OGP

International Association of Oil & Gas Producers

Asset integrity – the key to managing major incident risks

Report No. 415

December 2008

Purpose and target audience

OGP's Managing Major Incident Risks Task Force has developed this guide to help organisations reduce major incident risks by focusing on asset integrity management. It may be applied to new and existing assets at every lifecycle stage. The information presented within it is derived from good practices in mature operating areas where operators are required to provide structured evidence of sound risk management practices.

Although this guide may be used by anyone who contributes to the management of asset integrity, it is particularly targeted at senior managers, including those from a non-technical background, who lead operating organisations. Use of the included *question set* (Appendix) can help assure that major incident risks are suitably controlled at all times for all upstream hydrocarbon operations. This document also includes references for those who require more in-depth understanding of asset integrity management.

1 Introduction

E&P organisations need to manage a complex portfolio of risks. These range from minor events to major incidents that may involve serious personnel injuries, significant environmental damage or substantial financial impact. Globally, the E&P industry has been relatively successful in managing major incident risk. Nevertheless, the challenge remains to reduce the likelihood of such events.

Over the past two decades, the development and implementation of structured Health, Safety and Environmental Management Systems (HSE-MS) have provided a framework within which all hazards and the risks they pose can be identified, assessed and managed. The substantial improvements the industry has seen in Lost Time Injury Frequency (LTIF) and Total Recordable Incident Rates (TRIR) over this period (*see* Figure 1) are, in part, testament to the benefits of a systematic approach to risk management where there are close links between hazards and consequences.

In contrast to occupational injuries, large losses are typically the result of the failure of multiple safety barriers, often within complex scenarios. These are difficult to identify using a simple experience-based hazard identification and risk assessment process. Good occupational health and safety performance of an asset does not guarantee good major incident prevention. A common 'continual improvement management system' may be used, but additional technical skills and competences are needed to manage major incident risks. It is important to understand that the application of suitable equipment technical standards, though vital, is not a sufficient requirement for the prevention of major incidents. Well-managed organisational practices and individual competences are also necessary to ensure the selected barriers remain effective.

This guide summarises ways to manage major incident risk throughout the lifecycle of E&P operations. It outlines processes and tools that explicitly address such risks within an overall HSE-MS or corporate risk management system. It also includes examples of risk management process failures that could lead to a major incident.

Being able to work with an inherently hazardous product in a safe and environmentally responsible manner is critical to the success of any E&P organisation. Major incidents can have severe consequences for people, the environment, assets and company reputation. Although the risks of major incidents can never be reduced to zero, a systematic risk-management process – as outlined in this guide – can significantly reduce their likelihood and limit their effects.

DEFINITION

Asset integrity

Within this guide, asset integrity is related to the prevention of major incidents. It is an outcome of good design, construction and operating practices. It is achieved when facilities are structurally and mechanically sound and perform the processes and produce the products for which they were designed.

The emphasis in this guide is on preventing unplanned hydrocarbon releases that may, either directly or via escalation, result in a major incident. Structural failure or marine events may also be initiating causes that escalate to become a major incident. This guide applies to such events, but there may be additional considerations not covered here.

Broader aspects of asset integrity related to the prevention of environmental or commercial losses are not addressed. However, subject to appropriate prioritisation, the same tools can be applied for these risks.

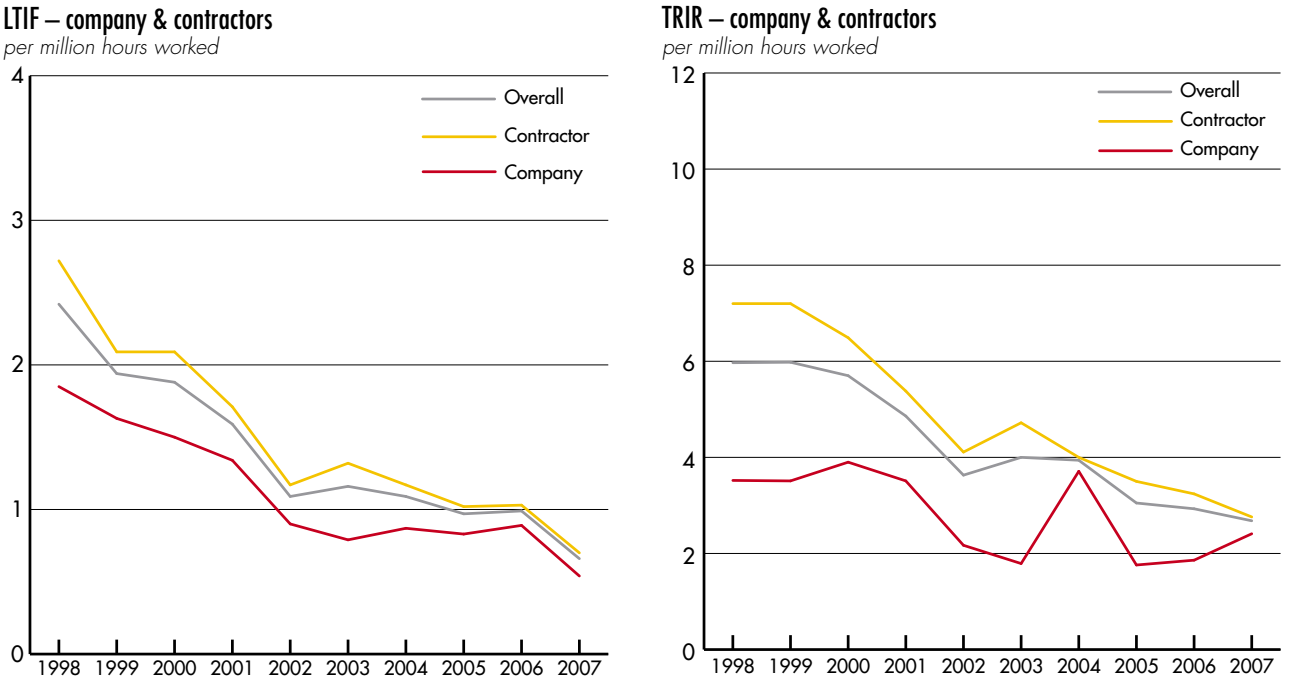


Figure 1 – data from OGP Report *Safety performance indicators – 2007 data*[1]

2 Asset integrity risk management process

The outline process in Figure 2 is based on a standard continual improvement cycle: Plan, Do, Check, Act (PDCA). Minor variations from this process and terminology may be used in other management system documents or standards. The five steps shown should preferably be part of the design process, but they may also be applied to existing assets, and be continued throughout their lifecycle.

DEFINITION

Major incident

An unplanned event with esclation potential for multiple fatalities and/or serious damage, possibly beyond the asset itself. Typically these are hazardous releases, but also include major structural failure or loss of stability that could put the whole asset at risk.

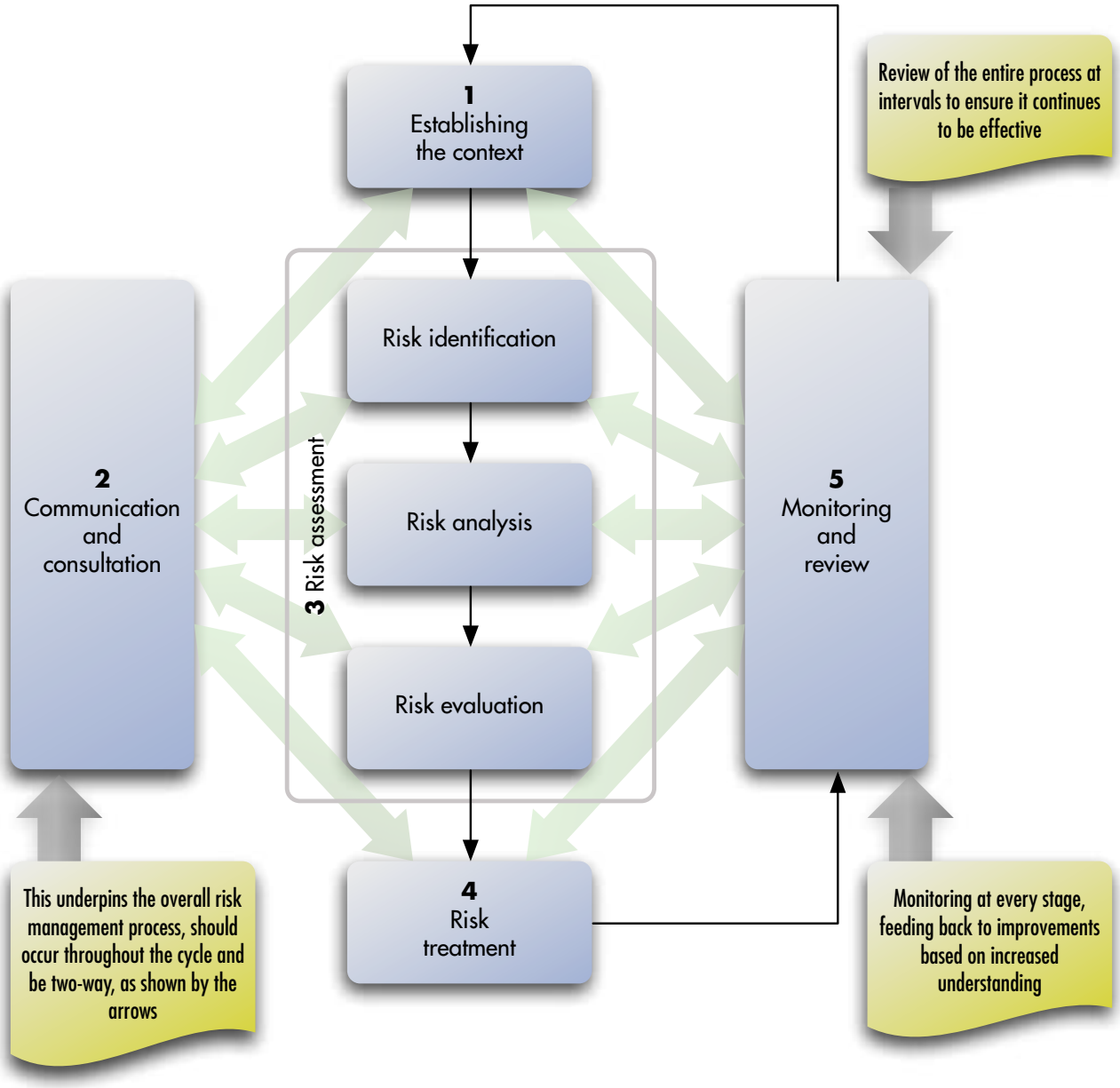


Figure 2 – based on ISO 31000 (draft)[2]

1 Establishing the context

"What drives us?"

Aspects include:

- **External context** – factors outside the organisation such as:
  - applicable legislation, codes and standards (including the terminology used)
  - key stakeholders such as partners, regulators, local communities, NGOs, major contractors and suppliers

Some applicable regulations or standards may specify standard safeguards and thus limit risk treatment optimisation as described in step 4.

- **Internal context** – factors inside the organisation and, for this guide, only those hazards that could result in a major incident such as:
  - corporate risk management standards, their processes and targets
  - governance systems including internal organisation & delegation of responsibilities
  - internal capabilities including persons who operate, maintain and manage activities at the facility

2 Communication & consultation

"Who else should be involved?"

The types, frequencies, style and content of communications should be determined by the internal and external standards, documents, stakeholder groups, etc. identified in step 1.

3 Risk assessment

"What can happen?" (A process carried out in three sub-steps – Figure 2)

- **Risk identification (may also be termed Hazard identification)**
  - Identifies potential harm to people, the environment and assets. Unless applicable major incident risks are identified, steps cannot be taken to eliminate or control them.
- **Risk analysis**
  - This stage involves realistic and detailed consequence assessments. An example would be to estimate how much gas or liquid might be released in the event? Or by what mechanisms could an initial small release escalate to affect people and other equipment? Risk Assessment Data can be used to estimate event frequency[3].
- **Risk evaluation**
  - It is very important to determine what risks are acceptable. For a new design, a wide range of risk reduction (treatment) options exist; for existing assets, the scope may be limited. Options generally include elimination, prevention, control, mitigation and recovery. Elimination is the best way to deal with hazards but is not always possible. For hazards that cannot be eliminated, other treatments should be considered and the most cost-effective combination selected (see step 4 below).

4 Risk treatment

"What do we do?"

Risk treatment involves considering all the feasible options and deciding on the optimal combination to minimise the residual risk so far as is reasonably practicable. This step lies at the heart of the overall asset integrity management process. Successful risk treatment includes ensuring the selected barriers are actually in place, not just 'on paper'.

Engineered safeguards are typically more reliable than procedural ones (see *Barriers*). Likewise, passive systems such as use of open space, gravity drainage and natural ventilation are typically more reliable than systems requiring activation such as firewater, foam, emergency teams, emergency isolation valves and blow down. But no safeguards are infallible. Therefore, a combination of both active and passive systems is typically used to minimise the consequences of integrity loss and expedite recovery. Some risk treatment options may not be possible for an existing asset (e.g. increasing open spaces); others may involve major modifications, requiring appropriate evaluation of the risk reduction benefits relative to the costs.

5 Monitoring and review

"What could we do better?"
"What can we learn, from ourselves and from others?"

As an asset is designed, constructed, operated, maintained and modified, the understanding of associated risks and good practices for its treatment will improve. This allows better risk management. It is also important to review periodically the approach taken for asset integrity risk management; ensuring that new knowledge is considered, changes are understood and the selected barriers continue to be cost-effective.

This review step is also important for newly acquired mature assets, or those being systematically risk-assessed for the first time. Some of the original design philosophy or key maintenance records may not be available and the use of additional barriers may be prudent until integrity monitoring provides sufficient experience or knowledge of the asset to make informed risk management decisions. Changes in key operating parameters (pressure, temperature, composition, *etc*) should also trigger an overall review of asset integrity risk management.

3 Barriers

Barriers are the functional groupings of safeguards and controls in place to prevent the occurrence of a significant incident. A good way to understand barriers is a model that likens them to multiple slices of 'Swiss cheese', stacked together side-by-side. Each barrier is represented as one cheese slice. The holes in the slice represent weaknesses in parts of that barrier. Incidents occur when one or more holes in each of the slices momentarily align, permitting 'a trajectory of accident opportunity' so that a hazard passes through several barriers, leading to an incident. The severity of the incident depends on how many barriers (cheese slices) have holes that line up at the same time.

The 'Swiss cheese' model covers both active failures and latent failures. Active failures are unsafe acts or equipment failures directly linked to an initial hazardous event. Latent failures are contributory factors in the system that may have been present and not corrected for some time (days, weeks, months or in some cases, years) until they finally contributed to the incident.

DEFINITION

Barrier

A functional grouping of safeguards and controls selected to prevent the realisation of a hazard.

Each barrier typically includes a mix of: plant (equipment), process (documented and 'custom and practice') and people (personal skills and their application). The selected combination of these ensures the barrier is suitable, sufficient and available to deliver its expected risk reduction.

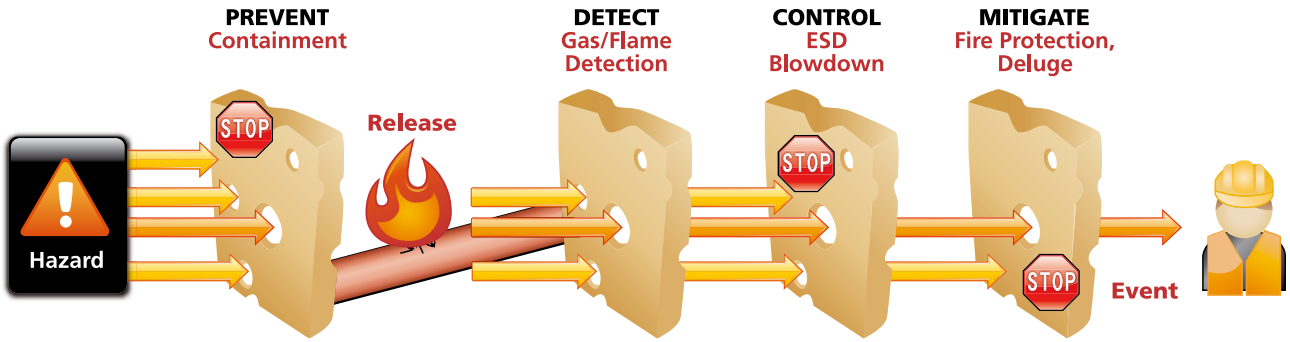


Figure 3 – Application of the 'Swiss cheese' model[4,5]

As shown in Figure 3, the 'Swiss cheese' model asserts that no barrier is ever 100% effective because 'holes' are always present, even though each may be temporary. The aim should be to identify holes and then make them as small and as short-lived as possible, recognising that they are continually changing (equipment deterioration, temporary safeguard bypasses, operational changes, maintenance lapses, personal and team competences, *etc*). Hence, multiple barriers are used to manage the risk of major incidents, thereby reducing the chance that all of the holes 'line up' and the worst-case event is realised.

An alternative way to visualise and determine the need for barriers is to use the 'Bow Tie' model (Figure 4). This indicates how barriers can both reduce the threats from a hazard and limit consequences if the hazard is realised.

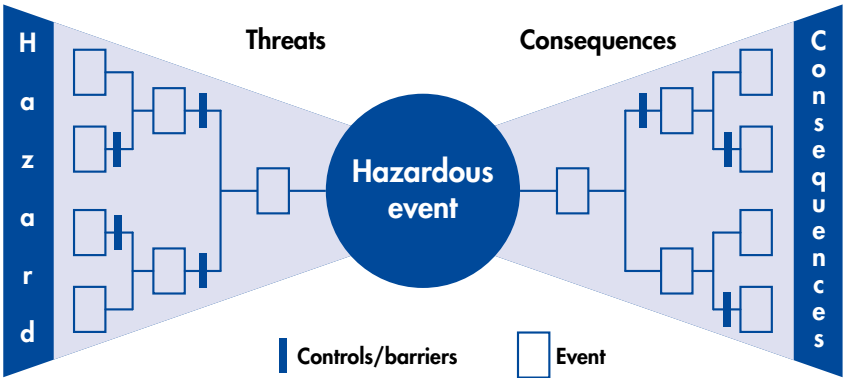


Figure 4 – 'Bow Tie' model

Typical equipment barriers

For E&P assets, integrity barriers can be considered in the following categories:

- **Prevention** – primary containment, process control, primary and secondary structure.
- **Detection** – control room alarms, fire/gas/leak detection.
- **Control and mitigation** – equipment orientation and spacing, secondary containment and drainage, blow-down systems, fire-protection and suppression.
- **Emergency response** – local alarms, escape and evacuation, emergency communications, emergency power.

With this approach, the number of barriers (hardware or management system) for an asset can be held at a logical and manageable level (usually less than 20). In contrast, a listing of individual 'critical equipment items' could number thousands and make systematic management difficult.

A detailed description is needed of the operational performance requirements for the whole barrier to meet the intended risk reduction. Hence, step 4 in Figure 2 – risk treatment – has two levels of increasing detail:

1. define barriers at a system level
2. define high level performance requirements for each barrier
3. define the required performance standards in detail – including those for constituent parts – as appropriate.

Within each barrier, individual equipment items may be suitably itemised and prioritised for criticality using risk criteria.

Performance standards for barriers

Performance standards for barriers are typically described in terms of functionality, availability, reliability and survivability. Performance standards thus determine equipment design specifications (original suitability) and also set requirements for maintenance and testing throughout the asset's lifecycle (ongoing suitability). It is helpful to consider a range of possible performance standards for each component – typically based on recognised design standards – and then optimise the overall barrier to give the most cost-effective risk reduction. Such barrier optimisation needs input from designers, operations and often risk assessment specialists to ensure that all relevant factors are considered. There can also be performance standard optimisation between barriers.

EXAMPLE

A faster blow-down time may reduce the fire protection requirements, but may also result in additional pipework, cooling or increased flare radiation.

Once performance standards are defined, assurance processes should be put in place to confirm that barriers remain fit for purpose. Typically, this will require initial equipment type-testing and/or barrier commissioning performance tests; operational controls and limits; maintenance, inspection and testing plans; performance records for both individual equipment items and the overall barriers; audit and review. Performance standards may be changed over a facility's lifecycle to reflect changes in operating parameters or a need to improve inspection and leak detection if process equipment deteriorates.

Emergency response

As noted above, one or more of the defined barriers should be emergency response: an optimised mix of hardware, procedures and personnel, with associated performance standards. However, as asset integrity improves, the justification for extensive emergency response (mitigation and recovery barriers) may reduce. Consequently, it can be challenging to convince designers and operators working hard to ensure asset integrity that they should also plan and implement robust emergency response barriers in case integrity is lost.

The major incident scenarios for which the emergency response barriers should be designed will be those identified in step 3 of the risk assessment process. This assumes full or partial failure of the preceding barriers, as appropriate. Similar scenarios and barrier failures may be used as a basis for operational training and assessment of the facility emergency response procedures and people, including both front-line personnel and those responsible for managerial response. Such training reinforces understanding of the purpose of major incident barriers and helps to ensure that suitable, timely actions are taken if their performance degrades.

DEFINITION

Performance standard

A measurable statement, expressed in qualitative or quantitative terms, of the performance required of a system, item of equipment, person, or procedure, and that is relied upon as the basis for managing a hazard.

4 Integrity throughout the asset lifecycle

Concept selection

Optimising early design choices can positively influence asset integrity cost and effectiveness throughout the life of a facility. However, optimisation also takes time and resources. Therefore it requires organisational leadership that recognises and balances asset integrity and full lifecycle costs against a design with the cheapest capital cost or shortest construction time.

Some design concepts are inherently more reliable than others. Identifying key hazards and the barriers needed to control them will also help avoid concepts with hard-to-manage asset integrity issues. Concept design decisions may also determine other operations and maintenance activities which have their own impacts on asset integrity risks.

EXAMPLE

Corrosion resistant pipework fully rated for maximum pressure is less likely to fail due to overpressure or corrosion than pipework that relies on instrumented pressure protection and the addition of corrosion inhibitors to maintain integrity, but there may be higher costs and new problems.

Performance standards for the main asset integrity barriers should be set during this stage to ensure fair comparison of options. It is easy to underestimate the true cost of future operations and maintenance. Doing so results in under-investment in asset integrity capital equipment. After concept selection, there is less available flexibility for eliminating hazards, reducing risk or simplifying asset integrity management.

EXAMPLE

Selecting a diesel-powered main generator rather than an external electric supply requires consideration of:

- Main generator system maintenance and backup
- Local diesel storage facilities, and increased fire protection in case of loss of storage integrity
- Diesel-supply operations, with associated transport and transfer spillage risks

Asset definition

As asset design is developed, the barriers for maintaining asset integrity should be worked in parallel. Overall performance standards for the main barriers should already be defined, so performance standards for systems and sub-systems should be ready to be determined. This ensures that equipment specifications take account of maintenance needs and operational capacities.

EXAMPLE

It is unreasonable to expect 96% uptime if key equipment requires 15 days annual inspection downtime, as there is then no contingency for any other downtime, planned or unplanned.

Barrier maintenance, inspection and testing requirements, including estimates of the associated system downtimes, are a design deliverable at this stage. It is also important to ensure the selected design is suitable for the ultimate decommissioning requirements.

EG

Must just the asset be totally recyclable, or must all land or seabed contamination also be removed?

At this stage a catalogue of applicable codes and standards should be compiled, with particular reference to those required to assure the barriers. This catalogue reduces the potential for misunderstandings or disputes about required barriers and performance standards during later stages. Also, by identifying and applying appropriate codes and standards, an initial estimate of residual risk can be made through comparison with a similar plant.

Detailed design

By this point, most key asset integrity decisions have been made. However, poor detailed design can significantly reduce asset integrity by making planned barriers ineffective. Full documentation is needed to describe the asset design, operating and maintenance strategies, and the major hazards management philosophy. Maintenance, inspection and testing routines should be developed for all barriers. Risk assessments should demonstrate that hazards and risks are appropriately managed through equipment specifications (plant), procedures and delegated responsibilities (process), and competent personnel (people). Operability reviews and familiarisation by maintenance and operations personnel should commence during this stage, and continue through the construction stage. At the completion of this stage all asset integrity barriers should be fully defined and documented.

Construction and commissioning

It is critical to ensure that any necessary changes made to the design are suitably managed and authorised so as to maintain asset integrity standards.

All required operating, maintenance and testing procedures should be finalised before commissioning begins, and competent personnel should be recruited and trained. This ensures that, as far as possible, the procedures and people elements of major incident barriers are fully functional when the plant elements are first operated. System commissioning tests may be needed to verify the functional performance elements of some barriers, *eg* blowdown systems, isolation valves.

Operation, modification and maintenance

All the asset integrity barriers defined in the earlier stages should be implemented and maintained. All subsequent changes to asset design, operating limits or maintenance frequencies should be subject to change control and review by a competent technical authority. This is also the time for operating limits to come into play, including control of system over-rides. Barrier performance should be tested regularly and any deficiencies appropriately addressed. To the extent that the earlier concept selection stage eliminated or reduced hazards, the need for ongoing intervention, maintenance and testing tasks can be greatly reduced. This can be particularly important with higher hazard materials and operating conditions, *eg* HPHT reservoirs, high H_2S levels.

Operations and maintenance managers should have the competence to understand and communicate major incident hazards and to describe how the equipment and procedures are designed to provide suitable and reliable asset integrity barriers, including recovery from minor deviations.

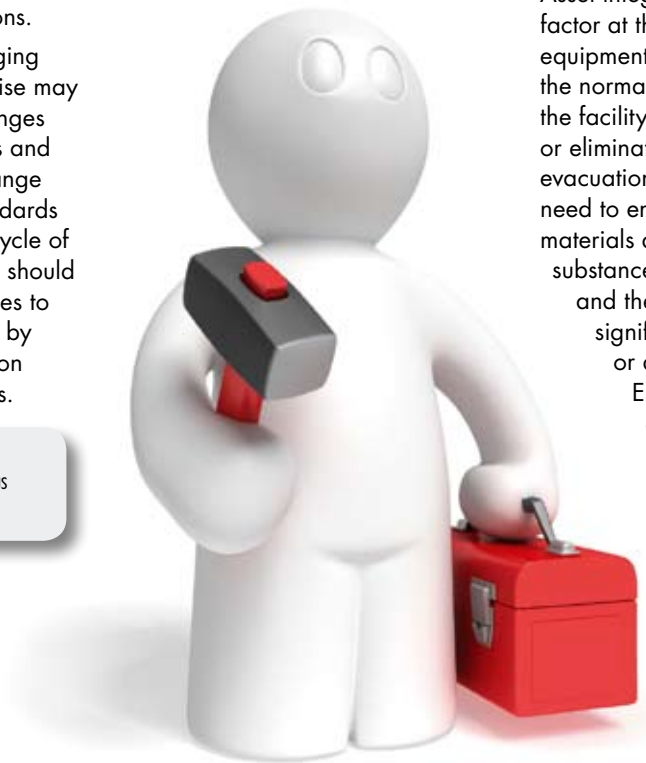
With operating conditions changing over time, an initial design premise may no longer be valid. All such changes potentially affect operating limits and so should be covered by the change control process. Codes and standards may also change within the lifecycle of the facilities. The original design should be reviewed against such changes to see if modifications are required by regulation or justified for reduction of new or newly understood risks.

EG A reservoir may produce solids (sand or proppant), water or unexpected hazardous substances (H_2S, mercury, CO_2, etc)

Acquisition

When considering asset acquisition, at whatever lifecycle stage, the availability of essential asset integrity information should be checked as part of the due diligence process. The costs of replacing any missing information should be included in the overall acquisition costs. Examples would be: design performance standards for the major barriers required to understand whether inspection and testing actions assure operating asset integrity, or detailed design information needed to define the scope of future decommissioning methods and costs. The same considerations apply for any mature asset where information about major incident risks and barriers is incomplete.

Decommissioning, dismantling and removal



Asset integrity can be a significant factor at this stage. As selected equipment is shut down or dismantled, the normal barriers for protecting the facility may be compromised or eliminated, such as escape or evacuation routes. In addition, the need to ensure removal of all process materials and other hazardous substances from both equipment and the affected site may be a significant concern to regulators or decommissioning personnel. Environmental impacts may also occur at lower quantities or concentrations than would be meaningful for a purely safety incident. Preventive asset integrity barriers that have remained fully effective and documented can be extremely beneficial at this stage of the lifecycle.

5 Human factors

There is a separate OGP guide on human factors[6], but it is worth highlighting those aspects that are relevant to major incidents. After all, human error is a key factor in most major incidents, so reducing the potential for errors is an essential part of asset integrity.

Without proper consideration of the human component, even the most sophisticated facilities are susceptible to loss of integrity caused by incorrect operations, unsuitable maintenance or de-motivated people. Designing facilities, work processes and tasks to properly address human factors can contribute significantly to the overall reliability and integrity of the asset, including the ability to manually initiate recovery if other barriers fail.

Equipment design and controls layout

- Arrange equipment for easy access and maintenance
- Easy manual activation with controls labeled or configured to make correct action obvious
- Standard configurations and/or colour schemes to reinforce consistent operation.

Displays and alarms

should have the following characteristics:

- Provide sufficient information to confirm the status of the operation and the effects of control actions.
- Alert personnel to abnormal or emergency conditions that require a specific response.
- Ensure alarms are not activated by routine operations or when changes do not require a response. High volumes of insignificant alarms may mask more serious events and produce a culture of 'automated acknowledgement' by operators without proper assessment of the situation.

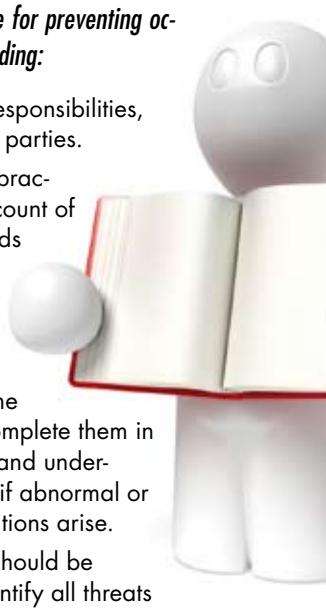
DEFINITION

Human factors

All the interactions of individuals with each other, with facilities and equipment, and with the management systems used in their working environment.

Work practices and procedures

should be similar to those for preventing occupational incidents, including:



- Clear roles and responsibilities, understood by all parties.
- Applicable work practices that take account of all relevant hazards and are applied consistently.
- Clear procedures that allow users to identify the required steps, complete them in the proper order and understand what to do if abnormal or unexpected conditions arise.
- Pre-Task reviews should be undertaken to identify all threats to people and plant, their current controls and what more might be done. Existing approaches exist in many companies looking at the occupational threats and are variously called Job Safety Analyses, Personal Risk Assessments or Task Risk Assessments. However, these need to be reviewed to ensure they also cover threats to the plant capable of leading to major accidents, diminishing the ability of the plant to control a major accident or reducing the ability of personnel to escape in an emergency situation.

EXAMPLE

Tasks on or near energised or operating systems should consider loss of process containment or structural integrity and how task activities might either initiate such a loss, or contribute to its escalation, and personnel involved should be competent to do this.

Work management and authorisation

roles should be defined.

- For tasks that could impact the facility or other workers, a permit-to-work system should be in place to agree, communicate and manage the necessary controls, task authorisation and handover of responsibilities.
- Permit systems should provide clear definitions and consistent application of the isolation and integrity testing minimum standards required for 'live work' tasks on the various process fluids and pressure systems present.
- In complex facilities it may be beneficial to use software-based systems to provide automatic and consistent guidance on suitable task precautions, including system isolations, de-isolations and integrity tests. Such tools may be referred to as an Integrated Safe System of Work (ISSOW).

Task design and individual or team workload

Worker fatigue and overload are key causes of human error. Tasks that exceed workers' capabilities, or whose scope, duration or pace result in fatigue, can lead to a decline in work quality, omissions, or faulty decision-making. Any of these can contribute to loss of integrity. Therefore:

- Tasks should be designed in consistence with the knowledge, skills, and physical capabilities of the person or team.
- Work scope and responsibilities for each role should avoid overload. In upset or emergency situations particularly, the simultaneous actions or responses required from a person or team must be within their capability or the event will escalate, possibly leading to a major incident.
- Work schedules should address the need for periodic rest to avoid both short-term and longer-term effects of fatigue, leading to errors and incidents. This applies to routine work schedules and high workload periods such as facility commissioning or turnarounds. Task schedules should take account of any physical conditions that increase fatigue and error rates such as restricted access, temperature or humidity extremes, or a noisy, damp or contaminated work environment.

Process safety culture

A culture that successfully manages occupational safety and health risks may still fail to deal with major incident risks – indeed, an ineffective process safety culture may be a common hole in multiple asset integrity barriers, leading to a major incident. Consequently:

- Leaders should encourage input from workers and provide adequate feedback for simplifying or improving the performance, reliability and availability of asset integrity barriers.
- Safety culture assessment and development tools[7] should be adapted and applied to the key major incident management elements outlined in this guide.

6 Competences

Competences for a position or team are analogous to the performance standards developed for a hardware system. This section concentrates on competences required to manage major incident risks.

Relevant competences are clearly required by construction, operations and maintenance technicians working directly on an asset. Suitable competences are also required by technical authorities, supervisors and managers. Regulators and other independent bodies who have oversight of major hazard assets also need suitable competences. This category includes insurers and management system auditors.

From the earliest stages of asset design to final shut down and dismantling, competent people can make the difference between flawless performance and major incidents. A frequent finding of major incident investigations is that though individuals involved had the necessary knowledge and skills, they were discouraged by the local culture from applying those skills to break the chain of escalation.

Competence for each role should be managed as follows:

- Identifying the required competences.
- Providing relevant training (knowledge and skills).
- Assuring or verifying these competences (ability to apply knowledge and skills).
- Refreshing competences as appropriate.

Identify the required competences

- Define the key tasks for each role (job position) associated with assuring major incident barriers.
- For each role, determine the range of skills, knowledge and personal attributes (competence elements) to successfully execute these tasks. These competences apply whether the person in the position is a direct employee or a contractor.
- Determine the required level of proficiency for successful performance of each competence element within the role. Consider each role separately, as the required proficiency levels may vary widely. Proficiency levels may be expressed as formal qualifications, or as internally-defined generic descriptors such as beginner, competent, expert or master.
- Identify which competences are prerequisites for filling the role, and which can then be assessed after an initial period in the role. This is especially important for deputies, stand-ins, and other non-regular workers in that role.

Provide relevant training

- Some training may be a pre-entry requirement, *eg* a recognised apprenticeship or a university degree.
- Internal training may include classroom instruction, practical sessions or exercises, and field experience under the direction of a mentor.
- Additional on-the-job experience may be specified to achieve the required level of familiarity and proficiency in the identified competence, *eg* minimum five-years' operations experience.

Assure or verify competences

- The most effective verification of competence includes a combination of written or verbal testing of basic concepts and a demonstration of applicable skills.
- Assessors of competence tests and demonstrations should themselves be competent to carry out the assessment.
- Documentation of assessed competence elements is an important component in managing a competence assurance process. For technical professionals, maintenance of personal Continuing Professional Development (CPD) records and certification by an accredited organisation is one way to verify competence in the required skill areas. Other ways to document individual qualifications and competences include an internal database or safety passports.

Refresh competences

- Periodically review which competences and associated proficiency levels are required for each role, as the requirements may change due to changes in technology, facility size, reorganisation, or identified deficiencies.
- Periodically re-verify personal competences to assure there has been no erosion, particularly in areas not regularly used, *eg* emergency response. Refresher training at set intervals – although widely practiced – is often an ineffective use of resources and is not a substitute for competence re-assessment when required.

DEFINITION

Competence

A person's ability to accurately and reliably meet the performance requirements for a defined role.

Competence includes the skills and knowledge necessary to perform the required tasks successfully, the ability to recognise personal limits and so seek physical help or input from others when appropriate, and the conscientious application of skills and knowledge every time they are used.

Competence thus includes a behavioural element, ie ability to apply personal skills and knowledge in typical workplace situations.

Typical competences

The following are examples of generic roles with competence requirements for ensuring asset integrity:

Technician

Understands current operating limits; responds appropriately to operational alarms; understands tasks required to successfully operate or verify a barrier, including task hazards and controls; accurately installs and removes temporary inhibits; identifies and records test results, including any defects; seeks assistance for critical defects.

Asset supervisor

Ensures operations are within currently defined envelope; authorises barrier tests, temporary inhibitions, etc. based on overall risk assessment; monitors barrier performance and ceases operations immediately if barriers are unacceptably degraded; consults technical authority about actual or potential barrier deficiencies.

Technical authority

Develops and defines suitable barrier or equipment performance standards; accurately interprets relevant codes and standards; advises on test methods and procedures; risk assesses performance standard variations and test results; for defective barriers, advises whether effective alternate temporary controls are possible.

Asset manager/leader

Provides leadership to demonstrate the value of effective barriers *(example – by using the Question Set)*; ensures suitable budget and competent resources are available to operate, monitor, test and manage barriers; monitors major incident leading and lagging indicators; acts on relevant audit findings.

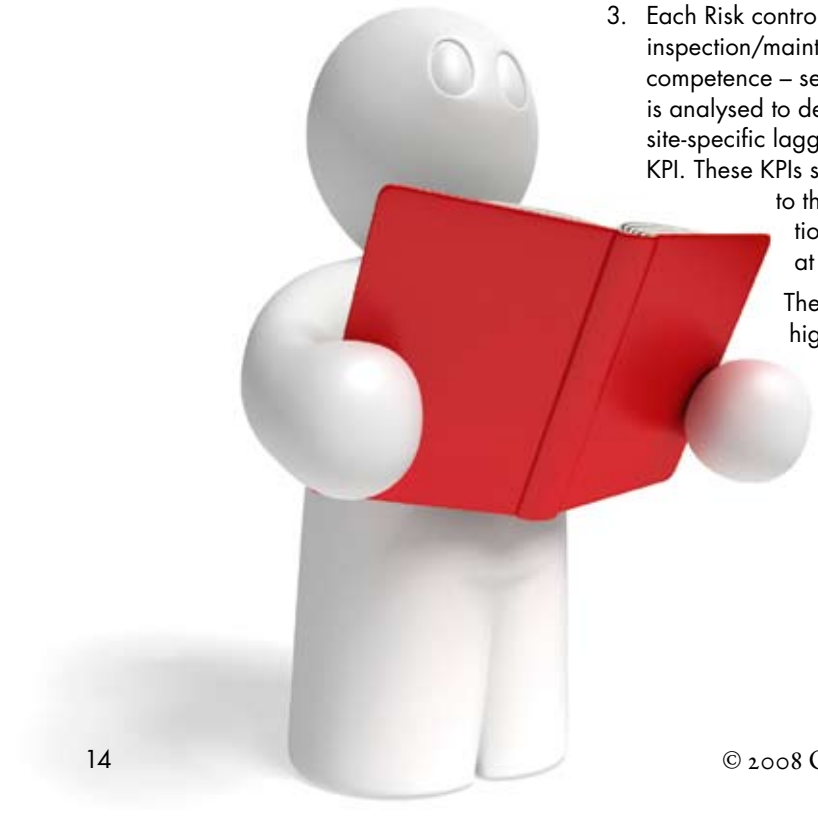
7 Monitoring and review

Monitoring and reviewing asset integrity performance (Check, Act) is as important as developing and implementing integrity plans and systems (Plan, Do). Integrity monitoring should be fact-based, rather than opinion-based, and may include the following:

- Key Performance Indicators (KPIs).
- Barrier performance standard verification.
- Audit findings.
- Incident and accident investigations.
- Benchmarking and lessons learned from external events.

Key Performance Indicators (KPIs)

KPIs can be used to evaluate asset integrity performance against stated goals. Because major loss-of-integrity events are relatively rare, it is important to record and monitor even minor incidents. The KPIs which record actual integrity failures are typically called 'lagging indicators'. By contrast 'leading indicators' can be used to assess the health of the safeguards and controls which make up the barriers.



Facility level KPIs

There is no universal set of KPIs that applies to all major hazard facilities – rather the KPIs selected should be aligned with the risk-management process for the facility, and these specific KPIs may then be used to aid the management of the five steps outlined above (see asset integrity management process). In addition, the leading and lagging indicators selected should cover all three aspects of incident prevention – plant, process and people. The major hazards regulator in the UK, the *Health and Safety Executive* (HSE), has produced a guidance document *Developing Process Safety Indicators*[8] outlining a method that may be used to develop suitable KPIs for an operating site. The method advocated by HSE is similar to that defined in this document, *ie*:

1. Immediate causes of a significant release are identified (wear, corrosion, overfilling, impact damage, over/under pressurisation, operations error, etc.).
2. Various Risk control systems are identified for each hazard – typically each system will contribute to risk reduction for more than one type of incident scenario.
3. Each Risk control system (*eg* inspection/maintenance; staff competence – see table opposite) is analysed to define suitable site-specific lagging and leading KPI. These KPIs should be specific to the actual operations carried out at the facility.

The typical high-level risk control system listed in the table opposite is likely to be relevant for many major hazard facilities. Example KPIs are also summarised in the table but should be further customised for a specific facility.

The Center for Chemical Process Safety (CCPS) document *Process safety leading and lagging metrics*[9] defines lagging KPIs which may be used to assign a severity rating to a hazardous release. These ratings can then be used in conjunction with worker exposure hours to calculate standard lagging 'process safety metrics', for performance comparisons between facilities and organisations. A lower level of lagging KPI for facilities is also suggested – based on a 'process safety near miss' reporting system, with examples of the types of event to be considered.

This CCPS publication also identifies possible leading KPIs for the following areas:

- Maintenance of mechanical integrity
- Action items follow-up
- Management of change
- Process safety training and competence, including assurance.

The CCPS book *Guidelines for Risk Based Process Safety*[10] provides further advice on setting suitable KPIs, including a four-level rating system for assessing how dependable KPIs are for improving organisational performance.

The Norwegian Petroleum Safety Authority (PSA) has also led work in the area. Their "Trends in risk level" project monitors the risk level development using various methods such as incident indicators, barrier data, interviews with key informants, work seminars, field work and a major questionnaire survey every other year. The results are presented in annual reports.

Generic barriers and example KPIs

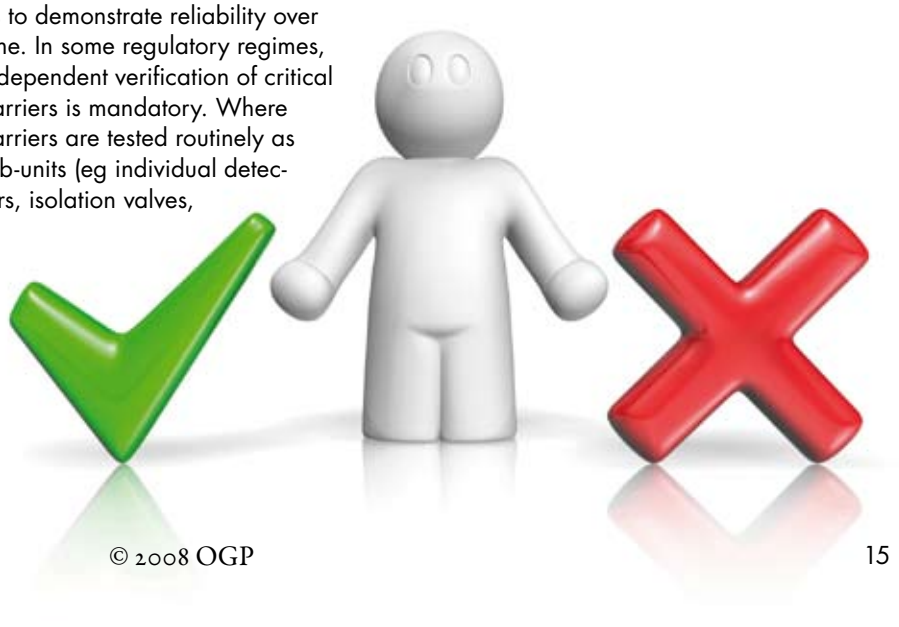
(Based on table 5 from the UK HSE guidance document: Developing process safety indicators)

Risk control system	Example lagging KPI	Example leading KPI
Inspection/maintenance	Number of loss-of-containment incidents	• % of safety-critical plant/ equipment that performs to specification when tested • % maintenance plan completed on time.No. of process leaks identified during operation or during downtime
Staff competence	Number of loss-of-containment incidents plant trips, equipment damage, etc. linked to insufficient understanding, knowledge or experience of correct actions	• % personnel meeting local assessed competence criteria (inc Supr/Mgr) • Average period required to become fully competent after appointment to a new position
Operational procedures	Number of operational errors due to incorrect/unclear procedures	• % of procedures reviewed and updated versus plan
Instrumentation and alarms	Number of incidents linked to failure of instrumentation or alarms	• % function tests of alarms/trips completed on schedule
Plant change management	Number of incidents linked to failure of MOC	• % plant changes suitably risk assessed and approved before installation • Average time taken to fully implement a change once approved
Permit to work (PTW)	Number of incidents where errors in PTW process are identified as a contributory cause	• % PTWs sampled where all hazards were identified and all suitable controls were specified • % PTWs sampled where all controls listed were fully in place at worksite
Plant design	Number of incidents where errors in plant design are identified as a contributory cause	• No. of post-startup modifications required by Operations • No of deviations from applicable codes and standards • % safety-critical equipment/systems fully in compliance with current design codes
Emergency arrangements	Number of emergency response elements that are NOT fully functional when activated in a real emergency	• % of persons sampled who have participated in an emergency exercise in past X months • % ESD valves and process trips tested, using a schedule defined in a relevant standard or the facility safety case

Performance standard verification

Where possible, testing, recording and verifying actual barrier performance, reliability, and availability should be carried out at intervals throughout the asset's operating life. Direct operational testing is preferred, but some barriers may have to be verified largely by suitable modelling at the design stage (eg structural) or by type testing (eg fire protection), as functional operational testing is not practical. In such cases it is typical to require periodic inspection of physical condition to check for evidence of degradation.

Operational functional testing should be realistic, objective and results should be properly recorded, so as to demonstrate reliability over time. In some regulatory regimes, independent verification of critical barriers is mandatory. Where barriers are tested routinely as sub-units (eg individual detectors, isolation valves, process trips, deluges, emergency lights) some overall system performance testing should also be required.



Audit findings

Audits should be an integral part of the system for managing major incident barriers. The purpose of audits is to:

- Determine whether the asset integrity management system elements are in place and performing effectively relative to company objectives and applicable regulatory or technical standards.
- Identify areas for improvement of asset integrity management. Improvements may include better results or improved efficiency (same results using less resource).

The risk profile of the asset should determine the type and frequency of integrity audit. Audits may be self-assessments conducted by personnel from within the organisation, or external audits conducted by resources outside the audited organisation. Audit scope should be the overall operation of the asset integrity management system and its integration into line activities. The scope may specifically address the following:

- Policy, organisation and documentation
- Risk evaluation and management
- Planning and resourcing
- Implementation and monitoring.

Asset integrity audits require adequate and knowledgeable resources using objective protocols. Auditors should identify sound practices where no change is needed, opportunities for improvement, and any serious non-conformances. Auditors may suggest solutions to identified problems, or they may simply note the nature of the problems and allow management to devise and implement appropriate solutions. In either case, the recommendations should be followed-up in the next audit cycle, to ensure identified issues have been addressed appropriately.

Lack of comment about asset integrity issues during general facility inspections by regulators, insurers, etc. should not be taken as evidence that asset integrity management is satisfactory. However, the results of any targeted inspections by external bodies may be included in the evidence submitted for management review.

Management review

Asset management should regularly consider evidence from each of the activities outlined above and should also look at the practices of industry leaders for possible improvement opportunities in asset integrity. Lessons learned from incidents and near misses within the company and in the operations of others may also highlight possible improvements. Case studies, such as those referenced in the next section, can provide valuable real life input to compare with existing internal strategies and practices.

Based on these data, managers can set suitable objectives for the next improvement cycle. Resources devoted to asset integrity monitoring and to improvements should be risk-based, *ie* based on the current facility-wide risk reduction benefits provided by assured barrier performance and the opportunities for improvement.

References

1. OGP. *Safety performance indicators – 2007 data.* Report № 409. 2008. The International Association of Oil & Gas Producers, London, UK.
2. ISO/DIS 31000. *Risk management – principles and guidelines on implementation.*
3. OGP. *Risk Assessment Data Directory* (to be published in 2009). The International Association of Oil & Gas Producers, London, UK.
4. James Reason. *Human Error.* Cambridge University Press. 1990. ISBN 978-0521314190.
5. James Reason. *Managing the risks of organizational accidents.* Ashgate. 1997. ISBN 978-1840141047.
6. OGP. Website: *Human Factors* area. http://info.ogp.org.uk/hf
7. OGP. *Human Factors – a means of improving HSE performance.* Report № 368. The International Association of Oil & Gas Producers, London, UK. 2005.
8. Developing Process Safety Indicators; A step-by-step guide for chemical and major hazard industries. HSE Books, ref. HSG254. 2006. ISBN 978-0717661800
9. CCPS. *Process Safety: Leading and Lagging Metrics.* Center for Chemical Process Safety, New York, USA. 2008.
10. CCPS. *Guidelines for Risk Based Process Safety.* WileyBlackwell. 2007. ISBN 978-0470165690

Bibliography

General

- CCPS. *Guidelines for Risk Based Process Safety, Center for Chemical Process Safety.* WileyBlackwell. 2007. ISBN 978-0470165690.

Introduction

- OGP. *Guidelines for the development and applications of health, safety and environmental management systems.* Report № 210. The International Association of Oil & Gas Producers, London, UK. 1994.

Asset Integrity Management Process

- ISO 17776: 2000. *Petroleum and natural gas industries – offshore production installations – guidelines on tools and techniques for hazard identification and risk assessment.*
- ISO 13702: 1999. *Petroleum and natural gas industries – control and mitigation of fires and explosions on offshore production installations – requirements and guidelines.*
- OECD. *Guidance on Safety Performance Indicators.* Organization for Economic Co-operation and Development (OECD). 2003. ISBN 978-9264019102.

Barriers

- HSE. Guidance on risk assessment for offshore installations. Health & Safety Executive, Aberdeen, UK. Offshore Installation Sheet 3/2006.

Competence

- Waterfall, Kevin; Young, Clyde; and Al-Anazi, Khalaf S. *Health, Safety, Security, and Environmental Competence Finds a Level Playing Field in the Industry.* Paper SPE 98516 presented at the SPE International Health, Safety, and Environment Conference, Abu Dhabi, 2–4 April 2006.

Case studies

- CCPS. *Incidents That Define Process Safety.* WileyBlackwell. 2008. ISBN 978-0470122044

Glossary

Asset

Facilities and associated infrastructure, e.g. structures, wells, pipelines, reservoirs, accommodation & support services.

Asset integrity

The prevention of major incidents (see expanded definition on page 3).

Availability

The ability, measured in terms of uptime percentage, of a system to perform its required function.

Barrier

A functional grouping of safeguards and controls selected to prevent the realisation of a hazard.

Competence

A person's ability to meet – accurately and reliably – the performance requirements for a defined role.

Control

see also *Barrier*. Used specifically for a barrier which mitigates the consequences of an initial event.

Escalation

The process by which initial & sometimes small events trigger further – sometimes larger – events.

Functionality

What a device or system is designed to do.

Human factors

All the interactions of individuals with each other, with facilities and equipment, and with the management systems used in their working environment.

KPI

Key Performance Indicator, may also be called metrics. See *References* for detailed definition and asset integrity examples.

Major incident

An unplanned event with esclation potential for multi-fatalities and/or serious damage, possibly beyond the asset itself. Typically these are hazardous releases, but also include major structural failure or loss of stability that could put the whole asset at risk.

Mitigation

A barrier whose role is to limit consequences, generally by limiting escalation, but which does not prevent the initial event.

Performance standard

A measurable statement, expressed in qualitative or quantitative terms, of the performance required of a system, item of equipment, person or procedure, and that is relied upon as the basis for managing a hazard.

Recovery

Safe and timely resumption of normal operations after an incident.

Reliability

Proportion of occasions a barrier or equipment item will function as designed (%).

Residual risk

Risk that remains when a barrier, or combination of barriers, operates as intended.

Risk treatment

see *Barrier*.

Survivability

Protection required by a barrier or equipment item to ensure continued operation during a major incident.

London office: 209-215 Blackfriars Road, London SE1 8NL, UK Tel: +44 (0)20 7633 0272 Fax: +44 (0)20 7633 2350
Brussels office: 165 Bd du Souverain, B-1160 Brussels, Belgium Tel: +32 (0)2 566 9150 Fax: +32 (0)2 566 9159
Web: www.ogp.org.uk E-mail:reception@ogp.org.uk A company limited by guarantee Registered in England, No. 1832064 VAT No. 241 240 903