Asset integrity – the key to managing major incident risks
Acknowledgements

Safety Committee

Photography used with permission courtesy of
© Alvo/Shutterstock and © petroleum man/Shutterstock [Front cover]
© Sascha Burkard/iStockphoto [Back cover]

Feedback

IOGP welcomes feedback on our reports: publications@iogp.org

Disclaimer

Whilst every effort has been made to ensure the accuracy of the information contained in this publication, neither IOGP nor any of its Members past present or future warrants its accuracy or will, regardless of its or their negligence, assume liability for any foreseeable or unforeseeable use made thereof, which liability is hereby excluded. Consequently, such use is at the recipient’s own risk on the basis that any use by the recipient constitutes agreement to the terms of this disclaimer. The recipient is obliged to inform any subsequent recipient of such terms.

This publication is made available for information purposes and solely for the private use of the user. IOGP will not directly or indirectly endorse, approve or accredit the content of any course, event or otherwise where this publication will be reproduced.

Copyright notice

The contents of these pages are © International Association of Oil & Gas Producers. Permission is given to reproduce this report in whole or in part provided (i) that the copyright of IOGP and (ii) the sources are acknowledged. All other rights are reserved. Any other use requires the prior written permission of IOGP.

These Terms and Conditions shall be governed by and construed in accordance with the laws of England and Wales. Disputes arising here from shall be exclusively subject to the jurisdiction of the courts of England and Wales.
Asset integrity – the key to managing major incident risks

Revision history

<table>
<thead>
<tr>
<th>VERSION</th>
<th>DATE</th>
<th>AMENDMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.0</td>
<td>December 2018</td>
<td>Minor corrections</td>
</tr>
<tr>
<td>1.0</td>
<td>December 2008</td>
<td>First release</td>
</tr>
</tbody>
</table>
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope</td>
<td>5</td>
</tr>
<tr>
<td>Foreword</td>
<td>6</td>
</tr>
<tr>
<td>1. Introduction</td>
<td>7</td>
</tr>
<tr>
<td>2. Asset integrity risk management process</td>
<td>9</td>
</tr>
<tr>
<td>3. Barriers</td>
<td>13</td>
</tr>
<tr>
<td>4. Integrity throughout the asset life cycle</td>
<td>17</td>
</tr>
<tr>
<td>5. Human factors</td>
<td>21</td>
</tr>
<tr>
<td>6. Competences</td>
<td>24</td>
</tr>
<tr>
<td>7. Monitoring and review</td>
<td>27</td>
</tr>
<tr>
<td>Appendix A – Question set</td>
<td>30</td>
</tr>
<tr>
<td>Glossary</td>
<td>37</td>
</tr>
<tr>
<td>References</td>
<td>39</td>
</tr>
</tbody>
</table>
Scope

IOGP’s Managing Major Incident Risks Task Force 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 life cycle 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 A) can help assure that major incident risks are suitably controlled.

This report includes references for those who require more in-depth understanding of asset integrity management.
Foreword

IOGP Report 415, Asset Integrity – the key to managing major incident risks was first published in 2008. It explicitly addressed asset integrity and process safety risks as part of a company’s overall management systems. Since then, approaches have continued to evolve.

Although this 2018 version of the report updates the formatting and branding, it sees only minor changes to the content.

Report 415 remains an informative overview and introduction to the concepts and management of asset integrity, within a company’s overall Management System. Readers wishing to deepen their knowledge or seeking more recent guidance are encouraged to consult the IOGP reports mentioned below. All are available to download from the IOGP online library http://www.iogp.org/Our-library

Guidance on establishing an Operating Management System (OMS) is now integrated within IOGP Report 510, Operating Management System Framework for controlling risk and delivering high performance in the oil and gas industry, published in 2014. Reports 415 and 510 both provide guidance on how to apply risk management as a fundamental process that puts planned measures in place to eliminate or reduce release of hazardous fluids by applying risk controls. IOGP Report 511, OMS in practice - A supplement to Report No. 510, Operating Management Systems Framework provides further guidance on establishing a new management system, or reviewing an existing one. Readers interested in leadership and safety culture are also directed to IOGP Report 452, Shaping safety culture through safety leadership.

Report 415 introduced the concept of establishing a set of barriers, each of which represents a grouping of risk controls. This was further developed in Report 544, Standardization of barrier definitions, published in 2016.

In 2011, IOGP published Report 456, Process Safety – Recommended Practice on Key Performance Indicators establishing four tiers of Key Performance Indicators to collect data on significant loss of primary containment events (Tiers 1 and 2) and to establish leading indicators to assess strength of barriers. The 2018 version of 456 took the barrier categories defined in Report 544 and proposes an approach to leading KPIs at Tier 3 and 4 levels.

IOGP started data collection of Tier 1 and 2 process safety events in 2010 and has published it annually since 2011.
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.

Over the past three decades, the development and implementation of structured Health, Safety and Environmental Management Systems (HSE-MS) have provided a framework within which 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.

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.

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 life cycle 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.

Figure 1: Overall Total Recordable Injury Rate and Lost Time Injury Frequency [1995-2017] reported to IOGP by IOGP Members [company and contractor data].
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 life cycle.

Major incident

An unplanned event with escalation 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: Example risk management process as described in IOGP Report 510, Operating Management Systems Framework
Step 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 accident such as:

- corporate risk management standards, their processes and targets
- governance systems including internal organisation and delegation of responsibilities
- internal capabilities including persons who operate, maintain and manage activities at the facility.

Step 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.

Step 3. Risk assessment

“*What can happen?*” *(a process carried out in the three sub-steps in Figure 2)*

1. **Risk identification** (may also be termed *Hazard identification*)

Identifies potential harm to people, the environment and assets. Unless applicable major incidents are identified, steps cannot be taken to eliminate or control them.
2. 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, see for example IOGP Report 418, Risk Assessment Data Directory and its related reports.

3. Risk evaluation

It is very important to determine what level of risk is tolerable. 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 practical.

For hazards that cannot be eliminated, other treatments should be considered and a cost-effective combination selected (see step 4).

Step 4. Risk treatment

“What do we do?”

Risk treatment involves considering 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.

IOGP Report 544, Standardization of barrier definitions was published in 2016 to help standardise barrier type and categories of processes safety barriers.
Step 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 risk 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\(^1\). 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.

---

**Barrier**

A risk control that seeks to prevent unintended events from occurring, or prevent escalation of events into incidents with harmful consequences. [From IOGP 510]

Figure 3 illustrates two primary types of barrier: hardware barriers and human barriers as defined in IOGP 544, *Standardization of barrier definitions*. Hardware and human barriers are put in place to prevent a specific threat or cause of a hazard release event, or to reduce the potential consequences if barriers have failed and an event has occurred.

Both hardware and human barriers are supported by the processes and procedures contained within the Management System Elements, such as those in the Operating Management System in Report 510.

---

Asset integrity – the key to managing major incident risks

Hardware barriers

Primary containment, process equipment and engineered systems designed and managed to prevent LOPC and other types of asset integrity or process safety events and mitigate any potential consequences of such events. These are checked and maintained by people (in critical activity/tasks).

Human barriers

Barriers that rely on the actions of people capable of carrying out activities designed to prevent LOPC and other types of asset integrity or process safety events and mitigate any potential consequences of such events.

Management System Elements

Management System Elements that group processes and practices designed to prevent LOPC and other types of asset integrity or process safety events and mitigate any potential consequences of such events. Management System Elements support hardware and human barriers.

**Figure 3:** Barrier types as described in IOGP 544, Standardization of barrier definitions
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. This indicates how barriers can both reduce the threats from a hazard and limit consequences if the hazard is realised.

The number of barriers (hardware or management system) for an asset should be held at a logical and manageable level, usually less than 20. A listing of individual ‘critical equipment items’ could number thousands and make systematic management more difficult.

A detailed description is needed of the operational performance requirements for the whole barrier to meet the intended risk reduction. Hence, the Control risks stage in Figure 2 has three 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 hardware 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 life cycle (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 a 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; and audit and review.

Performance standards may be changed over a facility’s life cycle 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.

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 life cycle

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 life cycle costs against a design with a lower 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 other issues.

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 could result in under-investment in asset integrity related 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.

At this stage a catalogue of applicable codes and standards should be compiled, with particular reference to those required to assure strength of the barriers.

Example

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

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, inadequate attention during 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, e.g., blow-down systems, isolation valves.

Operation, modification and maintenance

Asset integrity barriers defined in the earlier stages should be implemented, continuously monitored and maintained. 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 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, e.g., HPHT reservoirs, high H2S levels. Operations and maintenance managers should have the relevant competencies 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. Such changes potentially affect operating limits and so should be covered by the change control process. Codes and standards may also change within the life cycle 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.
A reservoir may produce solids (sand or proppant), water or unexpected hazardous substances (H₂S, mercury, CO₂, etc.)

Acquisition

When considering asset acquisition, at whatever life cycle 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 life cycle.
5. Human factors

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 designs and controls layout

- Arrange equipment for easy access and maintenance
- Easy manual activation with controls labelled 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:

- Provides sufficient information to confirm the status of the operation and the effects of control actions.
- Alerts personnel to abnormal or emergency conditions that require a specific response.
- Minimises cases where alarms are 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.

---

Human factors

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.
- 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 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 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 consistent 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 could 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 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 competencies 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.

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, i.e., an ability to apply personal skills and knowledge in typical workplace situations.

From the earliest stages of asset design to final shut down and dismantling, competent people can make the difference between good 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, e.g., 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, e.g., 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, e.g., 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.

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 task required to successfully operate or verify a barrier, accurately installs and removes temporary inhibits; identifies and records test results, including any defects; seeks assistance for critical defects.

**Technical authority**
Develops and defines suitably 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 supervisor**
Ensures operations are within currently defined envelope; authorised 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.

**Asset managers/leader**
Provides leadership to demonstrate the value of effective barriers (example – by using the Question Set provided in the appendix); 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, more ‘leading indicators’ can be used to assess the health of the safeguards and controls which make up the barriers.

Since the publication of this report in 2008, IOGP has published Report 456, Process Safety – Recommended Practice on Key Performance Indicators [2011]. Report 456 established four Tiers of Key Performance Indicators to collect data on significant loss of primary containment (LOPC) events (Tiers 1 and 2) and to establish leading indicators to assess barriers (Tiers 3 and 4). Please consult it for extensive guidance on establishing corporate and facility level KPIs.

Since 2013, IOGP has collected and published annual Safety performance indicators – Process safety events reports.

Performance standard and 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 (e.g., structural) or by type testing (e.g., 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 and 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 (e.g., 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
  resources).

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

The management review should include the performance of barriers. Where barriers are identified to be degraded, the increase in associated risk and corrective action plans should be endorsed by the senior management.

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, i.e., based on the current facility-wide risk reduction benefits provided by assured barrier performance and the opportunities for improvement.
Appendix A – Question set

These questions may be used to test how effectively asset integrity hazards are understood and are being managed. Supplementary questions or comments also indicate what good practice looks like.

Facility Major Incidents & Barriers

A1 What process do we have to identify major ‘loss of asset integrity’ scenarios?
  • Is there a list? Is it realistic?
  • Who is responsible for identifying, assessing and managing these major incident risks? Do they have suitable skills, and resources?
  • How would a new person learn about all this?

A2 In the context of current operations, what is one major incident scenario for this facility, and how could it escalate from an initial minor event?
  • How often can the initial event happen? How likely is it to escalate?
  • How far would the effects extend, initially and after escalation? (Heat radiation, explosion damage, smoke, etc. – this checks use of a suitable consequence model)
  • Could effects extend beyond the asset? Have neighbours been informed?

A3 For this scenario, what barriers ensure the risk is acceptably low? Which are your most important barriers and why?
  [this checks knowledge of specific major incident scenarios at the facility, understanding of associated barriers and their value in preventing such incidents]
  • How are key barriers and related Performance Standards defined and recorded?
  • Are structural failure, extreme weather and collision/impact barriers considered, as appropriate?

A4 What do we do when a barrier is by-passed or degraded (not fully operational)?
  • Does everyone involved understand and actively manage all the barriers needed to avoid major incidents? How do we know when barriers are degraded?
  • How do we respond when barriers are known to be degraded, etc. (including during maintenance)? What compensating systems are put in place?
  • Do you have written guidance about when to shut down if one or more barriers are degraded?

A5 How many safety device overrides do you currently have in your area?
  How were they authorised? Where are they recorded?
  • Are they all temporary? If some are long-term, for how long have these been authorised?
  • What additional measures do you have in place to compensate?
A6 What metrics/KPIs do you use for asset integrity performance?
- Do they cover all the main headings in this guide? If using CCPS Standard, how does performance compare with others?

A7 Do we follow up on loss-of-integrity incidents with suitable actions?
- How are you sure that possible management failings are considered, as well as those of workers?
- Is action closeout always timely? How many open items on the current list?

A8 What are the current focus areas for further reducing the probability of a major incident occurring? What have we done in the past 2–5 years?
- Is there a ‘continual improvement’ approach to managing major incident risk?
- Is there a documented management review within the past 2 years?

Critical Equipment (Hardware Barriers)

B1 How do we identify safety-critical equipment and devices? Which are linked to reducing the risk of major incidents?
- Is there a standard definition and practice for critical equipment categorisation?
- Who determines criticality? Do operations and technical authorities work well together?
- Is some non-critical equipment included, because of a role in ensuring personal safety?

B2 Are there clear Performance Standards for equipment critical to asset integrity?
- Do these cover reliability, availability, survivability, as well as what the equipment is designed to do?
- Which Performance Standards are met by the basic design specification, which have to be site tested or verified?
- How is barrier reliability and availability checked against the Performance Standards?

B3 How do we test each barrier (or equipment item), to make sure it works as intended? Do we ever test the whole barrier?
- Where are the records for the last test on each barrier or component? Do they include details of the test results or measurements and who did them?
- What would you do if a test was either missed or failed? When would you consider ceasing operations? Are relevant decision criteria documented and available?
- If the whole barrier is never tested, why not?
- How is actual barrier performance communicated and to whom? (Workers affected if it failed in a real incident, Asset Manager, Technical Authorities?)
B4 Do we deviate from supplier recommended inspection or maintenance frequencies? If so, how are deviations justified?
   • Are there sufficient records to justify increasing/decreasing intervals?
   • Do changes have to be approved by a competent technical authority?

B5 What is the current backlog of maintenance/inspection for critical equipment? Who monitors this?
   • Who is authorised to approve a delay/deferment? For how long?
   • Do records show an improving or deteriorating trend?
   • Have you ever shut down because critical equipment performance verification was overdue? Who made that decision? (Should not require high-level authorisation)

B6 Is there an up-to-date Management of Change (MoC) procedure? How does it apply for critical equipment (hardware barriers)?
   • How many changes to critical equipment have been registered in the last month/year?
   • How many are still being progressed?
   • How soon are all relevant drawings, documents, etc., updated after a change is made?

B7 How does the MoC process apply for minor changes to critical equipment, e.g., change of material spec, chemical dosing or alarm/trip settings?
   Permanent changes should be assessed by MoC process, with technical authority involvement and approval. Temporary changes should also be assessed, then recorded and time-bound.

B8 Are operating limits for all process equipment clear? Who is allowed to deviate from or change them?
   • Do all operating limits that are not self-limiting have alarms and trips?
   • Does the local MoC procedure cover permanent changes to alarm and trip settings?
   • Are all trip defeats recorded and made only by authorised persons?

B9 In typical operations, how often do alarms activate? Do all alarms require a response action (in addition to acknowledging the alarm to silence it)?
   • What is the proportion of ‘nuisance alarms’? If this is high, has any rationalisation taken place?
People and Processes

C1 Are there always sufficient competent people to operate, inspect and maintain the facility?
- How do we know our people are technically competent, including supervisors?
- What about long-term and short-term contractors?
- What about vacations and in emergencies? How do we maintain group competence? When some members are absent or are new workers?
- Are critical tasks ever carried out alone by persons not yet assessed as competent? (This may be part of their training, but they should not be alone)
- Who determines competence? (Self-assessed? Supervisor? Independent assessor? Are assessments recorded?)

C2 How do we ensure supervisors and managers are competent as leaders and in their understanding of this facility?
- Do competences include understanding of asset integrity barriers and their contributions to preventing, controlling and mitigating major incidents?
- Are all critical task competences assessed pre-appointment?
- Are there any challenges in ensuring this standard? (e.g., shortage of good people, need to rotate them, etc.)

C3 Are responsibilities for the performance of critical equipment/asset integrity barriers clear?
- Are both operations and technical authorities involved?
- Are timely decisions about required changes made and implemented as needed?
- Do operations personnel contribute suitably to technical studies and reviews (risk assessments, Hazops, etc.)?
- Do technicians have all the tools and equipment needed to efficiently operate, inspect and maintain the facility? Are these calibrated as appropriate?

C4 Is there a robust permit system in place to manage tasks that may affect asset integrity? Are all persons trained in its use and assessed before being authorised to sign any section?
- What are the hardest areas to implement consistently?
- Are Permits ever issued for tasks that involve no risks to or controls implemented by anyone other than those doing the work, if so why? (Detracts from higher risks)
- How do we decide what isolation standard is required for ‘live working’? How do we integrity test before re-introducing process fluids? (Operations standards for both should be defined, in agreement with technical authorities)
C5 How are workers using task risk assessments to identify situations that could affect asset integrity? Are there agreed standards for performing tasks that could directly affect the integrity of the asset?

- Are workers using JSA and personal task risk evaluation to consider ‘worst case’ asset integrity hazards or consequences (in addition to personal injury exposures)?
- Are there written standards/guidance for activities such as: start-up/shutdown/recovery; working on ‘live’ systems; opening process equipment, etc.? Have technical authorities and operations both contributed to the standards?

C6 Do the emergency response procedures include major incidents? How do we know the scenarios are realistic? Is everyone confident that barriers will work as intended?

- How are training and exercise scenarios linked to realistic failures of the key barriers?
- How do we simulate major incidents (fire, explosion, etc.) to provide realistic experience?
- Are all response authorities and deputies trained in major emergency scenarios?
- Are complex systems ever tested overall (e.g., ESD, full-scale flaring, HVAC shutdown, lifeboat launch and recovery)?

C7 How quickly do we usually detect and respond to a minor process fluid release to prevent it from escalating?

- Does this apply everywhere? (e.g., open areas, where detection is harder)
- Are there always enough people to patrol critical areas? (e.g., nights, weekends)
- In areas with no automatic detection, will personnel reliably detect a release, as it is a rare event?
Projects

D1 Are roles, responsibilities and accountability for asset integrity management and major incident risk reduction clearly and adequately defined for this project?
- What has been done to minimise life cycle risk, not just capital cost?
- How are barrier Performance Standards optimised during detail design?
- How can you be sure the overall major incident risk is acceptably low?

D2 In selecting a development concept or design how do you optimise asset integrity management/major incident risk reduction and assure it is achievable throughout the facility life?
- Which options were considered? What factors led to the selected option?
- What major hazard studies were/will be used to aid selection as the design develops?
- What examples are there of considering total life cycle cost, not just initial cost?

D3 How are asset integrity expectations and barrier optimisation communicated to designers?
- Are there examples of going beyond required minimum standards?
- How is operations concurrence with selected design options obtained?

D4 How are major incident barrier Performance Standards communicated to operations?
- Do any novel Performance Standards need to be verified by type tests during the design phase?
- How are Performance Standards verified before or during commissioning?
- How do reliability/availability expectations compare with what we achieve in existing facilities?

D5 Is there a readily available catalogue of the codes and standards utilised to design barriers?
- How were specific standards selected and what assurance process was followed to demonstrate their application?
- How do Technical Authorities and others use the catalogue?
- Has the catalogue been maintained? What changes have been made to the facility in response to revisions to codes and standards?
Culture

E1 What do you see as the important differences between personal and process safety?
There should be many similarities, e.g., both high priority, tracked with leading and lagging indicators and with clear management leadership actions. However, process safety risk assessments will more often be complex, and require specialist people and tools to select and optimise barriers. Operators and technicians are likely to have less detailed experience/understanding of the consequences when barriers fail, and thus may not fully understand the basis for some operating limits.

E2 How often does management discuss facility-specific major incident scenarios and the effectiveness of barriers with supervisors and operators on your facility?
• What are the greatest concerns of operations and of technical authorities? What is being done about these?
• Have supervisors and operators made improvement suggestions? How are these being actioned?

E3 What are we doing to improve the ability of workers at this facility to identify and raise concerns about situations that may contribute to a process incident?
Workers must be competent to recognise a deficiency or concern and must also feel empowered to take action to resolve it.

E4 Is there a plan to audit and review our barriers for managing major incident risks? Are we meeting that plan?
• Are there systematic reviews that specifically consider asset integrity and major incident risks?
• What data sources, including audits, are fed into the review?
• Is auditing done by truly independent and competent people?
• What strengths have been reported in recent audits, and what weaknesses?
• What actions have followed the review?

E5 Do people here feel management would support them if they stopped a job, or stopped production because major incident barriers were degraded?
• Do you have recent examples? Does everyone agree?
• For those unsure about management support, what would you do to change that?
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 in the Introduction.

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 and 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 escalation 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.
References


IOGP Report 544, Standardization of barrier definitions. 2016


IOGP Report 460 - Cognitive issues associated with process safety and environmental incidents

IOGP’s Managing Major Incident Risks Task Force 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 life cycle 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.