contains recommendations for the quality assurance of safeguards). Their role should however be recognised in any comprehensive approach to barrier analysis as ineffective safeguards can create the conditions for barrier failure or degradation.

Table 1 shows some examples of situations that would be associated with effective and ineffective human barriers.

Most of the problems shown on the right hand side of table 1 would be overcome if organisations implementing barrier management systems produced statements of the human performance that is intended and expected to deliver or support barrier functions: that is, if they developed Human Performance Standards supporting the proposed controls. A recommended means of doing this is set out in section 5.4.

Table 1

Characteristics of effective human barrier elements	Characteristics of ineffective human barrier elements
The task to be performed is clear and specific.	Task is vague or non-specific; not clear what would initiate the performance or how the operator would know whether the activity was successful.
It is clear who is to perform the function.	Responsibility for barrier performance not clearly assigned to any specific roles.
Task performer understands their responsibility and is aware of what to do, and when.	Relies on complex judgement or decision-making, especially when there is conflict between safety and performance.
Expectations about the human performance needed are realistic: a) identifying the situation that needs action; b) knowing or being able to work out what needs to be done; c) being able to do it in the time available, with the resources and equipment available, and under the likely conditions; d) having some means of knowing that the action has had the intended effect.	Range of contexts of task performance has not been considered: has only considered performance by the most competent people under good conditions.
Does not require operator to make real-time judgements that involve safety/performance trade-offs.	Does not allow for human variability: Assumes people will be fully compliant, and will perform to their best, even while busy and stressed.
Is amenable to monitoring.	Relies on operators having good Situation Awareness at all times, including awareness of the hazards and current risk profile of the risks the barrier is intended to mitigate.
Has clear characteristics that indicate if the barrier is not in place, or not likely to be effective.	Requires coordination between individuals who may have different personal or organisational responsibilities and objectives.
Criteria for work systems needed to support the function are defined and have been implemented.	No allowance for the unexpected or ambiguity.
Clear feedback on success.	Potential for conflict between what is expected for effective barrier performance and personal or organisational incentives.
Initiated by strong signals.	Relies on people identifying and correctly interpreting early signs of trouble that may be perceptually weak, ambiguous or unclear.

2.4 CATEGORISATION OF BARRIER TYPES

There is inconsistency among different users of barrier models, as well as in the published literature, about the nature and classification of barriers and their components. The following recommendations summarise how barrier elements should be classified in a way that allows proper understanding of the different roles of people in barrier systems.

1. Barriers and barrier elements can be either active or passive.

- Active barriers are reliant on the performance either of a technical control system, of people or, most commonly, a combination of both. For example, the combination of an alarm together with a human response provides an active barrier that intervenes when the conditions that cause the alarm to be raised exist and a human responds appropriately.
- Passive barriers are usually physical features or structures (walls, bunding, space, water, etc.) that are capable of blocking the progress of a threat simply by their existence. Passive barriers do not have explicit detect-decide-act functionality (although they may well rely on maintenance work to maintain their effectiveness).

2. Active Barriers must have detect-decide-act functionality – i.e. they must comprise one or more elements that allow them to:

- Detect the condition that is expected to initiate performance of the barrier function.
- Decide what action needs to be taken, and;
- Take the necessary action.

3. Detect-decide-act functionality can be inherent in a single barrier element, or can involve a combination of barrier elements working together (such as a sensor raising an alarm, a human understanding the meaning of the alarm and knowing what action to take, and then the human using a technical system to effect action).

4. Barrier elements can be either fully technical, fully human or rely on a combination of human and technical elements.

5. Human barrier elements can be either organisational or operational (PSA, 2003).

- Organisational barriers are where the organisation explicitly prescribes how decisions are to be taken, and/or what is to be done by means of written rules, instructions or procedures. Decisions and actions are taken by individual operators following the prescribed instructions. There is intended to be little room for autonomy or discretion in what is done.

- Operational barriers are those where there is no specifically prescribed manner of deciding or acting. Responsibility is left to individuals having the necessary competence to take appropriate action at the time consistent with the culture, guidance, principles and constraints set by the organisation. Operational barriers rely on individuals' skill and experience, capabilities in problem solving, decision making, and imagination, as well as team working skills including coordination and communication.

Whether organisational or operational, the role of people in assuring the performance of human barriers will take one or both of two forms:

- The barrier depends on human performance to achieve its function. For example, the calculation of mud weight in drilling, or ullage in tank management, or the operation of emergency fire suppression systems.
- The barrier depends on human performance to maintain its availability, reliability and/or survivability. For example, people may have to apply safety interlocks manually, or pipe work and vessels will be subject to periodic inspection for corrosion. Furthermore, measures of the extent and depth of corrosion will have to be maintained and remedial action taken when certain limiting values are reached. Similarly sensor systems will have to be tested and calibrated to ensure that they work with sufficient accuracy and to actuate at specified alarm points.

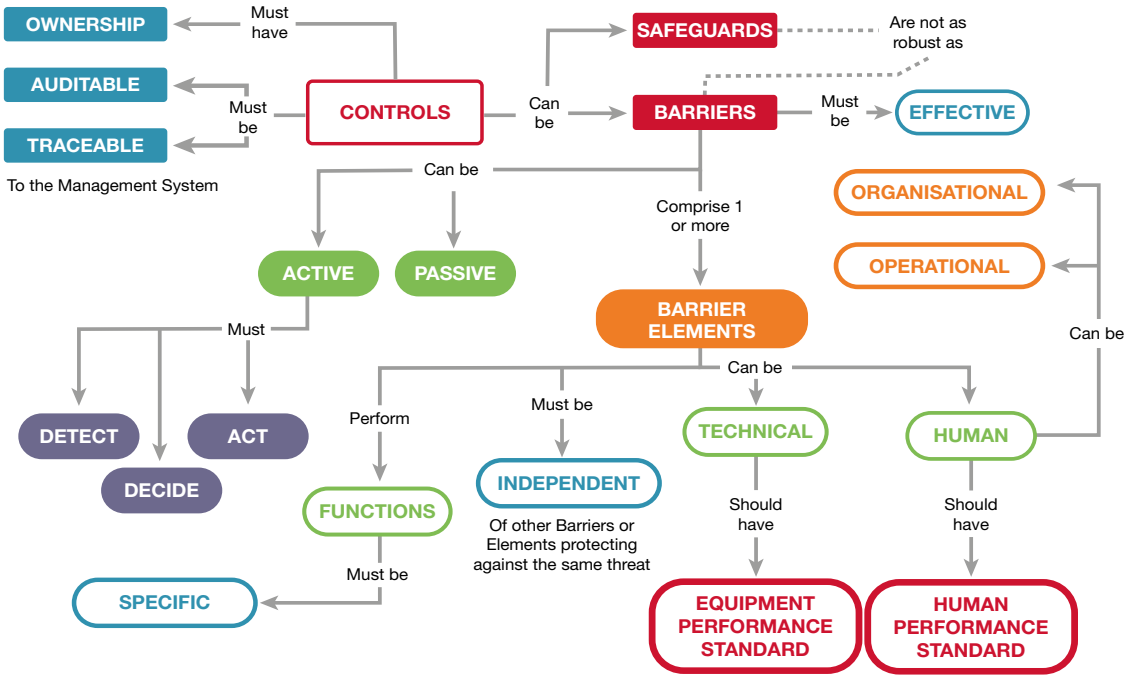


Figure 3: Summary of the relationships between components of a barrier system

2.5 ASSURING THE QUALITY OF BARRIER ELEMENTS

Potential controls, including those that rely on human performance, should be evaluated against, and should be expected to meet, at least six criteria: Having clear ownership, being traceable to the HSE management system, and being specific, independent, effective, and capable of being assured.

2.5.1 OWNERSHIP

Every control, whether barriers or safeguards, must have clear and unambiguous ownership – i.e. There must be some role or position in the organisation that has responsibility for the ongoing support and maintenance to ensure the control is in place and capable of functioning as intended when needed. That includes responsibility for the management of change associated with the controls they are responsible for. Without clear ownership, controls have no realistic prospect of being maintained effectively.

2.5.2 TRACEABILITY

Controls must be traceable to some requirement, process or activity in the organisations HSE management system. Changes to the HSE management system therefore must take account of the impact on controls at the operational front line. Similarly, changes in the implementation or operation of controls at the front line must be consistent with the content of the HSE management system.

2.5.3 SPECIFICITY

The human performance that is required for the barrier or barrier element, should be stated in a way that is as specific as possible to the threat that it is expected to prevent or mitigate. That includes three things;

- There should be a specific Actor expected to perform the function;
- There should be a specific Object in the world the function is expected to operate on, and,
- There should be a specific Goal to be achieved.

For example, an operator activity of 'monitoring' would only meet the specificity criteria if it was clear who (i.e. which role) was to do the monitoring (Actor), where they were expected to focus their attention to be able to detect the signals (Object)[9] , and what exactly the operator was expected to look or listen for (Goal). Similarly 'follow procedure' would only meet the specificity criteria for a barrier element (one that performed the Act function) if it was clear who was to follow the procedure, what procedure was expected to be followed, and what outcome was expected as a result of following the procedure. Simply assuming that there would be an operational procedure or work instruction that someone would carry out would not meet the criteria that the barrier was specific.

Note that information at this level of detail about the specific human performance that is needed for the barrier to function would not normally be available in a conventional Bowtie Analysis. It should however be contained in the human performance specification for the relevant barrier elements as recommended in section 5.4.

Box 3: The problem of operator independence

As mentioned above, many organisations place a high reliance on supervision and cross-checking, where one individual is relied on as an independent check on the performance of someone else. However, cross-checking and supervision have long been known to be unreliable.

- Decisions and actions taken at a corporate level or by senior leaders can create attitudes and incentives that undermine front-line operators' beliefs about the importance of barriers; these can range from unguarded statements in staff or shareholder briefings, reward systems, incentive schemes that emphasise production over safety, or contracts written in such a way that contractors are incentivised to find ways around the barriers and safeguards that are intended to be in place.
- In the classic 1983 study by Swain and Guttman that still provides the basis of most attempts to quantify human reliability, they said:

  " ...the checker often knows whose work it is that he is checking, or at least knows the technical level of the person who has done the work. Therefore, the behaviour of an operator and a checker are not independent. If the checker believes that the operator's work is reliable, he tends to assume that the operator's performance will be correct. This assumption and the resultant perceptual set or expectancy (what one expects to see) generally reduces the checker's effectiveness; he may miss an operator's error because he does not expect it. Even when the error is clearly visible and involves no interpretation, the checker will often fail to 'see' it." (Swain & Guttman, 1983)
- The final recommendations of the cross-industry Process Safety Leadership Group (PSLG) following the fire and explosion at the Buncefield fuel storage site in the UK in 2005, contains a rigorous discussion of the meaning of, and requirements for, independence when carrying out a Layers of Protection Analysis. In the discussion of the value of cross-checking, the PSLG noted:

  "Experience shows that the risk reduction due to checking is frequently not as great as might be expected. Operators asked to 'check' each other may be reluctant to do so, or the checker may be inclined to believe that the first operator has done the task correctly because they are known to be experienced. Therefore, the intended independence of the checking process may not in fact be achieved."

9. Note that in this example, the activity of 'monitoring' would be a barrier element, as it only meets the detect requirement for an active barrier. To be a full barrier system, the activity would need to be something like 'monitor and Intervene'. Again, specificity would be needed of what the expected intervention was.

2.5.4 INDEPENDENCE

If a single condition or event (such as relying on the same operator to cover a number of barriers) could defeat or seriously degrade the performance of more than one barrier element, then those elements are not independent; they would actually represent only a single barrier or element.

Many industries, for example, place a heavy reliance on cross-checking as a means of assuring work – i.e. where one individual is expected to carry out a check to confirm that someone else has carried out a task correctly. The effectiveness of such checks can however be degraded when the original 'doer' knows that their work will be checked and so may worry less about accuracy or avoiding errors. Similarly, 'checkers' are often not as diligent as is expected due to having trust or over-confidence in the ability of the 'doer' to carry out the task correctly first time. In both cases, the expected independence between the work performed by the 'doer' and the check is lost. Ensuring such systems maintain their independence requires being sparing in setting such checks and making the effort to ensure that both the original work and the checks are carried out independently and effectively.

> *Safeguards are any device, system or action that will likely interrupt the chain of events following an initiating event or mitigate the consequences. The effectiveness of some safeguards cannot be quantified due to lack of data, uncertainty as to independence or effectiveness, or other factors…*
>
> (CCPS, 2015).

In practice, it can be difficult to achieve genuine independence of human barrier elements (see Box 3).

Building on recommendations from the UK Process Safety Leadership Group (HSE, 2009), McLeod (2015) has suggested:

- That no two barrier elements should rely on the same people or groups of people or, if they do:
- No more than one of them should rely on any operator behaving pro-actively.
- No more than one of them should rely on any operator reacting to alarms.
- That no two people or groups of people that are relied on for the effectiveness of a barrier should have a common point of front-line supervision or direct line of management.
- That where a barrier element relies on an individual checking the actions of someone else, the requirement for the check should be documented in an accompanying procedure, and the procedure should require:
  - That the check is performed at the location where the activity being checked took place.
  - That the checker confirms the identity of the item that has been checked.
  - That the checker is able to objectively confirm the status of the item that has been checked.

2.5.5 EFFECTIVENESS[10]

Every barrier (comprising its barrier elements) on its own, should be capable of preventing an event from leading to an undesirable consequence in the circumstances likely to exist when the barrier function is needed. As long as the barrier performs as expected when needed, it will be successful in preventing the identified threat from leading to the top event. Effectiveness includes the ability to perform the barrier function in a timescale matched to the anticipated development of the threat.

2.5.6 ASSURANCE

Each barrier (and its barrier elements) should have characteristics that provide indications of its state, in order that its existence and ability to perform can be assured. Assurance can take various forms, from simple inspection, to testing or review of records.

Human barriers and barrier elements also need to be as resilient as possible. That is, they need to be capable of performing as intended across a wide range of situations where the identified threat might occur. In particular, they need to be capable of functioning to the expected standard:

- When events unfold in a way that has not been anticipated.
- In the presence of ambiguity and uncertainty about the actual state of the world.
- In the presence of stress and time pressure (especially for recovery barriers).
- Across a wide range of personality types and a range of competence (from just qualified to highly experienced).
- Where any human decision and/or action could have significant consequences for the organisation and where the individuals involved could therefore be in a position of having to make judgements that trade-off safety or environmental performance against productivity and profit.

2.5.7 CRITERIA FOR SAFEGUARDS

In general usage, definitions of the term 'safeguard' include a measure taken to protect someone or something or to prevent something undesirable, and "a precautionary measure, stipulation or device, or a technical contrivance to prevent accident". In the fields of international law, economics and politics, safeguards have a specific meaning. For example, nuclear non-proliferation is achieved through a series of 'Comprehensive Safeguard Agreements'. In these usages, the term implies a level of control that is rigorous, robust and can be assured by inspection or testing. This is essentially comparable to the standard of rigour that is expected of barriers in Bowtie analysis and other approaches to barrier management.

Safeguards should:

- Have clear ownership both within local management.
- Be directly traceable to some requirement, process or activity in the organisations wider Safety Management System.
- Be capable of being audited.

2.6 SUMMARY OF SECTION 2

The key points covered in this section are:

- The concept of having in place a number of controls to protect against incidents underpins most modern approaches to safety and risk management.
- Many, if not most, of the human and organisational elements of safety management systems that are relied on to assure high levels of reliable human performance and to prevent 'human error' from degrading or defeating barriers, are safeguards; they can rarely meet the standard needed to be considered as barriers.

10. Effectiveness is similar to what some organisations refer to as 'fully functional'.

This section sets out some important background in consideration of the role of people in barrier management.

It recognises that complex systems need to be understood as socio-technical systems, and that the causes of most significant incidents are systemic.

It recognises that rather than focusing on people as a threat that can defeat or degrade control measures, it is at least equally important to recognise that, usually, people are a significant contributor to incident-free performance.

It summarises some limitations in the implementation of barrier management and recognises the importance of the difference between formal and informal uses of barrier analysis.

The section also discusses differences in perspective between corporate and local operations that can lead to misunderstanding and confusion in the use and implementation of barrier systems.

3.1 COMPLEX SOCIO-TECHNICAL SYSTEMS AND SYSTEMIC INCIDENTS

The recommendations set out in this document focus on the management of risk in complex socio-technical systems; systems which seek to fulfill their purpose through a combination of engineered/technical and human components working together.

The term 'socio-technical' recognises that the social, cultural and technical contexts impose significant constraints and influences on the way systems function, and on what is considered acceptable system performance. Most significant incidents arise from the interaction between the many elements that make up such socio-technical systems; i.e. they are 'systemic' and need to be understood in terms of the interaction, communication, dependencies and control between different levels of the system. So any approach to barrier management must be capable of reflecting the role that elements at each level of the system hierarchy, including organisational factors, play in the performance, or degradation, of controls.

Complex systems can be expressed in hierarchical form, comprising a number of sub-systems operating at different levels of hierarchical control. For example:

A train driver sitting in the cab of a modern train is part of a sub-system comprising the immediate controls available to operate the train and the external signalling that tells the driver whether it is safe to proceed and the current speed limit.

The competence and fitness-to-work of the driver is controlled by a system that includes recruitment, selection, training, medical screening, working hours regulations and day-to-day manpower planning. Movement of the train along the network is controlled by a sub-system comprising rail tracks, signalling and control systems, and including train scheduling, procedures and regulations over train movements. All of these sub-systems are controlled by higher level systems including, among other things, corporate policies and standards, union agreements, incentive schemes, commercial agreements and government regulations.

The term 'systemic' means that, for example, the failure of a train driver to stop the train at a red light cannot be understood solely by reference to the abilities, actions and decisions of the individual driver or the signals he/she was following. Rather, understanding why the incident happened – and preventing the recurrence of future similar incidents – means understanding how factors at all levels in the system hierarchy came together to influence the performance of the individual driver in the specific circumstances and time.

The alternative to a systemic view of incidents is the view that incidents can be understood solely in terms of events and conditions within any single sub-system. Consequently, action to prevent future similar incidents can be contained within the boundaries of the individual system. For example, to change or improve the train driver or the design or positioning of the specific signal.

The evidence is overwhelmingly in supportive of the view that any serious attempt to improve safety must adopt a systemic view of incidents (Cullen, 1990; Baker, 2007; Haddon-Cave, 2009; CSB, 2016). Human Factors arise at all levels of a system hierarchy; that is the basis of the term 'Human and Organisational Factors' (HOF).

3.2 THE ROLE OF PEOPLE IN SAFETY MANAGEMENT

Much of the focus of human issues in barrier management revolves around either:

i. reducing the potential for human error to lead to top events, or

ii. the role of people in detecting, diagnosing and responding to top events that have occurred and preventing them from escalating to major incidents.

People are nearly always a positive element in complex socio-technical systems. There is growing recognition that people are often the reason operations go well despite the upsets and the everyday variability that is normal to complex activities (Reason, 2008; Eurocontrol, 2013; Hollnagel, 2014). Working flexibly to overcome over-rigid or unrealistic procedures or unforeseen events often allows effective and reliable operations. On the occasions when it doesn't, and an incident occurs, this same flexible working is frequently labelled 'non-compliance' and is seen as a problem. Well-known dramatic demonstrations of the ability of people to work flexibly in extreme and unexpected situations include the performance of Neil Armstrong in the final moments before he landed the moon-landing craft Eagle on the moon in 1969, and Captain "Sully" Sullenberger when he landed his Airbus A320 aircraft on the Hudson river in 2009 following a bird strike that caused the loss of both engines shortly after take-off.

Organisations should seek to ensure they have in place the necessary systems and support structures, and that they design and operate their activities in ways that allow people to be as productive and adaptable as they can be. Systems need to be tolerant of natural human variability and to enable people to recover from predictable failures without adverse system consequences; they need to maximise the opportunity for people to contribute to successful system performance. That can mean changing from a mindset that focuses on ensuring the risk of human error is ALARP, and towards one of ensuring operations and work systems are designed and operated in such a way that the human contribution to system reliability is 'As High As Reasonably Practical' – AHARP (Hollnagel, 2014). This has been termed 'setting people up for success'.

3.3 ORGANISATIONAL PERSPECTIVES AND THE IMPORTANCE OF CONTEXT

There are a variety of different organisational perspectives about what constitutes a good control. From an industry or corporate point of view, there is usually a need to talk in terms of approaches that are sufficiently abstracted and non-situation-specific that they can be readily applied across a wide range of operations. For example, the International Association of Oil and Gas Producers (IOGP) guidance document *Standardization of barrier definitions* includes "Operating in accordance with procedures" and "Acceptance of handover or restart of facilities or equipment" as examples of human barrier categories (IOGP, 2016). At such a highly abstracted level of description, neither of those barrier categories could satisfy the necessary conditions for being barriers (as defined in section 5).

Incidents however happen in specific circumstances and human performance (including loss of reliable human performance) is highly situation specific. The more controls are abstracted and generalised away from the local operational context, the less likely they are to meet the criteria necessary to ensure they will perform reliably when they are needed. That is true both for controls that rely on people and for those that are predominantly technological. Similarly, the factors that degrade or defeat reliable human performance are always situation and context specific.

From a human factors perspective, it is therefore essential that generalised and abstracted controls defined at an organisational level are translated into barriers and safeguards that will work reliably in local circumstances, including for the people who are expected to perform the functions.

There is little point in simply copying controls known to be reliable in a situation that is highly controlled and regulated, such as exists in most nuclear power operations, where there is usually a strong safety and organisational culture and stable, committed workforce. Such controls cannot be expected to perform as effectively in other situations such as construction sites, which, by comparison, are relatively uncontrolled, often with a largely transient and sub-contracted workforce.

Similarly, there can be significant issues in attempting to translate practices that have been developed and proved their value in an aviation context to other sectors. Examples include the way aviation uses standard operating procedures and cockpit checklists, or reliance on commercial pilots to make good decisions and perform under highly stressful emergency conditions. Such controls cannot simply be translated into a different sector without taking into account the many differences – in personality, recruitment, training (including simulator-based training in carrying out emergency response procedures), flight certification and a wide range of organisational safeguards – between commercial pilots and most other types of operation. As has been said: "those people don't work for you".

3.4 FORMAL AND INFORMAL USAGE OF BARRIER MODELS

Barrier analysis can be carried out either formally or informally. Formal use underpins an organisation's compliance expectations of those with a role in implementing or supporting the identified controls. An example is when the analysis or its products are intended to form part of a safety case or safety demonstration required either by regulators or by a company's own HSE management system. In such a formal usage, the human elements of barrier analysis should as a minimum have an adequate audit trail demonstrating that selection, implementation and verification of each human barrier (or barrier element) has followed accepted good practice, such as the recommendations set out in this document.

A barrier model is a representation of the total set of controls – both barriers and safeguards – an organisation considers necessary and sufficient to provide the required level of control over the risk of major incidents.

Barrier analysis can also be used in an informal sense. For example, Bowtie Analysis has been used as a means of exploring whether the organisation is confident it has adequate control over its major risks, though with no intention of giving the developed model a place in the HSE management system. Such informal analyses can be effective by raising management awareness of gaps in its control measures. They can also raise awareness and improve understanding of the role specific activities or operational positions play in avoiding major losses. In such informal usage, the recommendations set out in this document could be used as a point of reference to examine the robustness of the human elements of the developed barrier analysis.

When a barrier model is used in a formal sense and implemented, it is a powerful statement of intent by an organisation to its stakeholders. So an organisation should be prepared to invest the time and effort needed to properly implement its barrier model, including complying with the principles around the human elements. The extent to which this should be done formally depends on the nature of hazards and risks that need to be controlled. It will also depend on the willingness of the organisation to invest the time and resources necessary to implement and maintain effective barriers.

3.5 SUMMARY OF SECTION 3

The key points covered in this section are:

Complex systems need to be treated as socio-technical systems:

- Most significant incidents are 'systemic'. They need to be understood in terms of interaction, communication, control and dependencies between different levels of the system.
- People are nearly always a positive element in complex socio-technical systems: they are often the reason operations go well despite the upsets and the everyday variability that is normal to complex activities.
- There are a variety of different organisational perspectives about what constitutes a rigorous control. At corporate level, controls are often abstracted and non-situation specific, such that they can be readily applied across a wide range of operations. In terms of assuring the quality of barriers that rely on human performance however, controls need to be sufficiently specific to work reliably in local circumstances including for the people who are expected to perform the functions.
- Informal uses of barrier analysis can provide a great deal of value by providing awareness, insight and understanding of the controls an organisation intends and expects to be in place to prevent against the risk of major incidents. Such informal uses do not need to be capable of demonstrating the level of robustness and assurance that is expected of formal barrier management systems. Barrier models developed for informal use cannot be relied on for safety management at an operational level.
- When barrier models are used in a formal sense, barriers should be clearly distinguished from safeguards: barriers are the primary controls and must be capable of being assured to high standards; safeguards are important, but cannot be expected to meet the same standards as barriers.

32

There are many concerns about the implementation of barrier management and Bowties in particular. These include, for example: that different parts of organisations put too much emphasis on either the left (prevention) or right hand (recovery) sides of a Bowtie; that top events are frequently located too far to the right, and therefore allow too little room for recovery; that there is lack of awareness and reporting of failures of prevention barriers compared with recovery barriers; that barriers lack the resilience and flexibility needed to deal with events that were not anticipated; and that good performance of recovery barriers masks the need to improve the strength of prevention barriers. The range of opinions partly reflects different organisational experiences and the relative immaturity of formal approaches to barrier management, as well as the lack of standardisation and established industry best-practices[11].

4.1 LIMITATIONS OF BARRIER MODELS

Regulators and others recognise limitations in the reliance on barrier models in general, as well as the use of specific tools and methods such as Bowtie Analysis.

First, tools used to identify, assess and manage hazards and risks are just that – tools from the toolbox. What matters is less the integrity (validity/reliability) of the tools or methods used but that they are understood (including their limitations), selected and used appropriately. So the risk-holder must have a good enough overview of the processes and hazards under control, properly informed by operational knowledge and experience.

A particular risk is that the inputs to a barrier analysis are not realistic and properly informed about operational realities. For example, just having an experienced operator present in an analysis session is not enough. The operator needs to be enabled to contribute fully to the process through training and preparation. It is also essential that any analysis[12] session has an adequate task analysis as an input: especially during the crucial walk and talk-through of critical activities. This provides the realism that is required and generates a more realistic and complete set of events and scenarios. Facilitating a good walk and talk-through requires skill – not least in facilitation and communication – and needs preparation, practice and patience; it's not a job for everyone.

Second, a focus on controls depends on having done all the necessary screening, identification and prioritisation of those tasks and activities that are critical to the control of risk. For example, an early – and often problematic – focus only on safety-critical elements (rather than tasks and activities) in the UK offshore safety regime meant that wider critical aspects of the human element were often missed. A proper focus is needed on the totality of what people do, not just on the performance of technical systems.

There is also a risk of focusing too narrowly only on those tasks and activities directly associated with controls and not recognising the wider set of human tasks and activities that also play a critical role in safety management. Take, for example, the tasks involved in the safety-critical activity of bulk transfer (such as tanker unloading) of hazardous material. The barriers that will be identified as being associated with the transfer cannot be the limit of the organisation's efforts. They need to understand and manage the bigger picture of how people – both those directly involved in the transfer as well as those who may be remote in time, space and organisational structure – contribute to and influence the performance of the front-line activity.

Whatever activity or process is used to identify critical human activities, it is unlikely to ever be complete. If the

11. Gadd et al (2004) of the UK Health and Safety Laboratory reviewed a number of "pitfalls in risk assessment". Many of the pitfalls identified apply equally to barrier management and the use of Bowtie Analysis.

12. Task analysis is one of the most fundamental analysis techniques used in human factors and ergonomics. Generally, it refers to a variety of structured techniques intended both to identify the tasks and activities or steps that need to be carried out to achieve goals, and to understand important characteristics of those tasks and the relationship between them. Task analyses can be conducted to support a very broad range of objectives, including as the basis for the design of work systems, workplaces and user interfaces, understanding training needs and identifying the potential for human error. For an introduction to task analysis, see: https://www.usability.gov/how-to-and-tools/methods/task-analysis.html.

There are usability issues associated with current Bowtie Analysis software. Such tools are increasingly popular largely due to their ease of use and visual appeal of the models produced, as well as the ability to conveniently capture, manage, manipulate and share the data associated with Bowtie models.

Practically however, the size of the screens used to create and manipulate two-dimensional visualizations creates limits on what can be easily represented and thought about. Both maintaining an overview, as well as exploring in depth, becomes increasingly difficult as risk situations become richer and more complex.

One consequence is that, rather than thoroughly exploring the risk picture, how it is controlled and how those controls can be defeated, organisations frequently constrain their thinking, and the depth and breadth of their analysis, around what can conveniently be represented on current computer monitors. This is a practical constraint based on convenience, and can have little to do with the reality of the risks involved, and especially the role of people in managing and defeating those risks.

Sometimes paper, pen and a whiteboard, rather than the constraints inherent in any software tool, provides a better starting point for creative and expansive thinking around risk and how to manage it.

focus is defined too narrowly only around those tasks and activities directly associated with controls then important aspects of the bigger picture (i.e. the reliance on people) will be missed and, in time, the organisation will be 'surprised' by unforeseen events.

Prospective measures – such as monitoring, audit and review as part of an ongoing safety management system – need to be working well too. They need to be capable of realistic appraisal of when systems are working well, as well as detecting signs of developing weaknesses in operations and maintenance. And there needs to be emphasis not just on maintenance, inspection and testing around barriers but on all of the controls, including safeguards such as leadership and culture, the control of work, staffing and resourcing. If those wider safeguards are not also in place and effective, an organisation will always be vulnerable.

4.2 CHOOSING BARRIERS: THE BALANCE BETWEEN CONTROL AND RESILIENCE

There is a challenge in choosing barriers to achieve the right balance between controlling against threats and being resilient to unexpected events. Referring to the Bowtie model, the location of the top event, and the relative balance between reliance on left-hand side and right-hand side barriers, can be associated with many human and organisational issues. Most fundamentally left-hand side barriers emphasise compliance and control, while right-hand side barriers emphasise the resilience and flexibility of human performance. On the one hand, effort can be put into controlling operations via procedural compliance to prevent top events from occurring (focusing on left-hand side barriers), or, on the other, it can be put into building resiliency and flexibility such that, when unexpected events do occur, they don't result in undesirable consequences. What matters most is getting the balance right.

Barriers on the left-hand side of the Bowtie focus on controlling operations via procedural compliance to prevent 'top events' from occuring.

Barriers on the right-hand side involve building resilience and flexibility such that, when undexpected event do occur, they don't result in undersirable consequences.

Figure 4 uses the example of a medication overdose to illustrate some of the issues associated with the positioning of the top event, and the relative reliance on barriers on the left-hand and right-hand side of the Bowtie.

Ensuring barriers and safeguards on the left-hand side are robust and effective can be more cost-effective than relying on those on the right-hand side. For example, relying on accident and emergency services

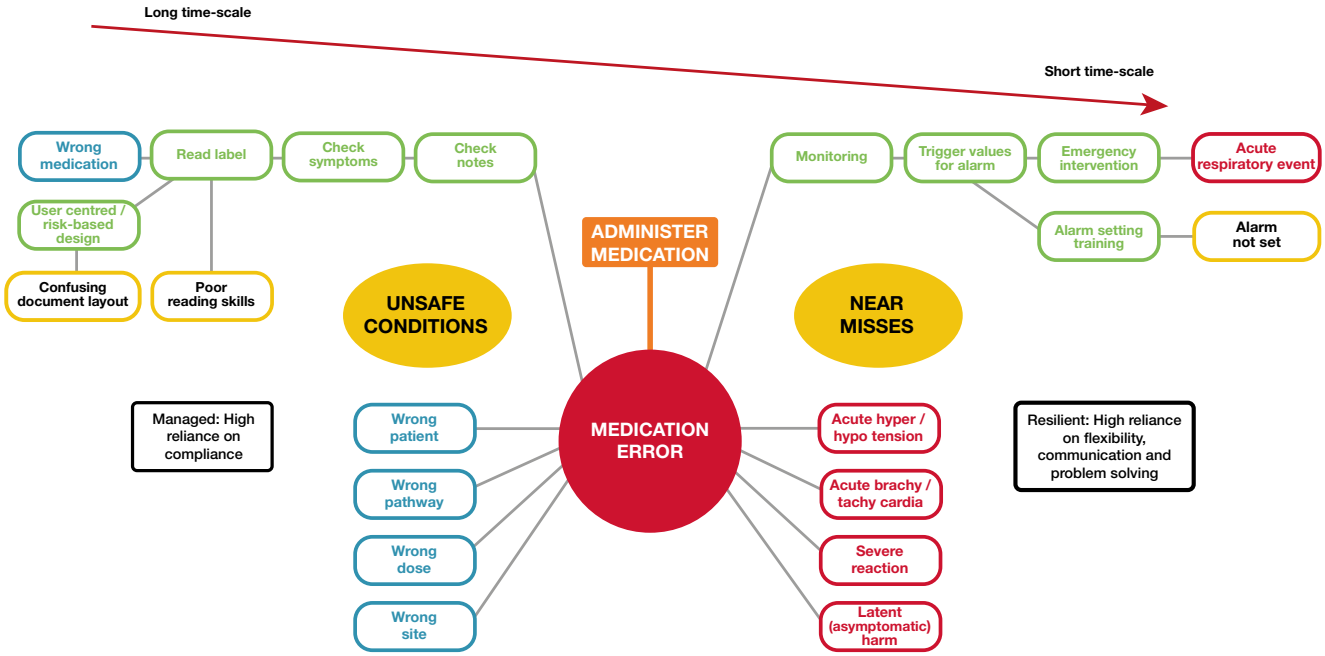


Figure 4: Locating the top event: differences between relying on barriers on the left-hand side and right-hand side for the top event of a medication overdose. (A&E = Accident and Emergency; ICU = Intensive Care Unit).

and intensive care units after a medication overdose has occurred could be orders of magnitude more expensive than ensuring the medical discipline of cross-checking prescriptions as they are written and before drugs are delivered.

An organisation with a policy of 'no incidents' is 100% reliant on barriers on the left-hand side (occurence of a 'top event' is considered an 'incident').

An organisation with a policy of 'no harm' relies on both the left and the right-hand side defences (harm only results if the right-hand side barriers fail to block the path between the top event and the consequence).

Similarly, ensuring alarm systems are well designed so that operators are made aware of what has happened and know how to respond in sufficient time, can be very low cost compared to responding to and dealing with operational upsets once they have occurred.

Figure 4 also illustrates how there is often a very different time-base between the functioning – and failure – of controls on the left-hand side compared with the right. Failure of left-hand side barriers leading to a top event often occurs over a timescale measured in days, weeks, or even years. By contrast, the time from a top event occurring to an undesired consequence will often be measured in minutes or hours. One consequence of this shortened timescale is that opportunities for identifying and intervening if right-hand side barriers fail become much more challenging, leading to a higher reliance on right-hand side barriers working first time.

A culture that has a high degree of confidence and trust in its systems and practices will tend to rely on left-hand side barriers. By contrast, a culture that has significant doubts about the robustness of the left-hand side barriers, but values its ability to solve problems and get out of trouble will tend to place a lot of emphasis on the right-hand side.

A key question for organisations that rely on Bowtie for management of major risks is: where do you spend your day?

Operating on the left-hand side means a policy of blocking threats and not experiencing the loss of control of a top event; this is a pre-emptive policy.

Operating on the right-hand side, in contrast, is to be reacting to losses of control and working quickly to prevent escalation and harm; this is a reactive policy.

There are also left and right-hand side differences in the information available from operations about the condition of barriers. Failure of barriers on the left-hand side will tend to be treated as unsafe conditions or situations. Failure of barriers on the right will usually be treated as near-misses. Near-misses are frequently under-reported compared to unsafe situations; there is often a perception of blame associated with near-misses that does not exist with unsafe situations. This can lead to a false impression that operations are conducted under greater control – more oriented towards the left-hand side – than they actually are. A final notable difference between left and right-hand side barriers lies with their respective ownership.

- Ownership of left-hand side barriers is often seen as lying with engineering and management – how the system is designed, and how operations are managed and controlled.
- By contrast, right-hand side barriers tend to rely on the skill, experience, adaptability and problem-solving capability of front-line operators – ownership of right-hand side barriers is therefore often seen as lying with operations.

Management end engineering often under-represent the right-hand side barriers and place the top event too close to the consequences. Front-line workers often know more about the recovery processes between the top event and a non-recoverable consequence (fire, explosion) than they do about the barriers and safeguards that are meant to prevent incidents.

An accurate and balanced picture of the existence, implementation and robustness of the totality of left and right-hand side controls is unlikely to be achieved without the involvement of both engineering/management and front-line staff. With more active workforce engagement, the top event is likely to move to the left.

Finally, there is an interaction between safety maturity and the use of Bowties: more mature organisations will seek to move top events to the left. They will also spend more time reporting and investigating the unsafe conditions that occur when barriers on the left-hand side fail. The maturity of an organisation is reflected in where near-misses are reported – on the left or on the right. Moving operational thinking away from responding to loss of control (emphasising right-hand side barriers) and towards preventing top events (emphasising left-hand side barriers) is a positive culture shift.

4.3 CONCERNS WITH THE TREATMENT OF HUMAN FACTORS IN BOWTIE ANALYSIS

CIEHF members have become concerned at how human performance is being addressed in some current approaches to barrier management, and in Bowtie Analysis in particular. A significant gap has developed between:

- What is known from research and experience as well as from innumerable incident investigations about the role of people in socio-technical systems, the nature of human performance and factors that contribute to loss of human reliability; and
- The expectations and assumptions about human performance – especially of those working at the operational front line – that are actually being embedded in many operational barrier models.

Eight concerns are especially important in addressing human and organisational factors in Bowtie Analysis:

1. Human error is commonly modelled as a threat, and barriers are put in place that try to block the error from leading to a top event. Indeed, human error is frequently the single most commonly identified threat in a barrier model. This focuses effort and attention in the wrong place. Effort is concentrated on trying to minimise the risk of human error rather than recognising the real barriers and ensuring they are as robust against any degradation factors – of which human error is usually only one – as they can be.

2. Equipment that is identified as performing a barrier function will typically have an equipment performance specification associated with it specifying precisely what performance is required of the equipment for the barrier to be relied on. Although Bowties frequently identify a reliance on human performance to achieve barrier functions, they rarely (if ever) specify the level of human performance that needs to be achieved for the barrier to function. (Section 5.4 makes recommendations about the content of a human performance standard for human barriers).
3. Top events are frequently located too far to the right: that is, the events that barrier systems seek to avoid by means of prevention barriers are too close in time to the consequences (fatalities, losses, etc) that those events can lead to. So while preventative barriers (those on the left-hand side) typically operate over a timescale that can be measured in weeks, days and hours, mitigation barriers (those on the right-hand side) typically have to operate in a timescale of hours and minutes. This can create pressure for people to perform to extremely high standards in situations of both stress and time pressure.
4. Too many 'barriers' are identified, most of which are not able to meet the generally accepted criteria for robust barriers (section 2.5). While they have a role as 'safeguards', they should not be confused with the principal barriers that need to be capable of being relied on.
5. Barrier models rarely take a systems view of the human and organisational factors associated with the threats they are trying to control. They rarely recognise the influence that a wide range of organisational factors – such as leadership, culture, incentive schemes, commercial arrangements, or contactor management – can have on the performance of people at the front line.
6. There is often a lack of understanding of the nature or complexity of the tasks – and especially the cognitive elements of those tasks – that need to be carried out for barriers to function as intended. Because of that, organisations frequently hold unrealistic expectations about what people will be able to do, and how they will actually perform, in the circumstances that exist when barriers need to function. Box 4 gives an example of such unrealistic expectations. Unrealistic expectations

Box 4: Unrealistic expectations of the human performance

The US Chemical Safety Board investigated the human and organisational factors associated with the loss of the Deepwater Horizon drilling platform in the Gulf of Mexico in 2010. Central to the findings were unrealistic expectations held about the ability of the crew, in the event of a "kick" from the well, to use the systems provided to divert the gas overboard. Doing so would have avoided the potential for an explosion.
Expectations about human performance included:

- That the crew would detect gas influx into the "riser" soon after it occurred.
- That they would quickly realise that the gas was of sufficient volume that it would need to be diverted overboard.
- That they would quickly complete the correct sequence of actions to send the gas overboard.

In reality, operating practices, the multi-step process involved and the cognitive complexity of the decisions and actions involved in the severe lack of time available made it unrealistic that any crew would have had a realistic chance of taking the expected action in time. In addition, the CSB concluded that both regulatory and financial issues could have incentivised the crew not to do what it was expected they should have done.

can be avoided by conducting task analysis, to understand what operators will actually need to do for barriers to perform as intended.

7. There is often a lack of awareness of the difference between "work-as-imagined" and "work-as-done" (Hollnagel, 2014). "Work-as-imagined" reflects an idealised, office-based view of how tasks and processes are to be performed without recognising the many situational factors – established work practices, practical difficulties, uncertainties, competing goals and stresses – that exist in reality at the front line. "Work-as-done" captures the reality of how work is actually done, including the compromises and adaptations made when carrying out tasks under real-world constraints and pressures. The intentions and expectations of human performance that are implicit in the decision to rely on people as part of a barrier system are rarely made explicit. They are therefore not communicated to those that need to implement, perform, support or maintain barriers.
8. Barrier models are often prepared, implemented and distributed to the workforce in a manner that does not properly support their operational use. The individuals assigned to carry out tasks, or whose performance is expected either to act as a barrier, or to ensure a barrier is capable of functioning, are frequently unaware of the significance of the task or their assigned role. Similarly, they are unaware of the importance of reporting when they are unable to perform in the expected way or to the expected standard.

4.3.1 WHAT IS WRONG WITH TREATING HUMAN ERROR AS A GENERIC THREAT?

One of the main concerns noted in section 4.3 with much current practice in Bowtie Analysis is in treating human error as a threat, and focusing on putting in barriers to try to block the error from leading to a top event. Effort is concentrated on trying to minimise the risk of human error rather than recognising the real barriers and ensuring they are as robust against any degradation factors as they can be.

Producing a Bowtie Analysis that shows barriers against the threat of generic human errors out of context can not only lead to a seriously false sense of security, but can interfere with attempts to create a positive safety culture. By marginalising people and focusing on the relatively few occasions when people make serious mistakes, representing human performance as a threat sends a fundamentally negative view of the role of people in process safety management, which can adversely impact development of a strong safety culture. The focus goes on optimising technology, leaving people, reluctantly, with whatever is left over. Such an attitude conflicts with the user-centered view of socio-technical systems that underpins the professional discipline of human factors and ergonomics.

This approach also misses the opportunity to build flexibility and adaptability into systems through a deeper understanding of the ways people contribute to resilience and avoid undesirable consequences.

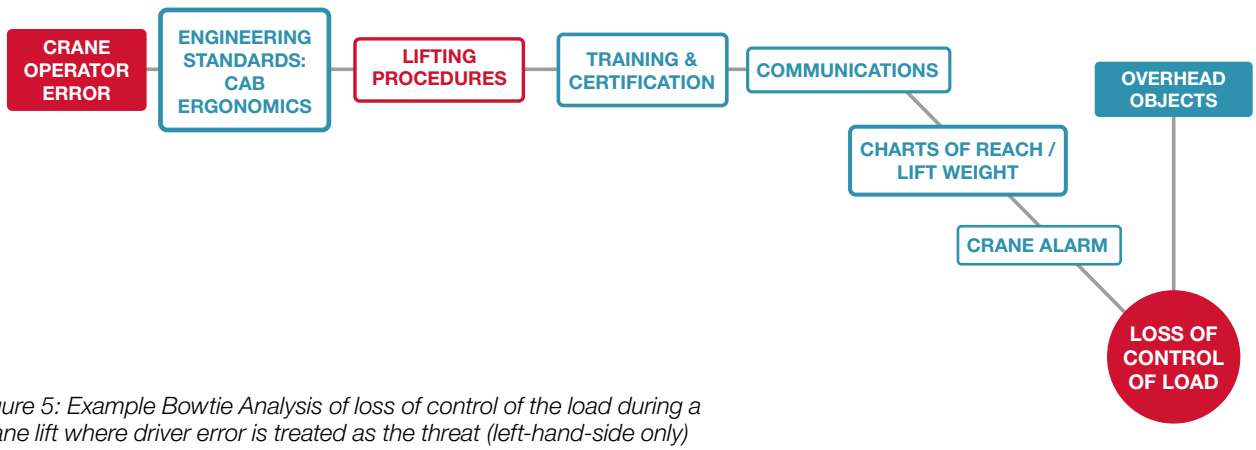


Figure 5: Example Bowtie Analysis of loss of control of the load during a crane lift where driver error is treated as the threat (left-hand-side only)

The alternative is to recognise the real impact of human error: which is to defeat or degrade other barriers. Rather than focusing on the human error, attention should be directed towards improving the inherent strength and resilience of the barrier(s) that the error could defeat or degrade.

In some situations, an analysis specifically sets out to explore barriers against the risk from a particular human error. Examples include where there is a need to explore user interface designs that are tolerant to specific types of error, or to explore disturbed or destructive behaviour to combat malicious acts or terrorism. Such cases are understandable, and common, however, the analysts should be clear that in preparing such a human-error Bowtie, they are not addressing the principal barriers in their safety management system. Rather, they are focusing on only one mechanism by which – usually – one main barrier can be degraded or defeated. In a formal use of Bowtie Analysis, such a human-error specific analysis should not be considered as sufficient to ensure there is adequate protection in the form of barriers against the top event in question.

An example: Treating crane operator error as a threat

The following examples illustrate both the incorrect, and recommended treatment of human error in Bowtie models. Figure 5 shows the left-hand side of a Bowtie that was created by an organisation concerned about the risk of a crane driver making an error resulting in the loss of control of a heavy weight during a lift. In this analysis, the hazard is the overhead object during the lift, and the top event is loss of control of the object during the lift. The threat is considered to be an error by the crane operator in attempting to lift an object that exceeds the crane's capacity.

This analysis (which is based on a real example), shows six 'barriers' expected to prevent crane driver error from leading to the loss of control of the object being lifted. With the exception of the lifting procedure, none of these 'barriers' could meet normal industry criteria for robust and valid barriers (see section 5): they are safeguards, not barriers. (Note that 'crane alarm' could be considered a valid barrier if it was re-phrased as 'crane alarm and operator response', thereby

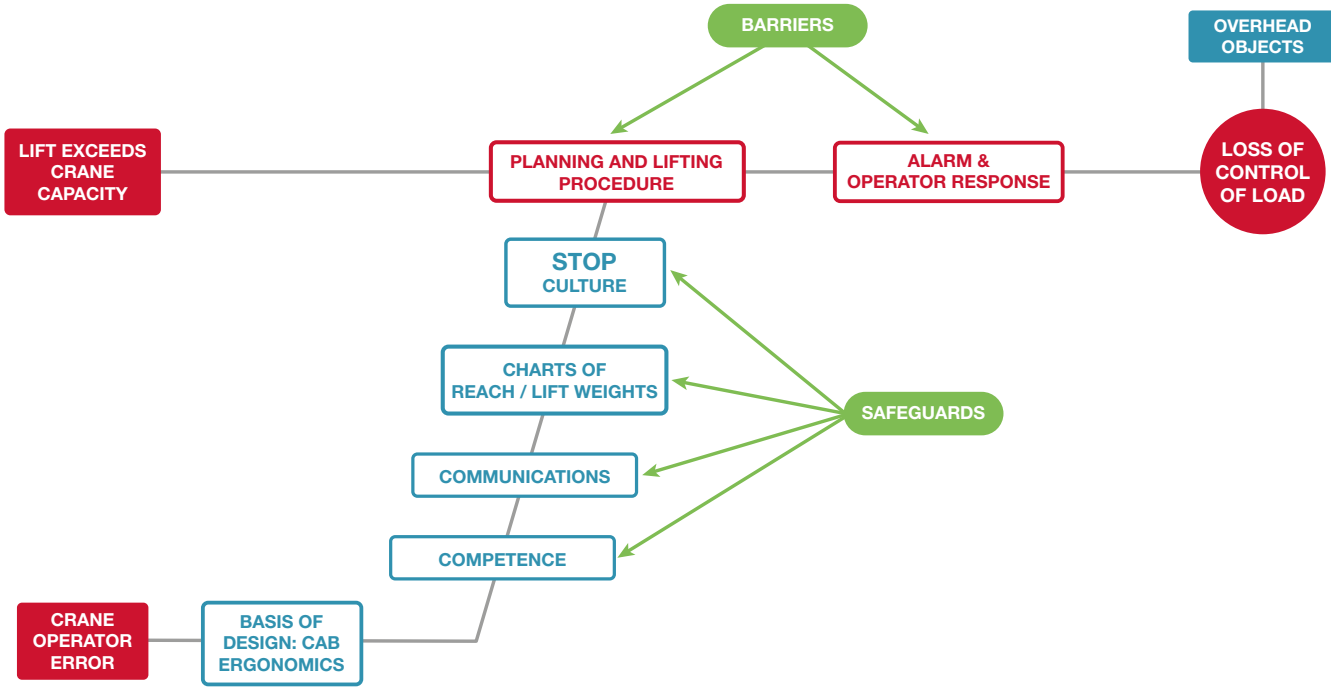


Figure 6: Example Bowtie Analysis of loss of control of the load during a crane lift where driver error is treated as a degradation factor leading to loss of effectiveness of the lifting procedure as a barrier (left-hand-side only).

meeting the detect-decide-act requirement for an active barrier – see section 5).

Figure 6 shows an alternative treatment of the same top event. In this treatment, the threat has been generalised to the situation where the lift exceeds the crane's capacity, rather than focusing solely on crane driver error (it could, for example, be a result of the organisation responsible for the lift being misinformed about the weight of the object being lifted as a result of miscommunication from the object supplier, due to missing or incorrect paperwork, or other factors). In this treatment, an error on the part of the crane driver is seen as one of potentially many factors that could defeat or degrade the effectiveness of relying on a standard operating procedure as a barrier. Figure 6 also shows a number of safeguards (driver competence, communications, etc) that may be put in place to prevent crane driver error from degrading the effectiveness of the procedure performing as a barrier.

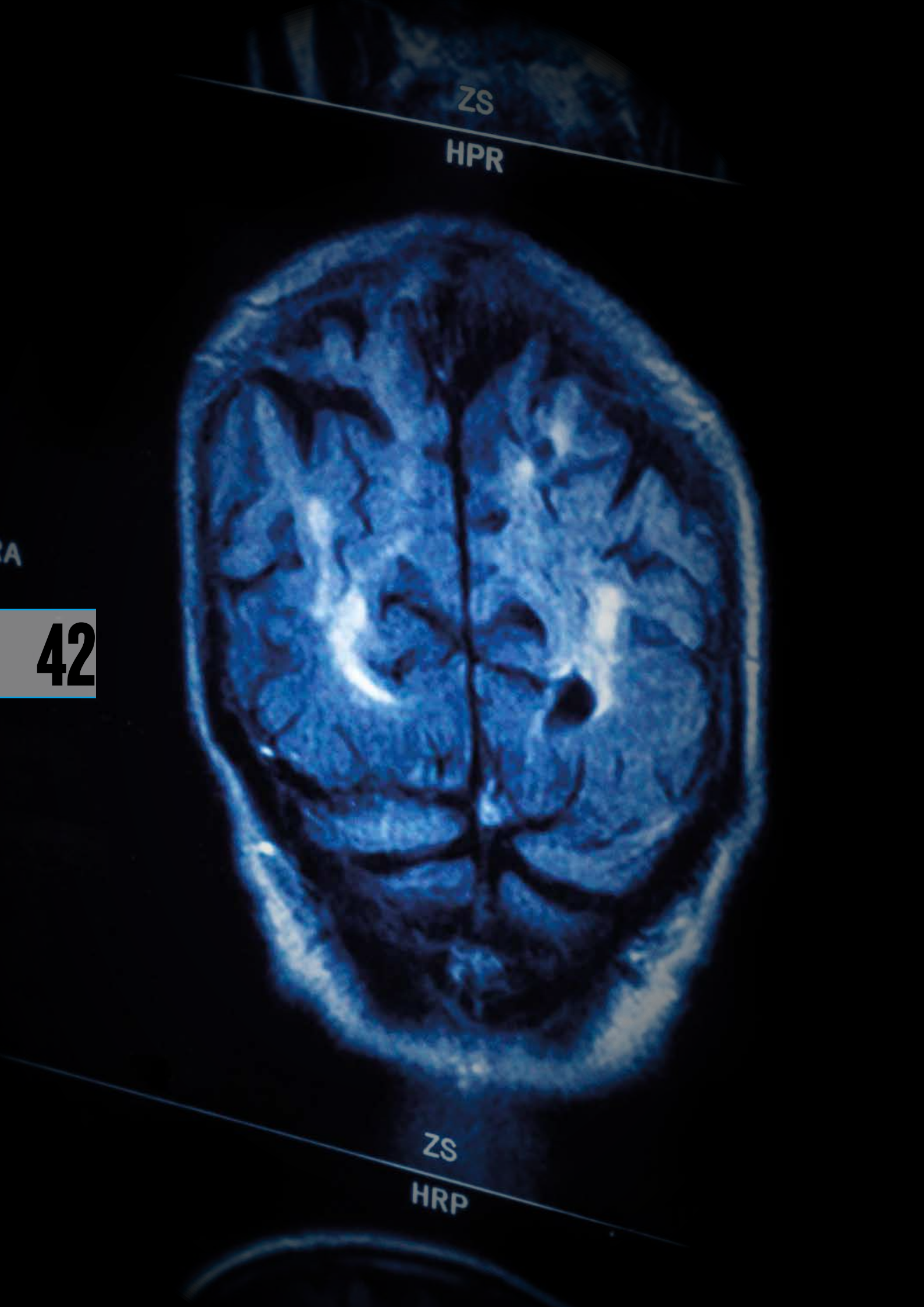
Figure 6 shows two barriers. The first ('planning and lifting procedure') comprises two barrier elements ('planning', and 'lifting procedure'. Both of these elements would be considered organisational in that the organisation has prescribed in advance precisely how each activity is to be carried out, with little discretion left for operator judgement. The second barrier comprises two elements ('alarm' and 'operator response'). The first of these is technical. The second could be either organisational – if the action the operator is expected to take when the alarm sounds is fully prescribed in advance, or operational – if the prescription was left at a high level (such as 'bring the lift to ground as quickly and safely as possible') and the driver had to use their skill and judgement to decide precisely what action to take to achieve the objective.

Finally, figure 6 also shows crane driver error identified as a degradation factor that could lead to the defeat of the 'planning and lifting procedure' barrier. Five safeguards are shown that are expected to prevent crane driver error from leading to failure of this organisational barrier.

4.4 SUMMARY OF SECTION 4

The key points covered in this section are:

- While approaches to safety based around barrier management have a significant role to play in safety management, they, alone, are rarely capable of capturing the full range of human and organisational factors that need to be in understood and managed to provide acceptable levels of safety assurance.
- The relative location of the top event between the threat and the consequences to a large extent determines the nature of the human and organisational issues the organisation needs to focus on. Careful attention needs to be given to getting the right balance between controls that prevent top events and having the resilience to respond to them when they do occur.
- The UK human factors professional community has a number of concerns about how the role of people in barrier systems is currently being addressed.
- Human error should not be modelled as a generic 'threat' at the top level of Bowtie models. Human error should be modelled as an event that has the potential to defeat or degrade main threats to barriers. Organisations using barrier models should focus attention initially on identifying the main controls and ensuring they are as robust as they can be to degradation by any factors, including human error.



42

This section sets out 33 recommendations intended to improve the development, implementation and management of those aspects of barrier management systems, and particularly those based on Bowtie Analysis, that rely on human performance or are intended to protect against loss of human reliability.

The recommendations reflect the scope as defined in section 2. That is, they are concerned with situations where: i) the identification, implementation and management of barriers is based around the use of Bowtie Analysis; ii) the resulting Bowties are used formally and are expected to be implemented and used to manage safety of real-time operations.

The recommendations build on the considerations and concerns discussed in sections 3 and 4. While they do not provide comprehensive coverage of all of the issues that need to be considered, they provide the basis for a step improvement in current approaches to managing the Human Factors aspects of barrier models.

Recommendations are organised into five topics:

1. General policy around the treatment of and attitude to barriers.
2. The categorisation of different types of barriers and barrier elements and their characteristics.
3. The lifecycle of the development and use of human barriers, including selection, verification, implementation and assurance.
4. Criteria to ensure human barrier elements, as well as the human performance that is relied upon for technical barrier elements to function, are sufficiently robust that they can be relied on.
5. The contents of a human performance standard for human barrier elements.

The section also describes a recommended approach, using progressively more detailed Bowtie models, that can be used to explore the implications of human error on barrier performance, and the safeguards that are relied on to assure human reliability.

5.1 POLICY

1. All barriers should be considered to be critical: they must be capable of being demonstrated to meet the minimum criteria necessary to be recognised as a barrier (see section 5.5).
2. Anything that is relied on to provide assurance that operations will be performed safely, but that does not meet the criteria for a barrier should be treated as a safeguard (see section 3.5).
    a. Safeguards should not be relied on to block the main threat line between threats and top events, or between top events and consequences;
    b. Safeguards can be included as a means of preventing barriers, whether human or technical, from being defeated or degraded.
3. Failure of a single organisational safeguard will often defeat or degrade many barriers. While they do not have the robustness of barriers, safeguards must be treated as seriously in development, implementation and assurance as barriers.
4. Barriers should be considered as barrier systems: i.e. in nearly all cases, for barriers to perform as expected, a combination of elements need to perform their individual functions in a coordinated manner[13]. The functionality and performance of barrier elements needs to be identified, understood and managed in their own right.
5. Human performance needs to be represented in barrier models in two distinct ways:
    a. As one type of barrier, or one element of a combined human/technical barrier system.
    b. As a factor that can degrade or defeat barriers.
6. It is a mistake to assume that risk is not increased, or that control over the potential for a major incident has not been compromised when a barrier is known not to have functioned

13. As an example, instrumentation in a car may detect the fact that brake pads are worn and raise an alert to the driver. The driver needs to recognise the significance of the alert and take the car to a garage to have the brake pads renewed. Each of these is a barrier element, with the overall barrier being to detect and intervene in response to the threat of worn brake pads.

or not to be serviceable based on the belief either that other barriers must have worked, or will work. An organisation that encourages or supports such thinking could be considered to have an immature safety culture.

7. Failure of any barrier or barrier element to perform its function, or to be identified as being unlikely or incapable of performing its function when demanded, should therefore be treated as a significant event. Whether they occur on the left-hand side of a Bowtie (i.e. between a threat and a top event), or on the right-hand side (i.e. between the top event and the consequences), they should be investigated, at least, as a near-miss in terms of incident reporting. (Note that this is already the case in industries such as aviation and air traffic management, where, for example, a loss of aircraft separation is treated as a significant failure and is investigated).

5.2 LIFECYCLE

SELECTION

Selection refers to the first pass at identifying potential human performance requirements to perform or support barrier functions. The key human factors decision to be made is whether the human performance required for the barrier element to perform its function is worth considering as an organisational or an operational barrier element.

8. The performance needed to deliver the required functionality should be capable of being described clearly: i) what state or events would initiate the performance, ii) what task(s) are involved in carrying out the function, and iii) when the function has been achieved;

9. The performance needed should be consistent with the job design of the individual(s) expected to be assigned responsibility for it. As well as being appropriate to the skills, knowledge, experience and responsibilities of the individual, it should be consistent with their values, and perceived status. For example, expecting highly qualified and trained individuals in senior roles – who are typically valued for their critical thinking and real-time problem solving capabilities – to blindly follow a written procedure is unlikely to meet with long-term success.

10. It should be clear whether the suggested control is capable of meeting the standards needed to be treated as a barrier, or whether it would be better managed as a safeguard.

VERIFICATION

Verification refers to the review of suggested organisational or operational barrier elements to ensure they are suitable – assuming they are correctly implemented and assured – to be relied on as human barrier elements. The decision to be made is whether the proposed human performance is considered to be sufficiently robust to be included as a barrier/ element.

11. The responsible organisation should satisfy itself that the proposed human barrier elements are capable of meeting the criteria defined in section 5.4.

12. Expectations about the standards of human performance and reliability that are needed for a barrier to perform its function should be reasonable and realistic, taking into account:

- The range of scenarios when the barrier function may be needed.
- The circumstances that can be anticipated to exist in the most demanding scenarios, and,
- The abilities of the least capable member of the workforce who may be assigned responsibility for the barrier, including on a temporary basis.

13. Human barrier elements, whether organisational or operational, should have an associated Human Performance Standard. (Section 5.4 makes recommendations for the content of a Human Performance Standard).

14. Both human barrier elements and degradation factors involving human error

14. Ellis and Holt (2009) describe a process for carrying out Human-HAZOP for critical procedures.

should be subject to Critical Task Analysis. The analysis should be sufficient:

a. To provide the basis of the Human Performance Standard for the barrier element, and;

b. To ensure the characteristics and situational factors associated with the human error are sufficiently well understood such that a) safeguards necessary to mitigate the potential for the error can be implemented, and b) the effectiveness of those safeguards can be assured.

15. The performance needed for the barrier/ element to perform its function:

    a. Should be amenable to training, assessment and continuous reinforcement.

    b. Should not rely on individuals making complex decisions or judgements that could involve trading off safety or environmental control against production. (If such decisions or judgements are unavoidable, the control is unlikely to achieve the standard required of a barrier, but should be treated as a safeguard).

16. Expectations about what it is reasonable to expect of people involved in performance of the barrier function should be subject to review by experienced operational personnel.

17. Where organisational barriers rely on compliance with procedures, a task analysis and walk-through/talk-through of the procedure should be conducted followed by a Procedural HAZOP[14].

IMPLEMENTATION

Implementation refers to the process of implementing barriers in the operational environment in such a way that the likely performance of the barrier is not degraded by the environment, work systems or organisational or commercial arrangements.

The key human factors decision to be made is whether the human barriers have been implemented in such a way that they are likely to perform as expected when needed.

18. Individuals who are expected to perform barrier functions must be aware of their role, why the barrier is needed, and understand what is expected of them for the barrier to work.

19. Each barrier should have a single 'owner' – i.e. the person who is responsible for the barrier performance. Where the owner is not also the individual expected to perform the barrier function, the owner should have direct line management responsibility for that individual.

20. While one individual or role needs to have ownership, responsibility needs to be capable of being delegated or transferred to others, either for short (e.g. lunch breaks) or longer term.

21. There should be some inherent incentive to do what is expected that forms a natural part of the job. Barrier owners should derive some benefit by performing the function as expected, and not see the task simply as burdensome. Benefits can include making it easier to achieve work objectives or achieving personal targets.

22. Performance incentives – both personal to the operators and commercial agreements of the organisation - should be consistent with and supportive of performance of the barrier. There should be no personal or commercial incentive that would lead to the required barrier performance being given a low priority.

23. Tasks involved in performing a barrier function should not be unduly demanding, difficult or likely to expose the individuals to excessive physical or emotional strain (e.g. embarrassment); there should not be an easier way to perform the task than the manner prescribed in the barrier definition.

24. The required barrier performance should be consistent with the equipment, facilities and other resources available in the immediate vicinity of the individual, or accessible within a timescale that is consistent with the time available for the barrier to be effective.

RECOMMENDATIONS

ASSURANCE

Assurance refers to the process of confirming that the working environment, work systems and operational and commercial arrangements are managed and maintained in such a way that the assumptions made about the ability of operators to carry out barrier functions successfully and for safeguards to perform as expected continue to be valid; that is, that 'work as done' has not deviated significantly from the way it was understood when the barrier was implemented.

The key human factors decision is whether the conditions necessary for effective performance of organisational and operational barriers are being maintained and assured in the workplace.

25. Individuals assigned responsibility for barrier performance need to have adequate opportunity to perform the task and to practice the skills needed under realistic conditions.
26. There should be clear lines of responsibility and accountability for the ongoing assurance of the capability to deliver barrier functions.
27. There must be a culture where operators expected to perform barrier functions are willing and able to call "Stop!" if they do not feel capable of performing the barrier function at any time.
28. There should be feedback available within the natural job process about the standard of performance achieved.
29. There should be clear indicators, available during training, at the front line where the barrier is expected to perform as well as to immediate line management, if the individuals expected to perform the barrier function are incapable or otherwise unable to perform the expected activities at a time when the barrier is expected to be operational.
30. Learnings from incidents, as well as other

operational experience should be used to review, maintain and improve the strength and resilience of human barriers. That should include reviewing what works well, as well as failures.

5.3. THE USE OF LAYERING TO MODEL HUMAN ERROR

Many organisations want to give special attention to the risks associated with human error. Bowtie analysis, and the software products supporting it, provides a convenient and highly visible conceptual framework for doing so.

31. Where that is the case, a layered approach should be adopted with bowties at lower levels being developed to give progressively more detailed attention to how human error can defeat barriers, and the safeguards that need to be in place to mitigate against it[15].

    a. For convenience, in such a layered approach the top level, or main level Bowtie, should be considered 'Level 0', and each progressively more detailed human error Bowtie should be labeled level -1, -2, etc.

Figure 7 illustrates the concept of layered Bowties. The figure shows a main Bowtie (Level 0) where human error has been identified as a degradation factor for Barrier 2. Two progressively more detailed levels are shown (Levels -1 and -2) developing more detailed understanding of the risk from human error and the safeguards that are relied on to mitigate that risk.

At Level -1, the hazard is the top event from Level 0 and the top event is the failure of Barrier 2. And at this more detailed level of analysis, human error can correctly be represented as a 'threat' to the performance of the barrier that is the focus of this level of analysis.

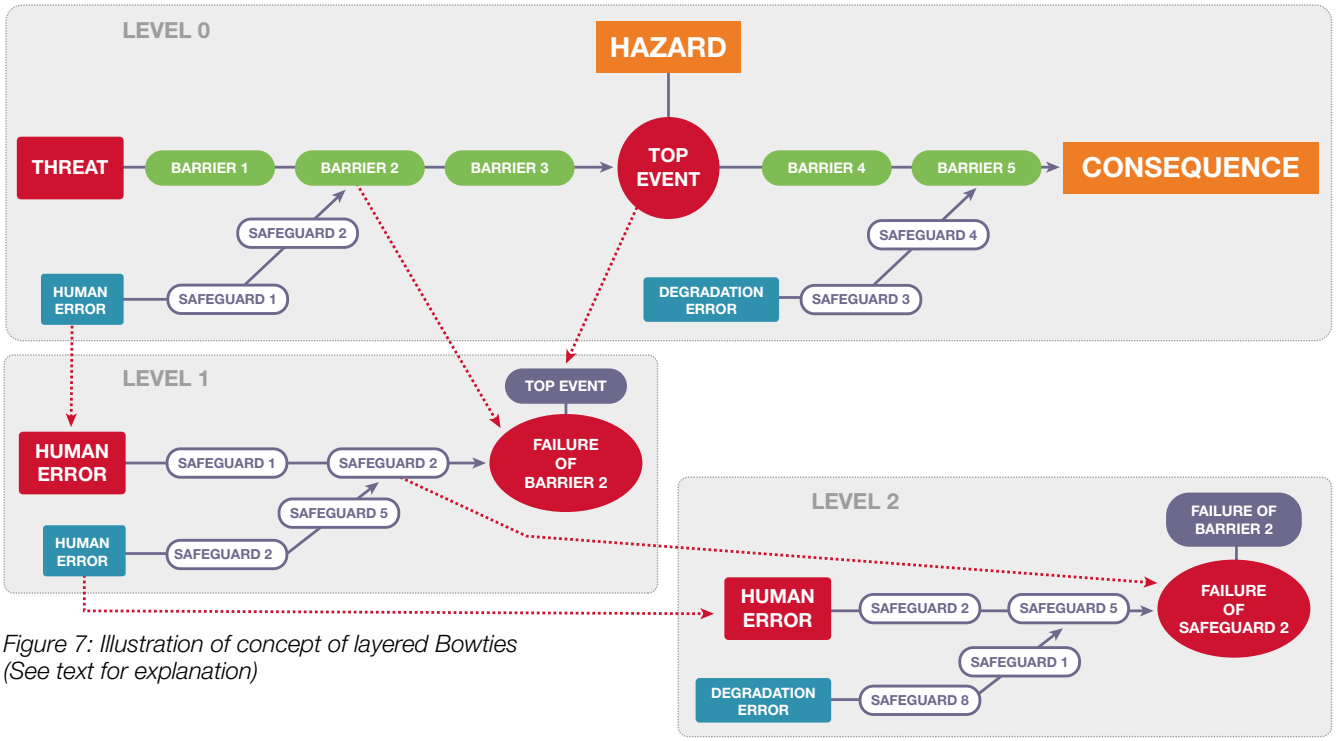


Figure 7: Illustration of concept of layered Bowties (See text for explanation)

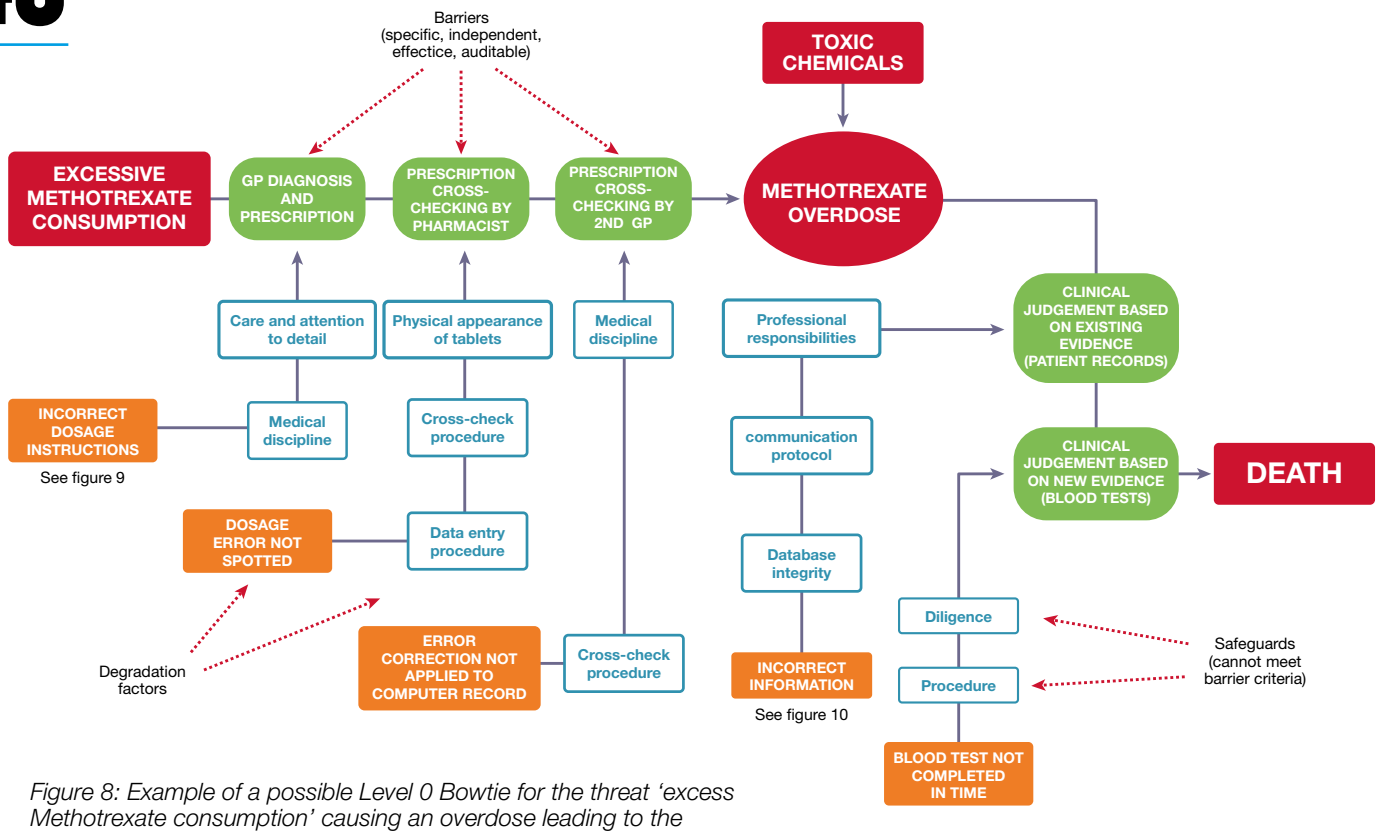


Figure 8: Example of a possible Level 0 Bowtie for the threat 'excess Methotrexate consumption' causing an overdose leading to the death of a patient. (Note that the controls in green are barriers. Those in white are safeguards).

There are a number of observations arising from consideration of figure 7:

i. The same safeguards can exist at any level of the analysis. For example, a safeguard of 'barrier awareness', or 'STOP culture' could occur anywhere in the hierarchy, and on either side of the Bowtie. This will lead to a degree of repetition when diagrams are viewed collectively. Because of this, some organisations prefer to remove these human factors safeguards from individual Bowties and either show them on a 'generic human factors Bowtie', or treat them elsewhere in their safety management system. Making them explicit in lower level Bowties however has the significant benefit of creating visibility of the ways in which these generic human factors safeguards are relied on to protect against very specific threats.

ii. The number of levels of analysis is at the discretion of the organisation. In many situations a two-level layered analysis might be adequate (i.e. Levels 0 and -1). Where there is a deeper concern about loss of human reliability however, it may be appropriate to take an analysis to three or more levels, to explore the reliance on human and organisational factors and the nature of the safeguards that need to be in place in more detail.

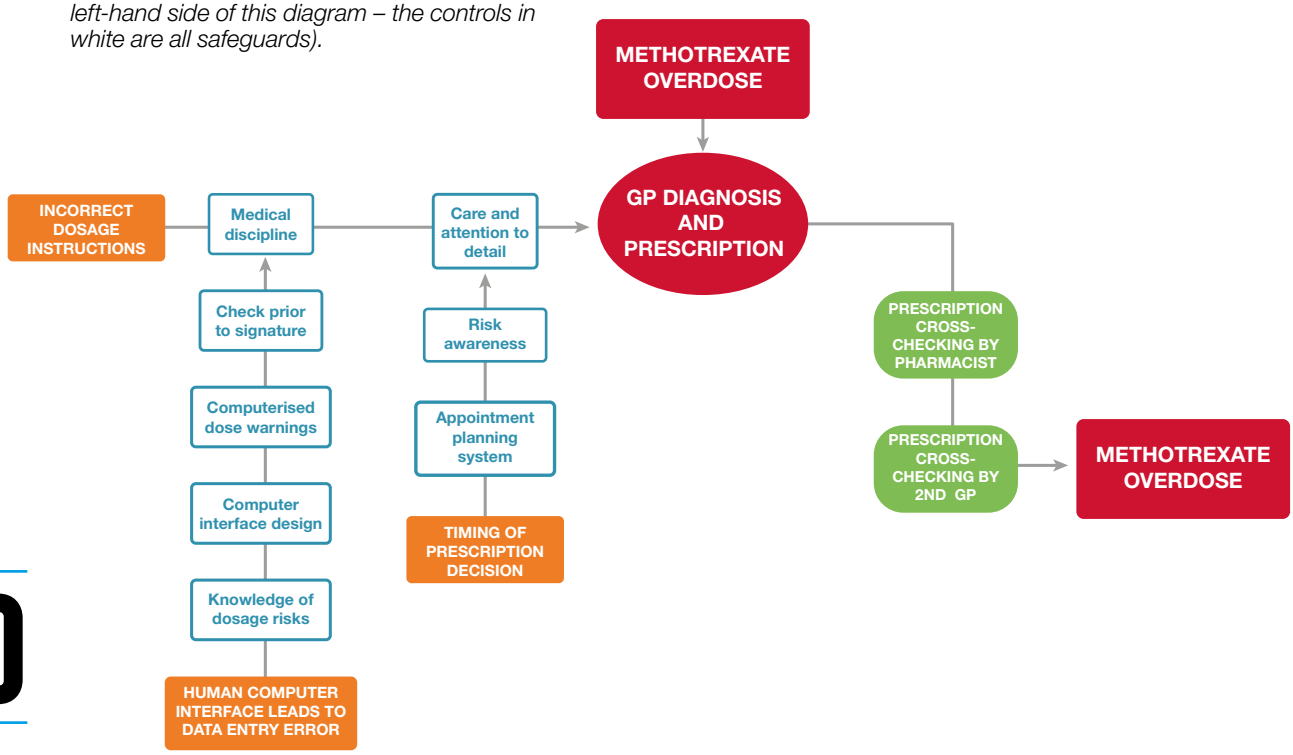
iii. There could in principle be multiple diagrams at Levels -1 or lower: i.e. each degradation factor at any level may have an associated analysis at the next lower level. It will usually be more useful however to develop threads exploring concerns over individual human errors, and identifying the safeguards that are relied on against them, to progressively lower levels of detail.

To illustrate the use of such a layered approach to explore human error and its safeguards, figure 8 shows an example of layered bowties using the incident of over-prescription the drug Methotrexate that led to the death of a patient that was summarised in Box 1[16]. Figure 8 shows a possible top-level diagram (Level 0) for the threat of overdose from Methotrexate. Figures nine and ten show an expansion at level -1 for two of the degradation factors shown at Level 0: a) 'Incorrect dosage instruction' leading to failure of the barrier 'GP Diagnosis and Prescription', and b) 'Incorrect Information', leading to failure of the barrier 'Clinical judgement based on existing evidence'. Note that only the five controls shown on figure 8 (in green) are considered capable of meeting the criteria to be treated as 'barriers'. All of the other controls are 'safeguards'.

15. A similar layered approach has been suggested by the Centre for Chemical Safety (CCPS) in its forthcoming book on Bowtie Analysis.

16. Note that the examples developed here are illustrative and do not capture the full extent of the issues involved in the incident.

Figure 9: Example of a possible Level -1 Bowtie examining the safeguards to protect against the human error 'Incorrect Dosage Instruction' defeating the barrier 'GP Diagnosis and Prescription' (Note: there are no barriers on the left-hand side of this diagram – the controls in white are all safeguards).



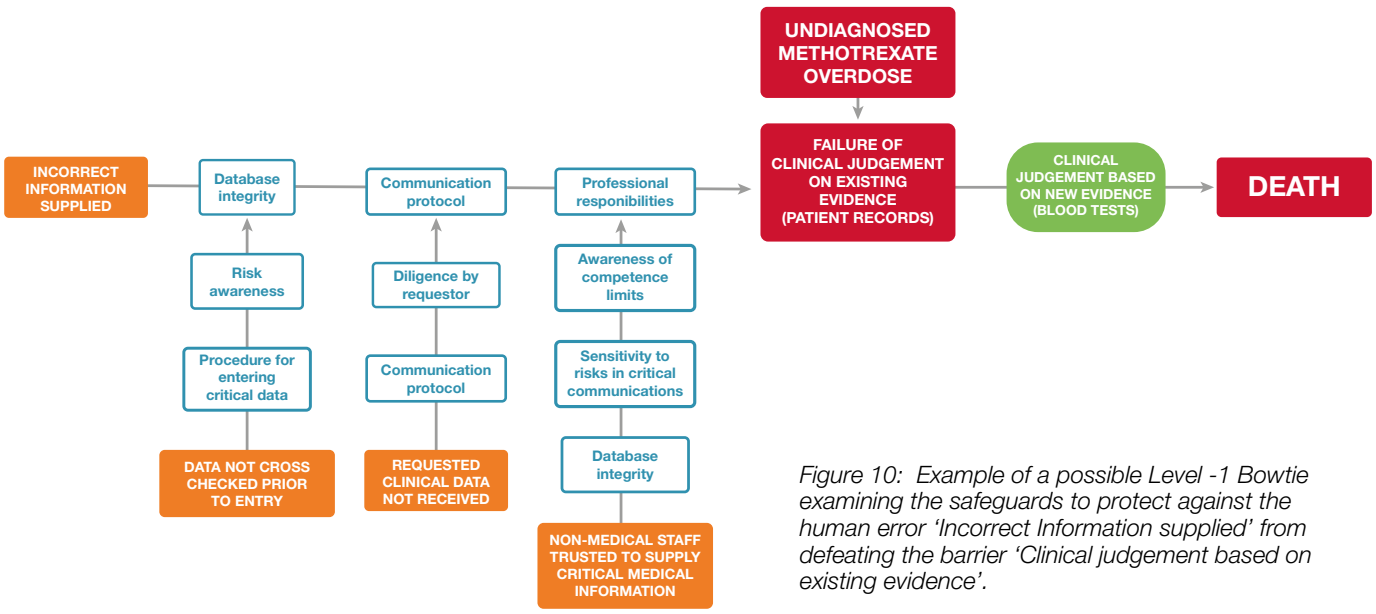


Figure 10: Example of a possible Level -1 Bowtie examining the safeguards to protect against the human error 'Incorrect Information supplied' from defeating the barrier 'Clinical judgement based on existing evidence'.

5.4 CONTENT OF A HUMAN PERFORMANCE STANDARD

This section contains recommendations on the content and structure of a Human Performance Standard associated with human barrier elements.

Barriers will have been identified and approved based on the expectation that they meet the expected standard of performance. Performance standards for barriers are sometimes expressed in terms of the barrier's functionality, availability, reliability, survivability and interaction, (Hamilton and Turner 2014). For each barrier a performance standard is usually developed that specifies the objective, measureable performance and assurance or verification steps required for that barrier.

> "...performance means the properties which a barrier element must possess in order to ensure that the individual barrier and its function will be effective. It can include such aspects as capacity, reliability, availability, effectiveness, ability to withstand loads, integrity, robustness and mobilisation time.
>
> (PSA, 2013, p.18)."

32. A Human Performance Standard for barriers, or barrier elements, should have six characteristics:

    a. The human performance the barrier will deliver should be specific to the threat and the situation when the barrier function is needed (i.e. the Actor, Object and Goal should be defined, as described in section 5.5):

    b. It should be clear who is expected to be involved in delivering the required performance. That includes:

        i. Who detects that the barrier function is needed.

        ii. Who decides what is to be done.

        iii. Who takes action to implement the barrier function.

        iv. Who is relied on to support the barrier.

    c. It should identify the level of competence to be held by each of the individuals involved.

    d. The expected timing of the performance of the function – both the initiation of the performance and its time to completion – should be appropriate to the timescale of the threat.

    e. The standard for successful performance of the barrier should be defined. For example, criteria could be:

        i. Time to detect an event or situation expected to trigger the barrier.

        ii. Accuracy of interpreting the state of the operation.

        iii. Time to initiate an intervention.

        iv. Time to complete an intervention.

        v. Maximum acceptable number or percentage of missed events (i.e. failing to perform the barrier function when it should have been performed).

        vi. Maximum acceptable number or percentage of false alarms (i.e. performing the barrier function when it was not needed).

        vii. Tolerance limits for acceptable performance.

    f. It should document any expectations made by those who approved the barrier about how operations around the barrier will be conducted that are especially critical to performing its function.

RECOMMENDATIONS

The Human Performance Standard will impose requirements on engineering/ design and organisational arrangements as well as the competence of the individuals involved. Note that the competence standard for roles or individuals who may be assigned responsibility for a barrier function should include delivering the skills, knowledge and aptitudes needed to be able to meet the criteria defined in the performance standard.

Tables two and three illustrate how a Human Performance Standards could be documented. The examples are based on the example shown on figure 3 of the left-hand side of a Bowtie where the top event is loss of control of a load during a lift by a crane or the barrier.

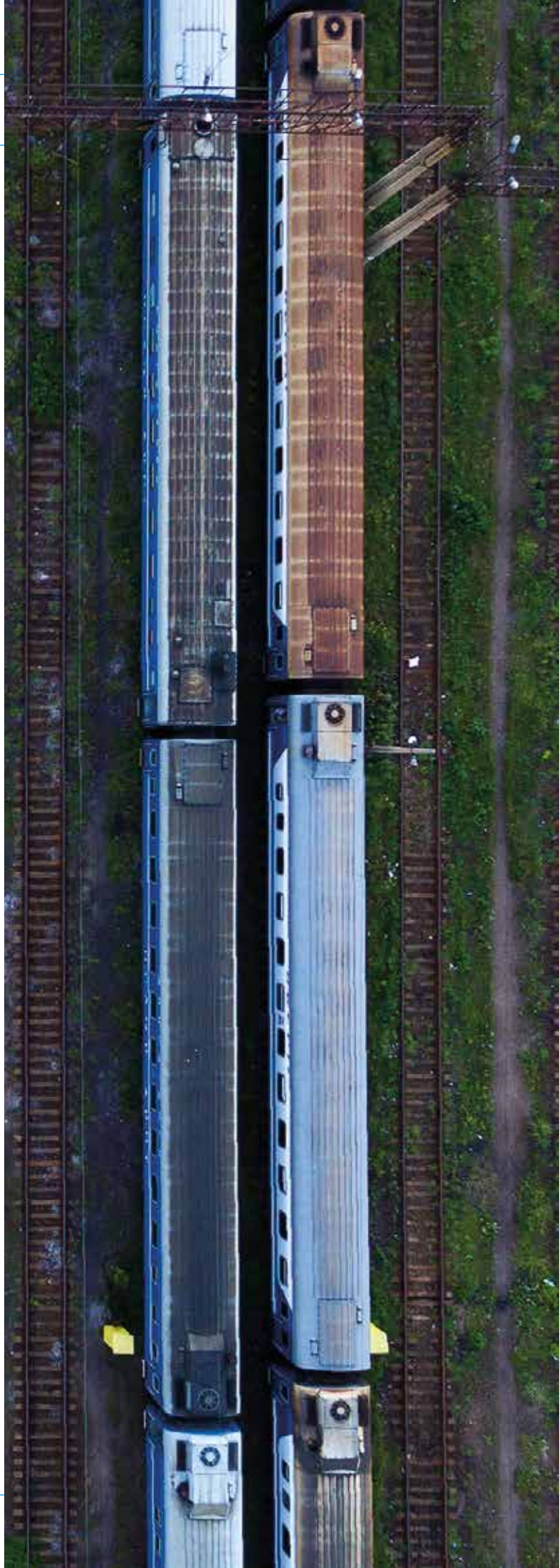


Table 2: *Example Human Performance Standard for human barrier 'planning and lifting procedure' (see figure 5)*

Barrier	Planning and Lifting Procedure
Barrier Element	Lifting Procedure
Type	Organisational
Barrier function(s)	Plan, prepare and carry out crane lifts in accordance with company standard xyz
Limits	The barrier is intended to provide protection for lifts carried out from a fixed base using mobile cranes with loads in the range from X to Y tonnes
Active or Passive?	Active
What makes the barrier specific to the threat?	Actor(s): Lifting Supervisor and Crane Driver Object: Lifts performed from a fixed base with loads in the range from X to Y tonnes Goal: Load safely picked up, carried and delivered without incident
Performance Criteria	Drivers should be able to: 1. Access lifting procedure ABC without having to leave their cab 2. Comply with all of the steps in the procedure, using only charts of reach/lift weights if necessary 3. Recognise when any proposed lift is outside the scope of the procedure
Timing	From the point where a load is clear of the ground, all lifts should be able to be completed without any change of crew, and before any significant change in weather conditions
Who is involved?	1. Lifting supervisor; 2. Crane driver ; 3. Banksmen
Competence Standards	Lifting Supervisor Crane Driver Banksmen
Who Detects?	Supervisor and crane driver should know when the Lifting Procedure is to be followed
Who Decides?	Decisions on lifts should be taken by the Crane Driver in compliance with the lifting procedure and charts of reach/lift weights
Who Acts?	Crane driver, supported by Lifting Supervisor and Banksmen
Information needed	■ Crane capability ■ Crane location ■ Location of lift and lay-down areas ■ Details of lifts ■ Lift route ■ Weather forecast for the lift period ■ Availability and experience of banksmen
Key judgements or decisions involved?	■ Whether any lifts are likely to approach safe lift limits ■ Reliability of weather forecast for duration of lift ■ Whether required lifts are within driver experience and competence ■ Whether there is sufficient manpower available
Actions	Carry out lift in accordance with lifting procedure
Feedback	Feedback to the crane driver of the state of the lift achieved by: a) direct visual monitoring of the load b) visual monitoring of in-cab instruments c) audio monitoring of radio communications between the crew d) visual monitoring of banksmen's hand-signals
Engineering standards	■ Cab ergonomics, including visibility and viewing angles to be compliance with ISO ■ Lifting accessories (hooks, shackles, link chains, etc.) to be compliant with X ■ Lifting points designed onto major items shall be in accordance with X
Critical Expectations associated with human performance for the barrier to be effective	■ Company lifting standard xyz will be up-to-date and a current version available in the crane cab ■ The lifting standard will have been subject to a Procedural HAZOP to ensure it is fit for use in a safety-critical role ■ Contractors will have no commercial or personal incentives not to comply with the plan ■ The driver and crew will understand the importance of complying with the lifting procedure and will advise line management if they have any concerns either about its suitability or with the way it is being implemented ■ Operational crew will not go ahead with lifts if the conditions of the lift (such as crane type, supporting structure or nature of the loads) are outside the limits of the standard

Table 3: *Example Human Performance Standard for human barrier element "alarm and operator response" (see figure 6)*

Barrier	Overload alarm and operator response
Barrier Element	Operator response
Type	Operational
Barrier function(s)	1: Stop the lift. 2: Ensure all personnel are in a safe place. 3: Prepare a plan to safely lower the load. 4. Safely lower load
Limits	Determined by alarm limits
Active or Passive?	Active
What makes the barrier specific to the threat?	Actor: Crane driver Object: Conduct of the lift Goal: Detect an unsafe condition and bring lift to a safe state
Performance Criteria	The driver should: 1. Detect and correctly understand the meaning of the alarm within 1 second of it sounding 2. Be capable of stopping crane movement within 3 seconds of the alarm sounding 3. Be capable of identifying that the alarm is not working before taking a load
Timing	As Performance
Who is involved?	1. Crane driver; 2. Supervisor or Banksmen
Competence Standards	Lifting Supervisor Crane Driver Banksmen
Who Detects?	Crane driver
Who Decides?	Crane driver
Who Acts?	Crane driver, in communication with Supervisor and/or banksmen
Information needed	■ Alarm status (working/not working) ■ Alarm function (active/not active)
Key judgements or decisions involved?	■ The element should not require any decision or judgement about the need to stop the lift immediately. There should be no doubt or ambiguity ■ Decision/judgement will be needed about how to bring the load to a safe state
Actions	■ Stop the lift ■ Plan how to proceed ■ Bring the load to a safe state
Feedback	Feedback available to the crane driver shall include: ■ Visual sightline of load ■ Visual confirmation from cab displays that movement of crane arm ha stopped ■ Visual confirmation from in cab display that weight has been taken off ■ Visual confirmation from banksmen that weight is on the ground
Engineering Standards	■ The overweight alarm shall be designed and tested to comply with Human Factors Engineering standard xyz ■ The location, layout and operation of controls associated with response to the alarm shall comply with Human Factors Engineering standard X. ■ Sightlines from the crane cab to be in accordance with ISO xyz.
Critical Expectations associated with human performance for the barrier to be effective	■ If the alarm fails to function to the expected standard, this will be clearly brought to the driver's attention ■ The driver will not initiate a lift if the alarm is not functioning to the expected standard ■ The barrier is dependent on 1: The alarm functioning reliably, 2: The alarm being designed and implemented so it is effective in capturing operator attention in any situation

5.5 BARRIER MANAGEMENT PLAN

Weaknesses in organisational cultural with respect to barrier management can undermine barrier effectiveness. Operational or commercial pressures can take priority, and assumptions, complacency and human error can all play a part in eroding the effectiveness of barriers. A barrier management plan is a way to bridge the gap between the claims that an organisation makes about the performance of its barriers and the assurance that it can and is delivering that performance, especially where there is a heavy reliance on human performance.

A barrier management plan makes the human and organisational performance claims for the barrier explicit and enables these claims to be monitored and measured, and for leading indicators to be established to signal when performance strays from the desired path.

33. To maintain effective barriers a barrier management plan should be developed to assure the operation and maintenance of the barrier system at an operational location. This plan should cover each barrier and barrier element expected to be implemented at that location.

Table 4: *Questions for barrier effectiveness culture (from Hamilton and Turner, 2014).*

Focus	Question
Critical tasks	What are the barrier management tasks to be performed? Could failure to perform the task properly invalidate the barrier?
Job role & responsibility	Who is responsible for performing the tasks (job roles)? Who is responsible for supervising the performance of the tasks?
Process	Is there a process defined for the tasks? Is that process complied with?
Human machine interaction	Are specialist tools or equipment needed for the task? Are these specialist tools or equipment available? How is the barrier tested and calibrated (if necessary)?
Personnel availability	Are the tasks part of the planned work schedule? How is this communicated to the people who will perform the task? Are there sufficient people available to ensure that the tasks are performed in a timely manner? How are workload and fatigue managed?
Competence	What special knowledge and skills are necessary for the task? How is the competence to perform the task assured?
Critical communications	What initiates the performance of the task (i.e. what are the initiating criteria)? How is the completion of the task checked and reported?
Learning and improvement	If there are defects how are these reported? How are deficiencies in the process identified and reported? How are standards of performance assessed?
Management of change	How is the process of repair of defects managed? Who is responsible for implementing required changes to the process?

5.5.1 DEVELOPMENT OF A BARRIER MANAGEMENT PLAN

A barrier management plan can be developed through a workshop process, based on verified Bowtie diagrams and the associated Human Performance Standards. For each barrier in the Bowtie diagram the workshop team is asked to respond to a set of questions relating to the integrity of the risk control strategy. A series of structured questions can be used to expand on the performance standards for both technical and human barriers and to define the broader human and organisational factors on which each barrier's effectiveness will depend. Table 4 suggests a set of questions about human and organisational arrangements that can be applied in such a workshop.

Once these questions have been answered a consolidated barrier management plan can be prepared that can be used to manage the assurance of barrier effectiveness. The barrier management plan can be organised into three parts:

i. The human and organisational requirements to operate the barrier's function;

ii. The human and organisational requirements to maintain the barrier, and

iii. Any concerns or actions for improvement.

5.5.2 LEADING INDICATORS OF BARRIER EFFECTIVENESS

A barrier management plan provides an explicit set of criteria for use in the assurance of the performance of barriers. It sets out precisely the aim and function of each barrier and the crucial human and organisational performance elements that are essential to deliver its functionality, while ensuring its availability, reliability and survivability. More importantly it provides a visible set of criteria that can be used to demonstrate that the planned control strategy is working. These criteria can serve as leading indications of barrier effectiveness.

These leading indications are derived directly from the operational and reliability criteria in the barrier management plan. They will include things such as manpower levels, competency records, task performance records, test measurements, defect tracking systems, maintenance and repair work and backlog, etc. The organisation can document these as management objectives and record and report their accomplishment. The identification of the specific barriers, their performance criteria and the responsibilities of personnel to perform the critical operational and maintenance tasks, plus the assurance of competencies for these tasks can all be expressed through the management system and audited regularly. Audits provide evidence that the claims made for barrier management are being met.

The barrier management criteria also serve as a basis to engage the workforce in their responsibilities for barrier function. Because the plan makes barrier management actions explicit, it can be shared with the workforce so that they will know why certain equipment and processes are needed to function as barriers or to assure barriers, and which safeguards are relied on to support barriers or to mitigate against the risk of barrier degradation. The workforce is therefore more informed and aware about the role they play in maintaining the risk control strategy. This awareness translates into a more effective culture of process safety management in which people have clear objectives, defined responsibilities, managed competencies and performance goals.

06 GLOSSARY, ACRONYMS AND DEFINITIONS

- ALARP: As Low As Reasonably Practical
- AHARP: As High As Reasonably Practical
- Barrier: Something that is expected, on its own, to be capable of preventing, controlling or mitigating undesired events or accidents. In Bowtie terms, a Barrier is something capable of preventing a Threat from leading to a Top Event. Barriers are Specific, Independent, Effective and Auditable. (Note: Barriers are nearly always Barrier Systems).
- Barrier Element: An individual component of a Barrier System. Usually performs one of the functions of: Detecting the existence of a threat, Deciding what action needs to be taken, or taking the Action necessary to prevent the threat from leading to the undesired outcome. (In Bowtie terms, Top Event or Consequence). Barrier Elements can be physical, electro-mechanical (including software where it acts on or reacts to elements in the physical world), organisational, or human.
- Barrier Function: The task or role of a barrier (PSA, 2013)
- Barrier Management: The totality of activities and processes carried out by an organisation to develop, verify, implement and assure that a Barrier Model is in place and effective throughout the lifetime of the asset or operation.
- Barrier Model: A representation of the total set of controls – both barriers and safeguards – an organisation considers necessary and sufficient to provide the required level of risk reduction over all Threats that could lead to the release of an identified Hazard.
- Barrier System: A combination of Barrier Elements that collectively provide the full functionality required of a Barrier.
- CCPS: Center for Chemical Process Safety.
- CIEHF: Chartered Institute of Ergonomics and Human Factors.
- Consequence; (Used in Bowtie Analysis). The end-state that may be reached after a top event occurs if all of the controls on the right-hand side of the bowtie are defeated.
- Control: Something that is intended and expected to block the path from an event or threat to an unwanted situation (top event or consequence). Controls can be either Barriers or Safeguards depending on the extent to which their performance can be assured.
- Defence: Has no formal meaning. Generally used as a synonym for Control.
- Degradation factors: (Used in Bowtie Analysis). Something with the potential to defeat or reduce the ability of a Barrier or one or more Barrier Elements to perform their intended function. (Also known as Escalation Factors).
- Expectation: Those features not under the direct control of the organisation that chooses to rely on a barrier that the organisation must assume will be in place in order for a Barrier to be capable of delivering its required functionality (such as people being available when the barrier is needed who are aware of their role, competent and fit to work, and are not incentivised to act in a way that could degrade the effectiveness of the barrier).
- Hazard: Something with the potential to cause harm or significant loss. (For example a source of kinetic, potential or chemical energy or radiation, chemicals with corrosive, pyrophoric or carcinogenic properties, excess dose of prescription drug).

- Hazardous Situation: A situation or combination of simultaneous events that either create or have the potential to release a Hazard. (For example, working with hydrocarbons under pressure, working at height, operating a crane, performing surgery, administering drugs, controlling a crowd, entry into a confined space).
- Intention: Those features under the direct control of the organisation that chooses to rely on a barrier that the organisation is responsible for ensuring are in place in order for a Barrier to be capable of delivering its required functionality (typically working conditions, work environment and organisational arrangements).
- Risk: An expression of the likelihood that an undesirable event will take place. Can be expressed quantitatively or qualitatively
- Safeguard: Something that has an important role in implementing, supporting or maintaining barriers but does not meet the minimum conditions necessary to be considered as a Barrier in its own right.
- Threat: (Used in Bowtie Analysis). Something that, unless prevented, will lead to a Top Event.
- Top Event: (Used in Bowtie Analysis). An event reflecting loss of control over a Hazard. For example, a spill of flammable fuel, wrong-site surgery, patient receiving wrong drug or wrong dose, vehicle hitting pedestrian, dropped object.
- Work System: A combination of people and equipment, within a given space and environment, and the interactions between these components within a work organisation (ISO,2004).

07 REFERENCES

Baker, J.A., Bowman, F.L., Erwin, G., Gorton, S., Hendershot, D., Leveson, N., Priest, S., Rosenthal, I., Tebo, P.V, Wiegmann, D.A, Wilson, L.D (2010). *The Report of the BP U.S. Refineries Independent Safety Review Panel*. US Chemical Safety Board.

Cambridgeshire Health Authority (2000) *Methotrexate Toxicity: An inquiry into the death of a Cambridgeshire patient in April 2000.*

Centre for Chemical Process Safety (2001) L*ayer of Protection Analysis: Simplified Process Safety Assessment* (A CCPS Concept Book). Wiley.

Centre for Chemical Process Safety (2015) *Guidelines for Initiating Events and Independent Protection layers in Layers of Protection Analysis.* Wiley.

Centre for Chemical Process Safety (In preparation) *Guidelines for Bowtie risk management.* Wiley.

Chemical Safety Board (2016) *Investigation report Volume 3: Drilling rig explosion and fire at the Macondo well.* Report no 2010-10-I-OS.

Cullen, W. D. (1990) *The Public Enquiry into the Piper Alpha Disaster.* HM Stationery Office. ISBN 0101113102

de Dianous, V., Fievex, C. (2006) *ARAMIS project: A more explicit demonstration of risk control through the use of Bowtie diagram and the evaluation of safety barrier performance.* J. Haz. Mat, 130: 220-233.

Duijm, N. J. (2009) *Safety-barriers as a safety management tool.* Rel. Eng. System Safety. 94: 332-341.

Ellis, G.R., & Holt, A., (2009) *A practical application of 'Human-HAZOP' for critical procedures Hazards XX!, Symposium Series No. 155.* IChemE. 434-439.

Eurocontrol (2013) *From Safety-I to Safety-II: A White Paper.* Eurocontrol.

Gadd, S. A., Kelley, D. M., Balmforth (2004) *Pitfalls in risk assessment: examples from the UK.* Safety Science, 42: 841-857.

Guldenmund, F., Hale, A., Goossens, L., Betten, J., Duijm. N.J. (2006) *The development of an audit technique to assess the quality of safety barrier management.* J. Haz. Mat. 130: 234-241.

Haddon-Cave, C. (2009) *An independent review into the broader issues surrounding the loss of the RAF Nimrod MR2 aircraft XV230 in Afghanistan in 2006.* The Stationery office.

Hamilton, I. W., Turner, C. (2014) *Building a culture of effective process safety management.* Society of Petroleum Engineers Annual Caspian Technical Conference and Exhibition, Paper SPE-172323-MS

Health and Safety Executive Research (2009) *A review of Layers of Protection Analysis (LOPA) analyses of fuel storage tanks.* RR716.

Health and Safety Executive (2010) *Safety and Environmental Standards for Fuel Storage Sites. Process Safety Leadership Group. Final Report.* HSE Books

Hollnagel, E. (2008) *Risk + barriers = safety?* Safety Science 46: 221-229.

Hollnagel, E. (2014) *Safety-I and Safety-II: The past and future of safety management.* Ashgate.

Hopkins, A. (2012) *Disastrous Decisions: The Human and Organisational Causes of the Gulf of Mexico Blowout.* CCH Australia.

International Council on Mining and Minerals (2015). *Health and Safety Critical Control Management.* ICMM.

International Electrotechnical Commission (2003) *Functional Safety – Safety instrumented systems for the process industry sector.* IEC 61511; IEC.

International Electrotechnical Commission (2010) *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems.* IEC 61508; IEC.

International Oil and gas Producer's Association (2016) *Standardisation of barrier definitions.* IOGP.

International Standards Organisation (2004) *Ergonomic principles in the design of work systems.* ISO 6385.

Jianfeng, L., Bin, Z., Yang, W., Mao, L. (2009) *The unfolding of '12.23' Kaixian blowout accident in China.* Safety Science, 47: 1107-1117.

Leveson, N. (2011) *Engineering a safer world*. MIT Press.

McLeod, R. W. (2015) *Designing for human reliability: Human Factors engineering for the oil, gas and process industries.* Gulf Professional Publishing.

McLeod, R.W. (2016) *Issues in assuring human controls in layers-of-defences strategies.* Chem. Eng. Trans: 48.

Mid Staffordshire NHS Foundation Trust (2013) *Report of the Mod Staffordshire NHS Foundation Trust Public Enquiry.* The Stationery Office.

Petroleum Safety Authority (2013) *Principles for barrier management in the petroleum industry.* PSA.

Reason, J. (2008) *The human contribution.* Ashgate.

Sklet, S. (2006) *Safety barriers: definition, classification and performance.* J. Loss Prev. Proc. Ind. 19: 494-506.

Svenson, O (2001) *Accident and incident analysis based on the accident evolution and barrier function (AEB) model.* Cog, Tech,. & Work 3: 42-52.

Swain, A.D., Guttmann, H. E. (1983) *Handbook of Human reliability Analysis with emphasis on nuclear power plant applications.* US Nuclear Regulatory Commission.


4.5m

redactive

Designed and published by
Redactive Media Group
17 Britton Street, London EC1M 5TP
Telephone 020 7880 6200. Email info@redactive.co.uk