ASSURANCE AND VERIFICATION PRACTITIONERS’ GUIDANCE DOCUMENT

Improving safety and effecting change through collaboration
Contents

1. Introduction 03
2. Legislation 04
3. Management of Major Accident Hazards 06
4. Assurance Process 10
5. Verification 15
6. Verification Interface with Other ICPs 30
   Glossary 31
   Appendix 1 33
   Appendix 2 39
   Appendix 3 41
   Appendix 4 49
   Appendix 5 52
Offshore oil and gas is a unique industry where we work and live in relatively close proximity to large inventories of flammable and toxic substances. This brings significant challenges in the event of an emergency, when there is an urgent need to distance ourselves quickly from the hazard or even to evacuate or escape by air or sea. It is therefore clear that offshore installations demand a high level of attention to risk management.

Following the Piper Alpha disaster, Lord Cullen’s inquiry and report raised 106 recommendations that were endorsed by the UK government and led to a suite of new goal-setting safety legislation. This safety regime was intended to put in place mandatory requirements which, if followed correctly, would reduce the likelihood that such a major accident could happen again. Today, this legislation remains the framework we use to address and manage the risks of Major Accident Hazards (MAHs) on offshore oil and gas installations within UK waters.

The Safety Case Regulations require duty holders to define Safety & Environmental Critical Elements (SECEs) and specified plant; this is the equipment, plant or software which prevents, controls or mitigates against the effects of Major Accident Hazards (MAHs), including the result of a subsequent Major Environmental Incident (MEI). Measurable minimum standards known as Performance Standards must be defined for each SECE. Performance Standards must be met at all stages of the installation’s lifecycle, i.e. when the installation is designed or modified, throughout operations, including decommissioning and abandonment.

The Assurance process is what the duty holder does to confirm SECEs are, and remain suitable throughout each phase of the installation’s lifecycle. This assurance process is checked by an Independent and Competent Person (ICP), known as the ‘Verifier’, through the process known as ‘Verification.’

The output from the Verification process is a report from the Verifier detailing the work carried out and, where applicable, the findings and associated recommended remedial action. Duty holders must take appropriate actions and respond to all findings and recommended remedial actions within an agreed timeframe.

The suite of Offshore Safety Regulations and associated Assurance and Verification processes is internationally recognised as best practice.

Step Change in Safety has developed this Assurance & Verification guidance to improve an understanding of:

- MAHs, MEIs, SECEs and Performance Standards
- Assurance & Verification processes
- The role and function of the Verifier

This guidance supports Step Change in Safety’s Major Accident Hazard Understanding programme to help the whole workforce, boardroom to tea shack, understand what an MAH is, how they are identified and how they are mitigated against.
Offshore Installations (Offshore Safety Directive) (Safety Case etc.) Regulations 2015 (SCR)

These Regulations require the risks from major accident hazards to the health and safety of the workforce offshore and any resulting major environmental incident to be managed. The regulations implement the main recommendations of Lord Cullen’s Report of the Public Inquiry into the Piper Alpha Disaster and also now incorporate the additional requirements of Directive 2013/30/EU on the safety of offshore oil and gas operations.

Offshore installations operating within the UK Continental Shelf (UKCS) are required to have a Safety Case which has been accepted by the Competent Authority.

The Safety Case includes a series of formal assessments which demonstrate:

- All major accident risks have been evaluated and their likelihood and consequences assessed
- The means to control major accident risks effectively is defined, implemented and maintained
- The design of the offshore facility and its management systems are consistent with the requirement for safe and responsible operation and include:
  - Risks to personnel and the environment are As Low As Reasonably Practicable (ALARP)
  - Arrangements are in place to protect personnel from hazardous events and protect the environment from significant adverse effects

The content of the Safety Case should include a description of the installation; its plant, pipelines within 500m of the installation, operations and combined operations; a description of the Verification scheme and the arrangements in place to protect personnel from hazardous events and situations.

The Safety Case includes a demonstration of how the duty holder assures legislative compliance with regards to the identification of Major Accident Hazards (MAHs), and the evaluation of the risks and provisions to manage these. A description of the ‘Verification Scheme’ and ‘Well Examination Scheme’ must also be included within the Safety Case.

The establishment of the verification scheme is required by SCR2015 Regulation 9. Further requirements are detailed in Regulation 10, Regulation 13(1) and Schedule 4 (Part 1)

The establishment of the well examination scheme is required by SCR2015 Regulation 11. Further requirements are detailed in Regulation 12, Regulation 13(2) and Schedule 4 (Part 2)
The Offshore Installations (Prevention of Fire and Explosion, and Emergency Response) Regulations (PFEER) (2015)

These Regulations are aimed at all those who own, operate or work on offshore installations and look at how to prevent fires and explosions as well as how to protect people working on offshore installations should they occur. It also looks at how to respond to emergencies, considering issues such as escape, evacuation, rescue and recovery.

These Regulations require that the duty holder takes appropriate measures to protect personnel on the installation from fire and explosion and secures an effective emergency response. The duty holder must assess and identify events which could give rise to a Major Accident involving fire or explosion; or the need for evacuation, escape or rescue to avoid or minimise the consequences of a Major Accident.

The equipment defined within PFEER as ‘Specified Plant’ should also be defined as Safety Critical and is therefore covered by Assurance and Verification.

The Offshore Installations and Wells (Design and Construction, etc) Regulations (DCR) (1996)

These regulations place goal-setting duties on installation owners and operators to ensure the integrity of an installation throughout its lifecycle. They provide a framework for ensuring the safe condition of wells on land and offshore, including an examination scheme, and implement the European Commission Extractive Industries (Boreholes) Directive with provisions mainly relating to the workplace environment.

These Regulations require all wells to be covered by a Well Examination Scheme. This scheme represents the activities performed by a Well Examiner to confirm that wells are designed, constructed, commissioned, operated, maintained, modified (including interventions and workovers) and abandoned in a safe and appropriate manner. The Well Examiner is an Independent Competent Person (ICP) appointed by the Well Operator (normally also the duty holder).

The requirements for the Well Examination Scheme have also been replicated within the 2015 Safety Case Regulation.

Wells are Safety Critical and fall under both Well Examination and Verification schemes. The Competent Authority does not expect work to be repeated or duplicated, but clear boundaries and interfaces between the schemes must be established to ensure all aspects are covered and legislative requirements are fully met.
Chapter 3.
Management of Major Accident Hazards

Major Accidents are events which cause or have significant potential to cause death, serious injury or major damage to plant – the full definition of Major Accident is given in Safety Case Regulations (2015).

Once identified, these Major Accident Hazards (MAH) must be assessed and managed. This means defining control measures to prevent or mitigate the hazard, then ensuring that these control measures remain effective for the entire life cycle of the installation. Details of the installation, MAHs, risks and how these risks are managed are contained within the Safety Case – a living document which must be written, submitted to and accepted by the Competent Authority before an installation can operate within the UK Continental Shelf (UKCS). Duty holders should assign SECE owners to ensure that systems are managed throughout their lifetime.

Safety and Environmental Critical Elements

Duty holders are required to define the barriers, or controls, in place to manage MAHs present on their installations. Safety and Environmental Critical Elements are:

parts of an installation and such of its plant (including computer programmes), or any part of those

(a) the failure of which could cause or contribute substantially to a major accident; or
(b) a purpose of which is to prevent, or limit the effect of, a major accident

Examples of SECEs can be found in Appendix 1.
Performance Standards

Having identified the Safety and Environmental Critical Elements (SECEs), duty holders must then define clear pass/fail acceptance criteria to prevent the major accident from occurring or escalating. If each SECE meets its Performance Standard the likelihood of a Major Accident occurring is reduced. The performance standard acceptance criteria must be relevant for all stages of the installation’s lifecycle including:

- Design, transportation, construction, hook up and commissioning
- Operations including management of change
- Decommissioning & Abandonment

Performance Standards should be written for each SECE at a system level, focusing on what the system is required to achieve. The requirements of the SECE may be described in terms of:

<table>
<thead>
<tr>
<th>Goal</th>
<th>What’s the purpose of SECE from a safety and environmental critical perspective? This should be linked to the relevant MAHs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boundary</td>
<td>Which items of equipment does the Performance Standard apply to?</td>
</tr>
<tr>
<td>Functionality</td>
<td>What the SECE must do from a safety and environmental critical perspective?</td>
</tr>
<tr>
<td>Availability</td>
<td>Will it be ready and able to perform when required?</td>
</tr>
<tr>
<td>Reliability</td>
<td>Will it function dependably?</td>
</tr>
<tr>
<td>Survivability</td>
<td>What kind of events does it need to survive and for how long?</td>
</tr>
<tr>
<td>Interactions</td>
<td>What systems the SECE interact with?</td>
</tr>
</tbody>
</table>

The Performance Standard acceptance criteria must be clear, measurable and auditable i.e. it must be possible to demonstrate the SECE meets the criteria. It is beneficial to include a reference as to how the criteria was derived within the Performance Standard. Performance Standards should be periodically reviewed to incorporate modifications, changes in operating conditions or to incorporate new learnings.

Examples of Performance Standards are given in Appendix 2.
Managing MAHs Through Barriers

A series of barriers (plant, process and people) are put in place to manage and control the Major Accident Hazard.

Safety and environmentally critical equipment (plant barriers) can be grouped by their function in defending people, plant and the environment from the hazard. No barrier is infallible and therefore multiple barriers must be in place. It is important that the barriers are independent of each other such that failure of one barrier does not result in the failure of another.

These barriers working together can be visualised through the ‘Swiss Cheese’ model and bowties.

‘Swiss Cheese’ barrier model

The ‘Swiss Cheese’ model shown below is a concept defined by James Reason and illustrates simple examples of SECE barriers in a loss of containment Major Accident scenario; the holes in the barriers are the SECEs failing to meet their Performance Standards and cause a path through which the hazard is realised.

Figure 1. ‘Swiss Cheese’ barrier model
Bowtie approach

A bowtie can be used to depict the multiple causes of a Major Accident and the barriers that are in place to prevent an event occurring. The event is in the centre of a bowtie with the potential threat / hazards listed on the left-hand side and control / mitigation barriers shown on the right-hand side. Each branch from hazard to consequence can be imagined as a single ‘Swiss Cheese’ model.

Examples of simplified bowties are shown below.

![Sample simplified bowtie diagrams](image)

Figure 2. Sample simplified bowtie diagrams
Chapter 4. Assurance Process

Assurance of SECEs is the activities performed by the duty holder to ensure SECEs meet the Performance Standard requirements for all phases of the installation lifecycle.

It is important that personnel understand how their activities interact with SECEs and their role in helping manage Major Accident Hazards. Duty holders should ensure that persons with a responsibility for SECEs are competent.

Assurance processes include many aspects of duty holder operations and are likely to include:

- Management of engineering change
- Operational Assurance activities
- Integrity management processes
- Actions to mitigate the risks due to degraded equipment
- Management of temporary equipment
- Continuous monitoring and management review
- Confirmation that availability and reliability targets are met

Duty holders should have in place appropriate systems for monitoring compliance and effectiveness of these programmes. This is often referred to as ‘plan, do, check, act’ and forms the framework for a widely recognised safety management system.

Figure 3. Integrity management system
4.1 Management of engineering change

An engineering change must assess the potential to affect SECEs and Major Accident Hazard. The duty holder’s SECE assurance process for engineering change must include the identification of new or impacted SECE, identifying or defining new performance standards then checking those standards are met for design, procurement, construction, commissioning, decommissioning and abandonment.

Where an engineering contractor is used, the duty holder remains accountable and must therefore ensure adequate processes and procedures are in place to confirm the new or impacted SECEs comply with the Performance Standard requirements and that Performance Standards are updated as necessary.

The duty holder must ensure the independent Verifier carries out appropriate Verification activities (see section 5.4)

4.2 Operational Assurance activities

Operational SECE Assurance is the activities carried out by the duty holder to confirm the equipment in service continues to meet its Performance Standard requirements. These activities are generally managed through a Computerised Maintenance Management System (CMMS) but may also include routine checks by operators.

Maintenance regimes, e.g. lubricating valves or dampers, changing engine oil, will be generally carried out in accordance with the manufacturer’s recommendations. ‘SECE Maintenance’ are those same activities carried out on equipment identified as safety and environmentally critical.

‘SECE Assurance’ is the check to confirm safety and environmental critical equipment continues to meet its Performance Standards. It confirms the SECE maintenance activities are appropriate and effective, e.g.

- Confirming fire and gas detectors function and alarm within the specified range
- Confirming valves operate and open / close within the specified times
- Confirming ESD logic operates as per the cause and effect charts
- Confirming blow down depressurisation rates meet the requirements
- Confirming firefighting systems operate on demand and deliver the required pressure / flowrates
- Confirming emergency response equipment remains available and functional

Measures should be in place to ensure that Assurance activities are carried out fully and in accordance with defined schedules. A deferral process should manage the risks associated with any delays to safety and environmental critical maintenance and assurance activities.

When an Assurance activity has been completed, the status of equipment to meet its Performance Standard should be positively reported and recorded, e.g. ‘as found’, ‘pass’, ‘fail and fix’, or ‘fail’. Data should be recorded in a manner that supports:

- Monitoring MAH barriers / KPIs
- Calculating failure rates, reliability and availability statistics
- Current status of SECEs to meet its Performance Standard
- Identifying when to implement mitigating measures
- Maintenance optimisation
The MMS serves as a data repository for maintenance and Assurance records through the lifecycle of an offshore installation. All relevant information should be accurately recorded and can then be used to demonstrate compliance with Performance Standards and for analysis, e.g., equipment condition, resources, failure / damage codes, inspection records, certification etc.

When checking equipment against performance standards, it is important to record the “as found” condition to understand what would happen if the equipment were required to operate under an MAH scenario. As found results can also be used for calculating reliability and used for Maintenance optimisation, i.e. increasing or decreasing maintenance and test frequencies.

The equipment’s ability to meet its performance standard after any tests or repairs has been carried out, its “as left” status, is equally important as this is used to determine where an Operational Risk Assessment should be carried out and what mitigating measures should be implemented. The time between failure and fix can also be used when calculating availability.

4.3 Integrity management

Integrity management is the processes carried out by the duty holder on static systems, which degrade over time, to ensure they remain fit for purpose throughout their service life (pipework, vessels, structure etc). The activities carried out include inspection, assessment and repair.

A robust integrity management system must be in place to ensure relevant SECEs remain fit for purpose throughout their lifespan. Integrity management is a key element of the assurance processes and includes:

- Inspection on topside structures, blast walls and passive fire protection
- Inspection on topside hydrocarbon systems
- Inspection on subsea facilities, e.g. pipelines, structures and manifolds
- Lifting equipment inspections
- Hose inspections
- Anomaly management
- Asset register
- Temporary repair process
4.4 Actions to mitigate risks from degraded equipment

When a SECE fails to meet its Performance Standard, immediate measures must be taken to assess and mitigate the risks to personnel on the installation. If the SECE is operable but in a degraded state, the risk assessment should determine if it is safe to continue using that equipment. Temporary mitigating measures should be implemented to reduce the identified hazards to as low as practicable and help support the justification for continued use, e.g. lower operating pressures, additional gas detectors. Oil & Gas UK’s Operational Risk Assessment Guidance gives more details on this (HS071).

Limits should be set for the continued use of the degraded equipment and the mitigating measures monitored until a permanent repair has been carried out. The risk assessment and justification for continued use must be documented and approved by the relevant Technical Authorities or equivalent.

Where SECE degradation or failure is such that there is a significant increase in the risk of a major accident, the duty holder must take suitable measures to ensure the risk is reduced to as low as reasonably practicable and take into account the cumulative risk. An example of such a situation may be failure of multiple barriers against one of the Major Accident scenarios. Where this occurs, the duty holder must notify the competent authority within 24 hours (see Offshore Safety Case Regulations, reg. 29).

4.5 Management of temporary equipment

Temporary equipment may introduce additional hazards or interact with SECEs. Duty holders therefore require effective management procedures for Assurance (and Verification) to ensure initial and continued suitability of temporary equipment.

A typical control process for temporary equipment may involve:

- Define SECEs impacted or any new SECEs introduced and subsequent Performance Standard requirements
- Specification of the equipment requirements
- Risk assessment of the equipment specification use and location
- Procurement of equipment to meet specification
- Assuring the equipment meets its specification and Performance Standards through inspection and testing
- Receive equipment offshore, check for transit damage and ensure correct documentation has been provided, confirm suitability for hook-up at location and enter details into temporary equipment register
- Ongoing Assurance of ‘continued suitability’ while onboard and in use

Duty holders should define a time limit for equipment to be regarded as temporary. For large load-outs of temporary equipment with multiple tie-ins to installation systems, the Management of Engineering Change process may be a more appropriate means to control temporary equipment.
4.6 Continuous monitoring and management review

The duty holder should aim to assess the effect of cumulative risk of impairments and failures on SECEs across all areas of plant, equipment and systems. See Oil & Gas UK’s Cumulative Risk Guidelines 2016 [HSE03]).

Key Performance Indicators (KPIs) are a recommended feature of a good management system. The indicators can be ‘leading’, where they flag low performance which could lead to problems or failures ahead, or ‘lagging’, where they record numbers of defects or failures.

KPIs will vary for each duty holder. However, it is essential to provide clear definition to ensure information is both consistently reported and understood. Examples of KPIs include safety critical maintenance backlog, number of inhibits / isolations under management, number of impaired SECEs, number of safety critical anomalies, Verification findings etc. These KPIs can then also be linked to MAHs.

Formal processes for the identification, monitoring, measurement and trending of performance indicators should be in place, and measured results should be tracked against performance targets to demonstrate compliance, delivery or improvement.

Audits of the activities defined and performed under the Assurance processes should be carried out periodically and used to drive improvement of the processes.

Figure 4. Example of an integrity dashboard
Chapter 5. Verification

5.1 Verification overview

Verification is an independent check of the duty holder’s Assurance process to confirm initial and continuing suitability of the Safety & Environmental Critical Elements (SECEs). The Verification process cannot be used as an alternative inspection regime.

Verification activities are defined within the ‘Verification scheme’ and are carried out by a ‘Verifier’ who is an Independent and Competent Person (ICP) appointed by the duty holder.

With regards to compliance with the regulations for Verification, duty holders are accountable for:

- Appointing the Verifier
- Ensuring all Verifier(s) are independent and competent
- Producing the list of SECEs
- Ensuring a Verification scheme is developed by, or in consultation with the Verifier
- Ensuring the Verifier reviews and comments on the list of SECEs and the Verification scheme
- Ensuring that the scheme is implemented and maintained
- Ensuring the activities defined by that scheme are completed by the Verifier
- Acting upon any findings and remedial actions recommended raised by the Verifier within a specified time frame
- Providing the Verifier with information necessary for proper implementation or revision of the scheme
- Providing the Verifier with the appropriate level of authority to carry out their role

The Verifier is appointed by the duty holder to undertake the activities defined within the Verification scheme, which is owned and maintained by the duty holder.

A good Verification process will not only ensure compliance with legislation, but will drive real improvements to the SECE Assurance process (See examples of Verification benefits in Appendix 4)

Duty holder senior management must support the Verification process within the duty holder’s organisation and provide adequate resources and financial provisions for the correct implementation and management of the process. Failure to implement an appropriate Verification scheme or complete the defined activities is a failure to comply with the Safety Case Regulations. The duty holder must have an effective communications process with the Verifier.
5.2 Independence of the Verifier

Duty holders must ensure the selected Verifier is independent from the duty holder; this includes both the design of the installation and the management systems / reporting lines.

‘Independence’ Definition, SCR 2 (7):

… a person is to be regarded as independent only where -

(a) the person’s function will not involve the consideration by that person of an aspect of something liable to be examined under regulation 9 (Establishment of verification scheme) or 11 (Establishment of well examination scheme) for which that person bears or has borne responsibility or where that person’s objectivity may be compromised; and

(b) the person is sufficiently independent of a management system which has, or has had, any responsibility for any aspect of something liable to be examined by the person under regulation 9 or 11 so as to ensure objectivity in carrying out the person’s functions under the scheme.

The Verification scheme should outline the principles applied by the duty holder in selecting a Verifier to carry out work under the Verification scheme. The information provided should detail how the Verifier’s technical expertise, knowledge, experience and independence were determined.
5.3 Competence

Duty holders must ensure the selected Verifier has the relevant competency. Those undertaking Verification activities must be competent and qualified to do so (e.g. technical expertise, qualifications and sufficient experience to undertake specific roles).

‘Competence’ Definition; SCR Interpretation:

… a person is not to be regarded as competent unless, in particular, the person has such reasonable technical competence as is sufficient for the person to carry out the functions of an independent and competent person under these Regulations, under a verification scheme or, as the case may be, a well examination scheme.

Each Verifier should have a documented competence system, with traceable means of assessment, clearly stating the criteria and method of assessing the individual. A Verifier’s competency scheme should contain the following elements:

• Competency criteria by engineering discipline or SECE specific
• Detailed criteria to define competence – in general a combination of technical knowledge and experience is required
• Frequency of review and assessment
• Definition of which lifecycle phase the person is considered competent for
• Various levels of competence may be defined

The duty holder should carry out regular competency reviews to ensure compliance against this process; those reviews are likely to include the following:

• Review of the Verifier’s competency management system
• Reviewing competency criteria by discipline and installation lifecycle
• Reviewing / approving specified competency levels for Verifiers
• Reviewing how tasks within the scheme are allocated to personnel qualified to undertake them

The duty holder’s Verification Scheme or Verifier’s own quality management system should define how any deficiencies in the competence management programme are to be addressed.

5.4 Verification scheme – nature and frequency

The Verification scheme defines how the Verifier will confirm the SECEs will be, are, and remain suitable for each phase of an installation’s lifecycle. The Verifier should carry out sufficient activities, as defined by the scheme, in order to form a professional judgement whether the SECEs are likely to remain in good condition and repair. Implementation of the scheme provides an independent view on the effectiveness of the duty holder’s assurance process and should confirm the parts of the installation deemed safety critical are, and remain, suitable.
The duty holder must ensure that a Verification scheme is developed by, or in consultation with, a Verifier.

Safety Case Regulations (2015) Regulation 10 (1) Schedule 4

1. The principles to be applied by the duty holder—
   (a) in selecting a verifier to perform functions under the scheme; and
   (b) in keeping the scheme under review.

2. The arrangements for the communication to the verifier of information necessary for the proper implementation, or revision, of the scheme.

3. The nature and frequency of examination and testing.

4. The arrangements for the making and preservation of records showing—
   (a) the examination and testing carried out;
   (b) the findings of the examination and testing;
   (c) any remedial action recommended; and
   (d) the remedial action performed.

5. The arrangements for communicating the matters specified in paragraph 4 to an appropriate level in the management system of the duty holder for the installation.

6. The arrangements for review and revision of the scheme.

Items 1, 2, 4, 5, and 6 can be grouped together by duty holders to form a ‘Verification scheme procedure’, i.e. the details of how they will manage the Verification process within the scheme.

Item 3 ‘nature and frequency’ defines what the Verifier will do in terms of activity, sample size and frequency. These activities are linked to the Performance Standards and are therefore specific and different for each phase of the installations lifecycle.

Duty holders should detail how they manage the verification process. This is typically done through a procedure or in the Verification scheme and would normally be integrated into the duty holder’s safety and environmental management system.

The process of how to manage Verification (operations / modifications / projects) should define requirements for:

1. Planning:
   • Ensure effective interface between Verifier and planning departments
   • Ensure good communications prior to execution of Verification activities with relevant personnel making them aware of the proposed Verification scope
2. Reporting of Verification activities
3. Reporting of Verification findings
4. Clear lines of communication between the Verifier / duty holder and engineering contractor where appropriate (an organisation chart may be beneficial here to identify key positions)
5. Review and revision of the Verification scheme
6. Describe how both the arrangements for well examination and the Verification scheme interact
7. Verification roles and responsibilities
8. The principles for selection of the Verifier. Defined criteria for the appointment of the Verifier, including measures to ensure their competence and independence.

A suitable scheme must include a commitment by both the duty holder and the verifier to a defined level of activity. What level is appropriate will vary considerably depending on the particular criticality, previous performance and number of the SECEs. For example:

• A high integrity protection system, preventing the over-pressurisation of a hydrocarbon system, may require to have its functionality regularly witnessed by the Verifier

• A fire and gas detection system with many detectors could be covered by the witnessing of an appropriate representative sample of the actual testing regime

• Where Verification activity is also carried out by the review of test records and results, similar principles apply. Sample size is particularly significant in this instance when the Performance Standard of a SECE requires the ongoing check of its availability / reliability

This should apply to operational, project and modification Verification schemes. The nature of the activity to be completed by the Verifier should be clearly stated. Terms such as ‘Verifier discretion’ / ‘witness or review’ should be avoided because these may allow the activity to be influenced by resource or budget constraints etc.

The guide to the SCR (Schedule 4 Para 401) states that there should be arrangements made to ensure that the sample taken is not repeatedly tested. The duty holder should therefore ensure this is addressed within the Verification Scheme. An example of how sample size can be defined within the verification scheme, is included in Appendix 5.

5.5 Verification scheme - review and revision

A Verification scheme should be subject to continual monitoring and periodic review throughout the installation’s life cycle. These arrangements could include the requirement for an annual review or a more fundamental revision in line with safety case reviews and revisions; these principals must be outlined within the scheme.

In addition to periodic reviews, a Verification Scheme review may be initiated by any number of scenarios such as:

• Regulations update
• Change of duty holder
• Revision of any codes or standards referenced in the Verification scheme
• Updates to safety case
• Updates to the list of SECEs, or Performance Standards
• Modification / projects
• Findings from audits and incident investigations
• Changes to the installation operating conditions
• Appointment of a new Independent Verifier

Changes to the Verification scheme need to be managed to ensure all relevant personnel are made aware and necessary approvals are obtained. The Verifier will need to be involved and depending upon the nature of the change could also include SECE Performance Standard owners, technical authorities, subject matter experts, discipline engineers, safety engineering and Verification focal points.

Audits of the Verification management process should be carried out on a periodic basis and should include all key stakeholders. These audits should also include the verifier to ensure that the process remains compliant with the legislation.
5.6 Initial suitability Verification (projects / modifications)

Verification schemes are required for the lifecycle of the installation and should therefore include greenfield projects (all new) and brownfield modifications (engineering change to existing facilities). The Verification activities that will be carried out by the Verifier will be based on new or impacted SECEs and defined within the Verification scheme.

The Verification activities for initial suitability must be in place and agreed between the duty holder and Verifier before the completion of the design (SCR 2015 Regulation 9, (5)) and, where practicable, carried out before the SECEs are brought into operation.

Examples of initial suitability verification activities:

<table>
<thead>
<tr>
<th>Phase</th>
<th>Duty Holder SECE Assurance</th>
<th>Verification Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>SECE identification</td>
<td>Identify and record SECEs being installed or impacted by the project / modification</td>
<td>Review and comment on the list of SECEs</td>
</tr>
<tr>
<td>Verification scheme nature and frequency</td>
<td>Develop the Verification scheme activities or approve the Verifiers proposal</td>
<td>Review or develop the Verification activities for the project / modification</td>
</tr>
<tr>
<td>Design</td>
<td>Develop / update design documents: P&amp;IDs / C&amp;Es / calculations / specification datasheets etc</td>
<td>Review design documentation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Audit design process</td>
</tr>
<tr>
<td>Procurement</td>
<td>Quality assurance checks on equipment / materials ordered and received</td>
<td>Review / examine procurement orders and goods received</td>
</tr>
<tr>
<td>Fabrication / construction</td>
<td>Factory acceptance testing quality assurance inspections / reviews</td>
<td>Examine / witness fabrication / construction</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Review fabrication / construction dossiers (material / welding / NDT / testing records)</td>
</tr>
<tr>
<td>Transportation / installation</td>
<td>Quality assurance inspections</td>
<td>Examine equipment, review records, witness installation</td>
</tr>
<tr>
<td>Site commissioning</td>
<td>Site Acceptance Testing / hydrocarbon Leak testing of SECEs to assure compliance with Performance Standards</td>
<td>Witness testing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Examine equipment against design</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Review records</td>
</tr>
<tr>
<td>Close out / handover to operations</td>
<td>Compile and review closeout packs Populate relevant databases for SECE maintenance / inspection</td>
<td>Review punch-list items</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Review technical deviations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Review databases for population of new equipment and suitability of assigned operational assurance activities, e.g. maintenance / inspection</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Review outstanding punch-list items and status of Verification</td>
</tr>
</tbody>
</table>

Notes:

1) The duty holder must ensure that the Performance Standards are being met by embedding them into each phase of the Assurance process and making people accountable for compliance. This can be achieved by obtaining appropriate engineering signatures to confirm compliance to the Performance Standards at key stages.

2) The duty holder can request the engineering contractor to provide a list of the documents (master document register, MDR) that will demonstrate compliance of each impacted SECE against the applicable Performance Standard criteria. This approach raises awareness with the engineering contractor of their duty to comply with the Performance Standards.

3) Like-for-like replacements may require Verification for initial suitability, since in some cases, the manufacturer may have modified or improved their product.
One method of creating a verification scope for an engineering change is to prepare a list of initial suitability Verification activities defined for each SECE that can be used to develop specific project or modification scopes. In doing so, the activities for the impacted SECEs are available in advance and can be fine-tuned depending upon the project or modification.

The extent of Verification should be based on the complexity of the modification and extent of the impact on the SECE and agreed between the duty holder and Verifier.

It is important that the Verifier is engaged early during the planning process in order to execute the workscope at appropriate times. For example, for design Verification to add value it should be completed after the design is finalised and before any hardware is purchased. The risk a duty holder takes by purchasing equipment before it is verified is that the Verifier may identify errors in its suitability such that it is unsuitable for use.

### 5.7 Safety Case material change

SCR 2015, Regulation 10, (4 & 5) introduced a requirement with regards to material changes:

> “(4) Where there is a material change to a design notification, a relocation notification, the safety case or a notification of combined operations the duty holder must refer the material change to the verifier for further comment in accordance with the verification scheme.”

> “(5) If the competent authority requests, the duty holder must communicate the outcome of the referral of the material change to the competent authority.”

The duty holder should involve the Verifier at an appropriate time, with sufficient information on the material change, to allow the Verifier to comment on the impact of any verification arrangements.

Where a material change is also an engineering change which impacts or introduces safety and environmental critical elements (SECEs) then the process within section 5.6 of this guidance Initial Suitability Verification (Projects / Modifications) should be followed.

Duty holders can use reports and workscores generated by the Verifier as part of the engineering change review process to demonstrate to the competent authority that the verification arrangements have been considered and the necessary work is in progress.
5.8 Operational Verification activities

For the operational phase, after the equipment is put into service the Verification scheme must be in place to verify the continued suitability of the SECEs. Nature and frequency in terms of activity, sample size and frequency must be defined for each SECE.

Typically, an operational verification scheme will specify the following types of verification activities:

<table>
<thead>
<tr>
<th>Type</th>
<th>Verification activities (nature)</th>
</tr>
</thead>
</table>
| Offshore | • Witness SECE Assurance activities (e.g. tests / inspections / musters etc.)  
|         | • Visually examine condition of SECEs (e.g. piping, vessels, hazardous area equipment etc.)  
|         | • Audit compliance with SECE Assurance processes (e.g. control of temporary equipment)  
|         |   o Management of inhibits, control of isolation valves  
|         |   o Management of defined life repairs etc through inspection and testing, and the review of any offshore records |
| Onshore | • Review maintenance (planned and breakdown) and inspection records confirming they are:  
|         |   o suitable for assuring the Performance Standard  
|         |   o conducted at the specified frequency  
|         |   o reported correctly stating ‘as-found’ and ‘as-left’ condition  
|         |   o reporting remedial work and ensuring it has been correctly prioritised / executed  
|         | • Review planned maintenance deferrals  
|         | • Audits (typically on a less frequent basis) of specific SECE assurance management systems, e.g. piping and vessels inspection strategy encompassing the RBI implementation, defined life repairs etc. KP3 style audits can be used as a basis for these types of audits |

Many duty holder Performance Standards quote reliability / availability figures. The Verifier should review how the duty holder assures that these figures are being met. In relation to this, the Verifier should ensure that any repeated failures to operate are identified and reported.

The Verification activities that the Verifiers witness offshore should be captured under Assurance routines, which are already in place. There should not be anything extra or additional that needs to be carried out for Verification; if there is, it suggests there are missing Assurance routines, which is a potential deficiency in the management of SECEs.
5.9 Planning

The duty holder must give the Verifier suitable authority to carry out the function defined within the Verification scheme (Ref SCR 2015, Regulation 10, 2 (c)). This includes allowing the Verifier to:

- Talk to any relevant personnel to allow them to undertake a task
- Undertake the full range of their duties, including examination and witnessing of tests
- Obtain the necessary support to complete their work. This support may include access to relevant records through to sufficient access to the offshore installation

Effective planning of Verification activities is key to ensuring the scope is completed in the most efficient manner. The Verifier can be provided with access to plans and given authority to identify and propose appropriate times for offshore visits that link with key activities, e.g. riser ESDV testing.

Good practice is to align the verification visits with the Assurance routines within the maintenance management system as this allows the Verifier to monitor how assurance routines are conducted.

For all Verification scopes, it is beneficial for the duty holder to set Verification milestones, e.g. design Verification to be completed by a certain date or annual operational Verification scope to be fully completed by a certain date. This then provides visibility to all parties and can be used to monitor progress against plan.

All incomplete activities at year end should be assessed by the duty holder and Verifier to determine:

- If the activity sample size should be temporarily increased for the next year,
- If the activity should be carried out by review of documentation,
- A combination of the above, or if there is no added benefit from either.

Completion of the activity in previous years should also be checked and taken into account to ensure any missed activities are not a repetitive occurrence.
5.10 Verification of temporary equipment

The duty holder's Verification scheme must define the Verification activities in terms of nature and frequency for temporary equipment that may introduce additional hazards or interact with SECEs.

- **Nature:** describes what the verifier will do. Essentially, the Verifier checks the duty holder's assurance process for the control of temporary equipment. This can be done through auditing and may involve examination, review and/or witness testing onshore or offshore.

- **Frequency:** describes how much the Verifier will do. Essentially, the Verifier should not be looking at every load-out of temporary equipment or have involvement with the approval process but should take a representative sample to gain confidence in the process from start to finish.

If the Verifier raises any findings the equipment should be removed from service and assessed by the duty holder to determine if it is considered safe to be put back into operation.

For details with regards to the assurance process associated with 'temporary equipment' see chapter 4.5

5.11 Roles and responsibilities

**Verifier Responsibilities**

The verifier has a responsibility to:

- Understand the MAHs and risks associated with the given asset at any point during its lifecycle
- Comment on the record of SECEs
- Draw up, or be consulted in the development of, the Verification scheme and thereafter the periodic review
- Perform Verification activities as defined in the Verification scheme
- Report to the duty holder on the suitability of SECEs detailing examinations / reviews performed, findings and remedial actions recommended
- Communicate any reservations on the list of SECEs or the content of the Verification scheme to the duty holder
- Provide comment on material change to the installation Safety Case

The Verifier is providing an independent view of the initial and ongoing suitability of the SECEs and PFEER-specified plant to manage the risks through the means defined in the safety case, and translated through the Performance Standards. The duty holder retains accountability and responsibility for managing risk through management systems and processes, people employed and their effective function, and the plant provided and its condition.

It should be noted that the defined role of the Verifier under the SCRs applies to activities in support of establishing the physical condition of plant and does not formally encompass the associated and essential activities in support of safety through corporate company management processes and procedures. These systems and roles and their effective performance are as essential to managing safety as the condition of the plant, and are required to be addressed by the duty holder. The Verifier should identify where the duty holder's Assurance processes are inadequate, or not being followed, in order to form a professional judgement whether the SECEs will be suitable and remain in good condition and repair.
Duty holder responsibilities (directly related to Verification)

The duty holder must:

- Define criteria for the appointment of the Verifier
- Periodically review the competence and independence of persons executing Verification activities
- Provide adequate resources to facilitate the management of Verification including the necessary financial provisions. This can be achieved by having clear nature and frequency defined within the Verification scheme to predict resource requirements
- Provide adequate asset specific documentation to facilitate the delivery of Verification including the necessary safety studies, Safety Case, bowties, drawings etc.
- Periodically audit the Verification scheme as part of the overall safety and environmental management system (SEMS)
- Ensure that a periodic review of the Verification scheme is completed by, or in consultation with, a Verifier and, where necessary, revise or replace it. This should consider the evolving phases of the lifecycle, material changes and thorough reviews of the safety case, and the impact of ageing where a more thorough review may take place
- Ensure that a note is made of any reservations made by the Verifier on the record of SECEs or on the scheme. It is a requirement that the Verifier will review and agree the list of SECEs and specified plant. The list should be formally issued by the duty holder and all responses should be logged. Additionally, there should be a record of the Verifier review of the Verification scheme
- Ensure that the Verification scheme is put into effect
- Notify the Verifier of any material change to the Safety Case
- Notify the Verifier of any information in relation to a fundamental change to a SECE, e.g. modifications and major repairs
- Ensure suitable arrangements for communication with the Verifier to get an understanding of the status of activities completed so far, and the status of SECE compliance with Performance Standards
- Ensure a correspondence file is kept by both the duty holder and Verifier
- Manage interfaces between two or more Verifiers. Where more than one Verifier is appointed by the duty holder, arrangements should be in place to manage interfaces in terms of responsibilities, communications and Verification scope, to ensure that the process is effective with no gaps

Additional activities by duty holder to assist Verification process

- Ensure Verifier access to the duty holder’s Assurance management system, safety and environmental management system and to the records of any specialist companies which the duty holder is using to manage their SECEs. It is recommended that the Verifier holds a controlled copy of the Verification scheme
- Verifier training: assurance management system training should be provided to the Verifier by the duty holder to give the Verifiers an understanding of the duty holder's Assurance process and ability to efficiently access records
- Setting of KPI’s - contracts can benefit from KPIs provided they are fair, measurable and do not drive influence or impact on the independence of the Verifier. If managed well, they drive and maintain performance. These could be around continuity of personnel / delivery of reports / timely response to Verification findings, completion of activities within programme etc. Note, this can apply to the Verifier as well as the engineering contractors involved in Verification
5.12 Combined operations

Any operation which involves the temporary interaction of two or more installations with an accepted Safety Case, e.g. a drilling rig operating alongside the platform or a bridge-linked floatel during major works on the platform is a combined operation.

There is a number of interfaces during a combined operation that are likely to result in amendment to the record of SECEs, e.g.

- POB control for size and limitations on temporary refuge, TEMPSC, life rafts, EERV
- Alarms and communication links
- Access and escape routes
- Firewater interconnections
- Fire and gas and ESD links
- Mooring lines / jack-up legs
- Dropped objects for pipelines, crane limitations etc.

The interfaces must be clearly defined before the combined operations begin. Each duty holder and Verifier for each installation must identify and agree the SECEs and Performance Standards affected, as well as the verification activities required and assurance requirements.

Each duty holder must carry out Assurance activities to confirm both initial and continued suitability of the impacted SECEs. Likewise, the Verification scheme should reflect those activities to be carried out by the Verifier.

The installation duty holder’s Verifier will normally carry out interface activities between the installation and the drilling rig / floatel. Any Verification findings raised should be managed as per the Verification scheme. Both duty holders should be notified of the outcome.

Once the drilling rig, floatel or vessel is removed, the Verifier should carry out Verification activities to ensure that the integrity of the installation has been returned to the original state, or complies with the requirements for the revised arrangements following modifications.
5.13 Decommissioning and abandonment

The decommissioning and abandonment phase will commence towards the end of the operations phase.

The activities required for decommissioning and field abandonment by the duty holder must be documented and are subject to approval by the Competent Authority.

A new hazard assessment should be carried out and the list of SECEs reviewed against the hazards associated with the decommissioning plans. Hazards will change during different phases of decommissioning and plans and procedures should be established for timely review/revision to ensure that appropriate SECEs, and Performance Standards, Assurance and Verification are in place for the correct hazards.

The Verification activities will have to be defined for each phase of decommissioning, concentrating particularly on what SECEs are required, what they must be capable of doing, and the order that safety critical equipment is removed/switched off. Note that all SECEs must remain fit for purpose and be Verified for continued suitability until the associated hazard is no longer present, e.g. gas detectors must remain operational until the installation becomes permanently gas free. The Performance Standards may also need revised to cover each decommissioning phase. Any new SECE introduced during the decommissioning phase needs to be fully verified throughout their lifecycle.

5.14 Verification reporting and monitoring

The duty holder must ensure compliance with the Verification scheme which includes completion of all Verification activities contained within it. Failure to complete the stated activities may increase the risk of a Major Accident and is likely to result in enforcement action by the Competent Authority. The duty holder should therefore monitor progress and completion of the Verification activities on a regular basis.

The monitoring of progress should be visible to all parties involved with each level of management regularly provided with an appropriate level of detail. Progress reports, dashboards, meetings, target dates and KPIs can all be used to aid this process. Any concerns or problems with execution of the Verification activities should be identified as early as possible such that recovery plan can be implemented in a timely manner.

Typical progress meetings would include:

AGENDA

- Verification progress versus plan: are 100% of Verification activities completed? If not why not, and which activities are outstanding? What is the recovery plan for the uncompleted activities? Are sufficient resources made available to complete the Verification activities?
- The current and continual suitability of the duty holder’s SECEs including Management of Change: based on Verification activities and the Verifier’s professional judgement
- Look ahead: forthcoming work of the Verification process
- Themes and areas of focus
- Highlights: What is going well?
- Areas for improvement: Verifier should highlight any areas of concern that could be considered as an improvement opportunity
5.15 Verification activity reporting

SCR 2015 Regulation 9 requires “the reporting by a verifier to the duty holder of any instances of non-compliance of the duty holder with the standards of the scheme and the creation of reports by a verifier on the examination and testing carried out; the findings; and any remedial action recommended.”

The reporting requirements for the Verifier should be defined within the Verification Scheme. Reports are issued after the activities have been carried out, and both positive and negative findings of the examination should be recorded to provide traceability that the required activity has been carried out. The Verifier should provide an adequate level of detail to justify the conclusions reached.

These reports should clearly state whether or not the SECE examined meets the Performance Standard requirements. If deficiencies are found, a finding with a recommendation is raised by the Verifier.

Each Verification report should typically include the following information:

- **SECE examined / reviewed**
- **Verification Scheme activity identifier / description**
- **Audit trail description of the equipment / records examined**
- **Details of any outstanding activities; including reasons for activities not being completed**
- **Findings from the examination (Note photographs should be taken for integrity related anomalies)**
- **Remedial actions recommended**
- **Name of the Verifier/author that undertook the examination**
- **Report revision and date of issue**

Verification reports should be issued in a timely manner, typically 5-10 working days following completion of the activities or visit to site. It is also good practice for the verifier to have a close out meeting with the appropriate parties and issue a draft report at site.
5.16 Findings and any remedial action recommended

The process for management and investigation of Verification findings should be defined by the duty holder. This process should cover:

- Categorisation of remedial actions recommended
- Escalation process
- Close-out process

To ensure the agreed remedial actions are expedited to closure, it is recommended the below items are considered to facilitate the process:

- Actions from findings should be given realistic target closure dates (in accordance with severity and remedial actions) which are agreed between the Verifier and duty holder
- Risks associated with the MAHs and specific installation must be considered when assessing the severity and remedial actions of the finding
- Duty holders should aim to identify and remedy the root cause in order to avoid recurrence and to promote internal learning
- Findings which remain open after the target date are classed as overdue and should be escalated to senior management within the duty holder’s organisation
- Remedial actions should be regularly reviewed to ensure they are being progressed
- Database systems which can be accessed by both the Verifier and duty holder are seen as best practice as they provide good visibility and facilitate effective information management
- Recommended remedial actions should be closed by the Verifier when provided with suitable evidence (e.g. work order, photo, updated document / procedure etc.) of remedial action by the duty holder

Verification findings within the industry are categorised in many ways as per the requirements detailed within each duty holder’s Verification scheme. However, as an industry, verification findings are reported to Oil & Gas UK for input into an industry KPI to track the level of open and overdue findings for the industry. The current definitions used by Oil & Gas UK are as follows:

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1</td>
<td>Performance Standard satisfied, but Verifier may suggest an improvement to the system or may request additional information to demonstrate compliance with a Performance Standard</td>
</tr>
<tr>
<td>Level 2</td>
<td>Single Performance Standard failure with no significant threat to the installation</td>
</tr>
<tr>
<td>Level 3</td>
<td>Fundamental weakness of the SECE Assurance system that: -involves multiple failures of a Performance Standard (s); or -presents a significant threat to the integrity of the installation</td>
</tr>
</tbody>
</table>

Note: If duty holders wish to monitor their findings against industry average it would be beneficial to use the definitions set by Oil & Gas UK.

In addition to the above, the Verifier may also issue a formal letter to the duty holder if there is fundamental concern that should be highlighted to senior management. Examples of formal letters are:

**Letter of Reservation** – A letter of reservation will be issued by the Verifier when there is a Regulatory compliance concern with regards to the ‘Verification scheme’ that is required to be brought to the attention of the duty holder’s senior management. Examples include poor identification of SECEs, inadequate Performance Standards, Assurance processes or Verification activities (nature and frequency).

**Letters of Concern** – A letter of concern will be issued by the Verifier when there is a fundamental concern with regards to the ‘management of Verification’ that is required to be brought to the attention of the duty holder’s senior management. Examples include mismanagement for findings, the cumulative effect of open or overdue findings, failing to assist or provide access to allow the Verifier to complete the scheme activity requirements.

Note that certain findings may be reportable by the duty holder to the Competent Authority under Implementing Regulation No 1112/2014. Refer to ROGI.
Chapter 6. Verification Interface with Other Independent Competent Persons (ICPs)

Verification activities are carried out by an Independent Competent Person (ICP), also known as the ‘Verifier’. The Competent Authority does not expect work carried out between ICPs to be replicated or duplicated. However, the duty holder remains accountable for ensuring the SECEs have been examined by an ICP for both initial and ongoing suitability.

Where a duty holder appoints more than one Verifier for a given asset, the duties and scope of each Verifier must be clearly established and documented.

Verifiers are often provided with results of work done by another ICP as evidence of a SECE's suitability. To credit the Verification activities (without duplication of effort) the Verifier should confirm that the examination undertaken corresponds to that defined in the Verification scheme.

For example, certification issued under the Pressure Equipment Directive (PED), is often presented as evidence that equipment is fit for purpose. In this case the Verifier may check:

- The certification is for the specific equipment
- Design conditions match or exceed the requirements of the Performance Standards

Well Examiner

SECEs for well containment include downhole safety valves, Xmas trees and the well containment envelope. The SCR and DCR regulations require wells to be examined by a Well Examiner, an ICP. A Well Examination scheme must be in place to define the activities that will be carried out by the Well Examiner. This creates a potential overlap with the Verification as both schemes are checking the same SECEs. The duty holder should therefore ensure that all Assurance aspects for the SECEs are covered between the two schemes. One means of achieving this is to provide a diagram showing the interfaces between the two schemes then including this diagram (and associated text) in both schemes and in the safety case. It may be beneficial to have periodic meetings between the Verifier and Well Examiner to address any interface issues.

LOLER

Lifting Operations and Lifting Equipment Regulations 1998 (LOLER) require all lifting equipment to be examined for both initial and continued suitability by a competent person. Lifting equipment can be an SECE, therefore the activities in the Verification scheme must take account of this and ensure there are no gaps or overlaps. One means of achieving this is to provide a table showing the interfaces between Verification and LOLER.

Class Surveyor

Classification societies establish and maintain technical standards for the construction and operation of floating structures. The overlap between Classification & Verification applies to FPSOs, FSUs and MOUs which are classed. The class society validates construction in accordance with their standards and carries out regular in-service surveys to ensure ongoing compliance with those standards. These surveys are carried out by a ‘Class Surveyor’ who is also an ICP.

To avoid duplication of work and assuming the class surveyor has the necessary competency and independence [as defined in Regulation 2(7)] duty holders can appoint the class surveyor as Verifier to carry out the activities within the Verification Scheme. Where a class surveyor has been appointed as a Verifier, the scheme should provide a description of how independence will be maintained. The class surveyor cannot be the Verifier of their ‘own’ work if they have in some way been part of that Assurance process, either through direct examination or through certifying duty holder assurance activities. Class surveys are generally reported by exception therefore, when conducting Verification activities, reporting should be in accordance with Chapter 5.14.
Abbreviations, acronyms and meanings

POB: Personnel on board

DCR: The Offshore Installations and Wells (Design and Construction, etc) Regulations 1996

ESD: Emergency shutdown

FPSO: Floating production storage and offloading

FSU: Floating storage unit

ICP: Independent and Competent Person

KP3: Key Programme 3 – Asset Integrity Programme (a report by the Offshore Division of HSE’s Hazardous Installations Directorate)

KPI: Key performance indicator


MAH: Major Accident Hazard

MOU: Mobile offshore unit

ORA: Operational risk assessment

PED: Pressure Equipment Directive

PFEER: The Offshore Installations (Prevention of Fire and Explosion, Emergency Response) Regulations 2015

QA: Quality assurance

RBI: Risk-based inspection

SCR: The Offshore Installations (Offshore Safety Directive) (Safety Case etc.) Regulations 2015

SECE: Safety and Environmental Critical Element

SMART: Specific, measurable, achievable, responsible, timely

TEMPSC: Totally enclosed motor propelled survival craft

UKCS: United Kingdom Continental Shelf
Definitions

**ATEX:** EU directives describing what equipment and work environment is allowed in an environment with an explosive atmosphere

**Major Accidents:**
(a) an event involving a fire, explosion, loss of well control or the release of a dangerous substance causing, or with a significant potential to cause, death or serious personal injury to persons on the installation or engaged in an activity on or in connection with it;
(b) an event involving major damage to the structure of the installation or plant affixed to it or any loss in the stability of the installation causing, or with a significant potential to cause, death or serious personal injury to persons on the installation or engaged in an activity on or in connection with it;
(c) the failure of life support systems for diving operations in connection with the installation, the detachment of a diving bell used for such operations or the trapping of a diver in a diving bell or other subsea chamber used for such operations;
(d) any other event arising from a work activity involving death or serious personal injury to five or more persons on the installation or engaged in an activity on or in connection with it; or
(e) any major environmental incident resulting from any event referred to in paragraph (a), (b) or (d), and for the purposes of determining whether an event constitutes a major accident under paragraph (a), (b) or (e), an installation that is normally unattended is to be treated as if it were

**Material change:** likely to be one that changes the basis on which the original safety case was accepted. This would involve changes to the basis on which risk control decisions are made or which necessitate a review of the adequacy of major hazard control measures. It includes both physical modifications and operational management changes of sufficient significance.

**Assurance:** the checking of Safety and Environmental Critical Elements (SECEs) by workers who are assigned to maintain or test them.

**Competent Authority:** In UK, the Competent Authority is a partnership of the Health & Safety Executive (HSE) and the Offshore Petroleum Regulator for Environment & Decommissioning (OPRED – formerly DECC) that is responsible for overseeing industry compliance with the EU Directive on the safety of offshore oil and gas operations

**Independent and Competent Person:** A person appointed by the duty holder to verify that safety critical elements on an installation are, and remain, suitable.

**Performance Standards:** Performance Standard (PS) describe the essential requirements that must be maintained or provided on demand throughout an installation’s life. The PS is defined in terms of its functionality, availability, reliability, survivability and interdependency.

**Safety and Environmental Critical Elements:** parts of an installation and its plant which could cause or contribute substantially to a major accident, or which purpose is to prevent, or limit the effect of a major accident.

**Verification:** ensures Safety and Environmental Critical Elements (SECEs) are, and will remain, compliant with Performance Standards through each phase of the installation’s lifecycle. The scheme provides additional confidence, independent of the duty holder’s assurance process, that the parts of the installation deemed to be safety critical, are suitable, or actions necessary to support their suitability are identified.
Elements of a Performance Standard

**Goal:** What’s the purpose of the SECE from a safety and environmental critical perspective?

This should be linked to the relevant MAH(s) i.e. achievement of the performance standard directly contributes to preventing, detecting, controlling, mitigating or responding to a Major Accident Hazard. The Goal should set a clear objective with which to define and assess the required function and performance of the equipment.

The following example is given to demonstrate a goal objective:

e.g. collision avoidance: The collision avoidance system is to provide a means to ensure that other vessels and aircraft are aware of the installation. To provide a system which will monitor marine traffic around the field and provide reliable, secure and effective warning if a vessel maintains a course, which could lead to impact with the installation.

**Boundary:** Which items of equipment does the Performance Standard apply to? This should be a clear description of the exact extent and limits of the SECE. Where appropriate, a list of the items may be more useful.

The following example is given to demonstrate a boundary scope:

e.g. Uninterrupted power supply (UPS) systems: Examples of UPS systems include:
  - Shutdown system
  - Fire and gas system
  - Emergency related telecoms
  - PA/GA system
**Functionality:** What the SECE must do from a safety and environmental critical perspective?

Functionality defines the key duties that the SECE is required to perform. The minimum level at which that function is achieved must also be defined. Criteria is considered ‘measurable’ where it is possible for a person carrying out an assurance activity to clearly understand what the critical requirement is, and to be able to measure or observe that the criteria is being achieved.

During the operational phase of the installation, the Performance Standard has to reflect how it shall be assured that the SECE is maintained in the minimum acceptable condition. This may not be the same as the design criteria - an acceptable level of safe degradation should be defined.

For ‘static’ or ‘passive’ systems (structures, containment, lifting equipment etc) measurable criteria for operational suitability may be expressed in terms of the maximum allowable degradation that can be tolerated. This may derive from international standards, Duty Holder’s anomaly classification criteria, industry guidelines or other ‘best practice’.

For ‘active’ systems it is likely that performance can be clearly quantified and confirmed by function test (active fire system discharge rates, instrument alarm and trip set points, ESD valve closure time and leakage rates etc).

Detailed functional analysis may be required to determine the failure modes (including computer systems) which lead to loss of critical functionality and the means of identifying them. Equipment that is ‘self-testing’ may make functional failure evident.

For SECEs such as personal survival or escape equipment where continual suitability is primarily achieved by original design specification, it may be more practical to define periodic service or re-certification intervals. Defining a ‘fixed life’ for equipment replacement may also be appropriate.

The following example is given only to demonstrate a single functional criteria:

<table>
<thead>
<tr>
<th>SECE - UPS</th>
<th>CRITERIA</th>
<th>ASSURANCE REFERENCE</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FUNCTION</strong></td>
<td><strong>PERFORMANCE</strong></td>
<td><strong>CRITERIA</strong></td>
</tr>
<tr>
<td>UPS shall maintain power to the defined emergency systems.</td>
<td>UPS systems shall provide a back-up power supply to enable continued operation of the following emergency systems in the event of failure of normal and essential power.</td>
<td>Duty holder should provide details of assurance activities or specific cross references to CMMS database tasks.</td>
</tr>
<tr>
<td>The following systems shall be capable of operating at full load for a minimum duration of XX minutes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shutdown Systems (XX Ampere hours)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fire and Gas (XX Ampere hours)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Emergency related Telecoms (XX Ampere hours)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PA/GA Systems (XX Ampere hours)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Availability: Will it be ready and able to perform when required? (Alternatively, the ability for the system to provide access to its resources in a timely manner for a specified duration.)

Availability is the ability of the SECE to meet its intended function, including its interaction with other SECEs, e.g. an electrically driven fire pump can only be deemed available if the power can be provided to the pump from the emergency switchboard and the pump can deliver the required flow rate to the distribution system. If any part of the system is defective, it will cause the pump to have reduced Availability. There is often a close correlation between reliability and availability.

Availability may be better understood and measurable where it is described in terms of the amount of time it is tolerable for the critical functions to be unavailable, or to describe mitigation measures that need to be implemented where Availability is less than 100%. Availability should be considered during design of an SECE, i.e. the designer should specify how the system will manage failure modes and therefore how it will remain available, e.g. by providing diverse systems and redundancy.

Quantitative risk assessments are often carried out to assist in defining the design requirement. The result of such a study will produce a target, e.g. 97.8% availability which equates to an acceptable annual downtime of approximately 8 days. In theory, this may be a good basis for design, but how shall this remain meaningful during operations? Is it safe to state that it would be acceptable to continue operation with an essential safety system out of operation during those days? In practice, it is rarely possible to carry out a meaningful volume of testing to capture sufficient data to demonstrate that such targets are met.

In general terms, the SECE availability target should be 100%. In practice, the SECE may never achieve 100% but if (or rather when) an SECE fails in some manner (note the Performance Standard should define through measurable criteria when such a failure occurs), the immediate shortcoming has to be addressed through risk assessments and through the Safety Management System. The Duty holder should then aim for improvement, i.e. how to prevent similar failures in the future. Where appropriate measures have been set, it is necessary to ensure that the means to capture required information are defined in order to assess availability. This may be through clear recording of failed components, downtime records and safety critical risk assessments.

The example given below describes the overall goal and the design criteria which have been used to meet this. It is a requirement to assure / verify that this specification remains available, e.g. both sides of the public address (PA) system are being examined for continued effectiveness and availability of the complete system remains at 100% (i.e. failures of individual components may be considered acceptable dependant on the impact on the ability of the system to operate on demand).

The following example is given to demonstrate possible availability criteria:

<table>
<thead>
<tr>
<th>SECE – COMMUNICATION SYSTEMS</th>
<th>AVAILABILITY</th>
<th>ASSURANCE REFERENCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Function</td>
<td>Criteria</td>
<td>Assurance Reference</td>
</tr>
<tr>
<td>The PA/GA System shall maintain 100% Availability.</td>
<td>The PA system has been designed with built in redundancy. The PA/GA shall be a dual (sub-systems A &amp; B) system, with each sub-system being capable of independently providing audible alarms, visual alarms and speech in all areas, such that no single failure can impair both subsystems. Each sub-system shall be fed from independent Uninterruptible Power Supplies. Any failure which affects the ability of BOTH systems to operate shall be subject to immediate safety critical risk assessment and appropriate mitigating measures implemented.</td>
<td>Duty holder should provide details of assurance activities or specific cross references to CMMS database tasks.</td>
</tr>
</tbody>
</table>
Reliability: How likely is it to perform on demand? (Alternatively, the ability of an item to perform a required function under given conditions for a specified time interval.)

Those SECEs for which it is required to measure reliability during operations should be identified at the design stage. Reliability targets are set during the design phase based upon safety studies carried out in support of the Safety Case.

A target for Reliability is practical for ‘active’ systems that need to perform critical functions in response to a Major Accident (e.g. Fire & Gas detection, fire pump starting, ESD valve actuation etc). Reliability targets are also appropriate for systems which actively monitor the status of other systems (e.g. alarms for loss of area pressurisation, mooring tension, bilge flooding etc). Reliability targets are not appropriate for passive systems such as structure or passive fire protection.

Any critical function that has a demand to operate in response to a Major Accident must have a low probability of failure to meet that demand. High reliability is achieved through the initial design specification of equipment (i.e. robust, simple design, self-diagnosis, redundancy etc). Performance Standard criteria for reliability can be expressed in terms of probability of failure on demand (PFD), safety integrity level (SIL) or mean time between failure (MTBF).

The ability to meet the Performance Standard is demonstrated by functional testing at an appropriate interval. From these tests, accurate data must be recorded and reviewed in detail to assess if the required reliability is being achieved. If the required level of reliability is not being achieved, appropriate action must then be taken to improve it. This may include system redesign, amendment of test intervals or revision of the maintenance strategy. Targets for reliability in operation may not be possible for some SECEs as there may be no possibility to collect sufficient data to assure the target is met. In cases such as deluge valves or fire pumps there should be a general expectation that they shall operate on demand every time. It is vital that Technicians understand this concept and record when failures are observed during routine maintenance and testing, i.e. the reliability of an SECE is compromised when they have to carry out corrective maintenance in order for the intended function to complete its action.

The following example is given to demonstrate possible reliability criteria:

### SECE – ESD System

<table>
<thead>
<tr>
<th>FUNCTION</th>
<th>CRITERIA</th>
<th>ASSURANCE REFERENCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESD Valves for hydrocarbon risers shall have a probability of failure on demand less than xx%.</td>
<td>ESD Valves are designed to [STANDARD]. Testing carried out according to functional requirements, any failure to close during testing are reviewed at the time of test according to SCRA procedures, appropriate mitigation measures shall be agreed with TA within xx time. Reference to QRA study for target reliability requirement.</td>
<td>Duty holder should provide details of assurance activities or specific cross references to CMMS database tasks.</td>
</tr>
<tr>
<td>All components within a shutdown loop e.g. detector device, logic solver through to final actuated element shall meet defined reliability</td>
<td>The shutdown system design, engineering and maintenance activities shall be carried out and performed to meet the requirements defined within IEC 61508 and IEC 61511.</td>
<td>Duty holder should provide details of assurance activities or specific cross references to CMMS database tasks.</td>
</tr>
</tbody>
</table>
Survivability: How will the system perform post event, e.g. after a fire, explosion, ship impact, dropped objects, extreme weather etc?

The Performance Standard criteria for survivability must be defined if the SECE is required to operate in the event of a Major Accident and should state for how long the system should continue to be effective. Each SECE should be considered against the MAH defined in the Safety Case. Does the Major Accident event have the possibility to impair the ability of the SECE to operate? If so, how shall this be mitigated against?

Survivability is often determined at the design stage and initial suitability assessment of the equipment (physical location, fire rating, mechanical strength, fatigue life etc).

The following examples are given to demonstrate possible Survivability criteria:

<table>
<thead>
<tr>
<th>EVENT</th>
<th>COMPONENT</th>
<th>CRITERIA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extreme Weather</td>
<td>All Refernce to structural design report based on Met-ocean data for specific location.</td>
<td>Jacket structures shall withstand the specified (XX-year return) extreme environmental conditions specified in the site specific Metocean report without collapse.</td>
</tr>
<tr>
<td>Fire and Explosion</td>
<td>Primary structure within X metres of the YY deck. Reference to Fire Risk Assessment.</td>
<td>Passive Fire Protection is applied to structural members in the defined area.</td>
</tr>
</tbody>
</table>
**Interactions**: What systems the SECE interacts with?

Systems of SECEs are often dependent upon each other in order that the MAH is mitigated. It is useful to define the SECEs which are required to function in order for the one in question to also operate effectively.

The following examples are given to demonstrate potential Interactions: e.g. HVAC System:

### SECE – HVAC SYSTEMS

<table>
<thead>
<tr>
<th>Interactions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fire and Gas System</td>
<td>Fire and Gas Detection System will initiate closure of damper and shutdown HVAC systems</td>
</tr>
<tr>
<td>Passive Fire Protection</td>
<td>All fire dampers shall maintain the integrity of the boundary in which they are installed for the defined endurance period of that boundary</td>
</tr>
</tbody>
</table>

### SECE – TEMPORARY REFUGE

<table>
<thead>
<tr>
<th>SECE</th>
<th>Reason for Interaction / Dependency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Structures</td>
<td>To provide mechanical integrity of the Temporary Refuge. To retain sufficient integrity to preserve positive pressure following loss of HVAC.</td>
</tr>
<tr>
<td>Communications and Alarms</td>
<td>To inform personnel of the need to muster and / or evacuate. To provide communication facilities with aircraft, shipping (including the Emergency Response &amp; Rescue Vessel) and external rescue agencies.</td>
</tr>
<tr>
<td>Escape and Evacuation Routes</td>
<td>To enable access to and egress from the Temporary Refuge from all areas. To provide sufficient illumination for personnel to muster in safety, don their survival equipment and evacuate / escape. To provide sufficient illumination for persons in command of the emergency to be able to perform their duties.</td>
</tr>
</tbody>
</table>
Appendix 2

Example of an operational performance standard template populated with typical content

Note that for a new build or engineering change modification the assurance and verification activities will be focused on the activities around design, procurement, construction and commissioning, although performance criteria remain pertinent for the life cycle of the installation.

The contents of the table are not exhaustive and the actual content should reflect the installation’s Major Accident Hazard assessments.
Example of an operational performance standard template populated with typical content

Note that for a new build or engineering change modification the assurance and verification activities will be focused on the activities around design, procurement, construction and commissioning, although performance criteria remain pertinent for the life cycle of the installation. The contents of the table are not exhaustive and the actual content should reflect the installation’s Major Accident Hazard assessments.

<table>
<thead>
<tr>
<th>Goals</th>
<th>To provide a temporary place of safety for all personnel to muster following an incident for XX time To provide essential command and control facilities to enable effective emergency response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boundaries</td>
<td>All accommodation areas within the living quarters including the emergency control centre, primary muster areas and sick bay</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Functionality</th>
<th>Assurance</th>
<th>Verification</th>
</tr>
</thead>
<tbody>
<tr>
<td>F1</td>
<td>The maximum acceptable leakage rate for the Temporary Refuge shall not exceed XX Air change per hour at a differential pressure of +/-XX Pa</td>
<td>XX Temporary Refuge leak test</td>
</tr>
<tr>
<td>F2</td>
<td>Primary Muster areas sized to accommodate 100% POB XXm² per person shall be allocated within the Temporary Refuge Muster Areas to be kept clear of obstructions</td>
<td>XX Temporary Refuge boundary inspection</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sensitivity</th>
<th>Assurance</th>
<th>Verification</th>
</tr>
</thead>
<tbody>
<tr>
<td>F3</td>
<td>The emergency control centre shall…</td>
<td>… … … …</td>
</tr>
<tr>
<td>F4</td>
<td>Emergency equipment located at each Muster Point shall include…</td>
<td>… … … …</td>
</tr>
<tr>
<td>F5</td>
<td>Alternative muster areas shall have…</td>
<td>… … … …</td>
</tr>
<tr>
<td>F6</td>
<td>Doors shall be self-closing, opening in the direction of escape…</td>
<td>… … … …</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Availability</th>
<th>Assurance</th>
<th>Verification</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1</td>
<td>Maximum impairment frequency…</td>
<td>… … … …</td>
</tr>
<tr>
<td>A2</td>
<td>TR to be available for use at all times during normal operational activities</td>
<td>… … … …</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Reliability</th>
<th>Assurance</th>
<th>Verification</th>
</tr>
</thead>
<tbody>
<tr>
<td>R1</td>
<td>TR boundary fire dampers…</td>
<td>… … … …</td>
</tr>
<tr>
<td>R2</td>
<td>Doors…</td>
<td>… … … …</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Survivability</th>
<th>Assurance</th>
<th>Verification</th>
</tr>
</thead>
<tbody>
<tr>
<td>S1</td>
<td>External boundary element… shall be fire rated XX and designed for XX mbar overpressure</td>
<td>… … … …</td>
</tr>
<tr>
<td>S2</td>
<td>Internal floors and walls shall be rated…</td>
<td>… … … …</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SECE</th>
<th>Interactions and Dependencies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blast and passive fire protection</td>
<td>Protects the Temporary Refuge from the effects of fire and explosion</td>
</tr>
<tr>
<td>Primary structures</td>
<td>Provides structural support for the Temporary Refuge…</td>
</tr>
<tr>
<td>Egress and access routes</td>
<td>Provides access to and from the Temporary Refuge</td>
</tr>
<tr>
<td>Fire &amp; gas system</td>
<td>Detection of fire, gas, smoke</td>
</tr>
<tr>
<td>HVAC</td>
<td>To provide a positive pressure within the Temporary Refuge prevent ingress of smoke / gas</td>
</tr>
<tr>
<td>Emergency lighting</td>
<td>…</td>
</tr>
<tr>
<td>ESD</td>
<td>…</td>
</tr>
<tr>
<td>Firewater</td>
<td>…</td>
</tr>
<tr>
<td>Ignition prevention</td>
<td>…</td>
</tr>
<tr>
<td>Communications</td>
<td>…</td>
</tr>
<tr>
<td>Personnel protective equipment</td>
<td>…</td>
</tr>
</tbody>
</table>

References - List of standard, studies, guidance and assessments which were used in developing the performance standard criteria above. When a SECE degrades to the point of no longer meeting its performance standard, the information on how those minimum requirements for safety was defined becomes critical when assessing risk and defining mitigation.
### Appendix 3  PREVENTION SECE Barrier table

<table>
<thead>
<tr>
<th>SECE Example</th>
<th>Functions</th>
<th>Availability</th>
<th>Reliability</th>
<th>Survivability</th>
<th>Interdependence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process Containment</td>
<td>- Mechanical strength/integrity - Limits for corrosion, erosion, fatigue, coating breakdown, mechanical damage, water ingress to insulation, security of supports etc.</td>
<td>By design - operational target not appropriate. To be 100% available in operation to avoid loss of containment</td>
<td>By design - operational target not appropriate as failure cannot be tolerated.</td>
<td>- Dropped object resistance/protection - Blast resistance - Pool and jet fire resistance - Environmental criteria</td>
<td>- Topside Structures to provide support and impact protection - Deluge or Passive Fire Protection to meet Survivability criteria</td>
</tr>
<tr>
<td>Well Integrity</td>
<td>- Mechanical strength/integrity of wellheads and Christmas trees - Internal and external leakage - Closure time for actuated shutdown valves - Calibration of annulus gauges - Condition of wellhead control panel/HPU - Condition, rating and operation of fusible loop</td>
<td>By design - operational target not appropriate. To be 100% available in operation to avoid loss of containment</td>
<td>Identify Safety Integrity Levels (SIL) for operation of actuated tree valves</td>
<td>- Dropped object resistance/protection - Blast resistance - Pool and jet fire resistance - Environmental criteria</td>
<td>- ESD System to monitor well status and initiate trip of tree valves - Well Examination Scheme - Fire &amp; Gas to interface with fusible loop - Deluge systems to meet Survivability criteria</td>
</tr>
<tr>
<td>Hull Integrity</td>
<td>- Girder strength - Limits for corrosion, erosion, fatigue, coating breakdown etc. - Condition of deck hatches and water/weather tight doors - Operation of remote door position indication - Hull penetration valves - integrity, operation and position indication (remote and local) - Cathodic protection systems</td>
<td>By design - operational target not appropriate. To be 100% available to avoid loss of integrity</td>
<td>Identify Safety Integrity Levels (SIL) for operation of actuated hull penetration valves</td>
<td>- Design strength to withstand ship collision - Dropped object resistance/protection - Blast resistance - Pool and jet fire resistance - Environmental criteria</td>
<td>- Ballast system to maintain hull stability - Inert Gas system to prevent cargo tank over/under pressure - Navigational Aids to avoid ship/aircraft collision - Safeguarding Instrumentation to prevent collision during Shuttle Tanker approach and offloading operations - Emergency power system to supply position monitoring system</td>
</tr>
<tr>
<td>Jacket and Topside Structures</td>
<td>- Mechanical strength/integrity - Limits for corrosion, erosion, fatigue, coating breakdown etc. - Structural elevation - Air gap required between wave crests and the underside of topside structures - Limits for scour and debris at foundations - Limits for weight and marine growth</td>
<td>By design - operational target not appropriate. To be 100% available to avoid loss of integrity</td>
<td>By design - operational target not appropriate as failure cannot be tolerated.</td>
<td>- Design strength to withstand ship collision - Dropped object resistance/protection - Blast resistance - Pool and jet fire resistance - Environmental criteria</td>
<td>- Navigational Aids to avoid ship/aircraft collision - Deluge or Passive Fire Protection to support Survivability criteria</td>
</tr>
<tr>
<td>Lifting Equipment</td>
<td>- Mechanical strength/integrity - Overload protection - Ropes - security of terminations and discard criteria</td>
<td>Cranes to be 100% available during lifting operations Action on loss of power Weather limits for crane operations</td>
<td>By design - operational target not appropriate as failure cannot be tolerated.</td>
<td>- Environmental criteria</td>
<td>- Navigational Aids to avoid ship/aircraft collision</td>
</tr>
<tr>
<td>Helideck</td>
<td>- Load limits - Dimensions (‘D’ value) - Layout and markings - Identification of permanent obstructions - Means to prevent temporary obstructions - Weather limits for helicopter operations (adverse weather policy)</td>
<td>By design - operational target not appropriate. To be 100% available in operation to avoid loss of integrity</td>
<td>By design - operational target not appropriate as failure cannot be tolerated.</td>
<td>- Helideck protected from blast overpressure by location (by design) - Helideck to resist design scenario helicopter crash landings - The helideck is not expected to remain usable in scenarios involving the generation of large amounts of smoke or high levels of thermal radiation - Environmental criteria - Wave-off/warning beacons to prevent landing during emergency (event escalation)</td>
<td>- Topside Structures to provide support - Drains systems to handle fuel leaks/spillage - Active fire protection systems in the event of helicopter collision - Crash box and personal protective equipment provided to helideck crew - Escape routes for access and egress - Navigational Aids to avoid aircraft collision</td>
</tr>
<tr>
<td>Mooring System</td>
<td>- Mechanical strength/integrity - Limits for material loss, corrosion, erosion, fatigue, coating breakdown, mechanical damage etc. - Marine growth limits - Design limits for tension - Indication of tension (input to heading control system) - Excursion limits and alarms</td>
<td>By design - operational target not appropriate. To be 100% available to avoid loss of integrity</td>
<td>Safety Integrity Levels (SIL) to be defined for position and mooring monitoring systems (Test intervals to ensure SIL level is achieved).</td>
<td>- Environmental criteria</td>
<td>- Environmental criteria</td>
</tr>
</tbody>
</table>

**STEP CHANGE IN SAFETY - ASSURANCE AND VERIFICATION PRACTITIONERS’ GUIDANCE DOCUMENT**
<table>
<thead>
<tr>
<th>SECE Example</th>
<th>Functions</th>
<th>Availability</th>
<th>Reliability</th>
<th>Survivability</th>
<th>Interdependence</th>
</tr>
</thead>
</table>
| Fire & Gas Detection |  - Detection methods and types (including MAC)  
  - Functionality (reference Cause & Effects)  
  - Set-Points for alarm & trip activation  
  - Time limits for instrument response  
  - Failure modes  
  - Logic Solver voting  
  - Status Indication (what & where)  
  - Electromagnetic compatibility |  - Overall F&G system availability of XX.X%  
  - Location and spacing (detectors, MACs)  
  - Provision of status indication within Temporary Refuge  
  - Fault monitoring - provision of alarms on field detector failure |  - Safety Integrity Levels (SIL) to be identified (test intervals to ensure SIL levels are achieved) |  - Fire rating for field cables  
  - Ingress Protection (IP) rating for field devices  
  - Fire detector response time should activate and initiate executive actions before direct exposure destroys detector or cabling.  
  - Operation of loss of main power supplies |  - UPS systems supplies Fire & Gas system on loss of main power  
  - Ex Certification ensures electrical equipment suitable for operation in hazardous areas |
| ESD System (Inputs) |  - Process sensor types (manual and automatic)  
  - Functionality - Set-Points for alarm & trip activation (reference Cause & Effects)  
  - Time limits for instrument response  
  - Instrument response time  
  - Failure modes  
  - Operation of ESD timers  
  - Operation of Blowdown system sequencing logic  
  - Logic Solver voting  
  - Status Indication (what & where)  
  - Electromagnetic compatibility |  - Overall ESD system availability of XX.X%  
  - Provision of status indication within Temporary Refuge  
  - Fault monitoring - provision of alarms on field detector failure |  - Safety Integrity Levels (SIL) to be identified (test intervals to ensure SIL levels are achieved) |  - Fire rating for field cables  
  - Ingress Protection (IP) rating for field devices  
  - Operation of loss of main power supplies |  - UPS systems supplies Fire & Gas system on loss of main power  
  - Ex Certification ensures electrical equipment suitable for operation in hazardous areas |
| Safeguarding Instrumentation |  - Rotating equipment Over-temperature / vibration protection  
  - Lubrication/seal oil status monitoring systems  
  - Heading control systems |  - Fault monitoring - provision of alarms on field detector failure |  - Safety Integrity Levels (SIL) to be identified (test intervals to ensure SIL levels are achieved) |  - Fire rating for field cables  
  - Ingress Protection (IP) rating for field devices  
  - Operation of loss of main power supplies |  - UPS systems supplies on loss of main power  
  - Ex Certification ensures electrical equipment suitable for operation in hazardous areas |
<table>
<thead>
<tr>
<th>SECE Example</th>
<th>Functions</th>
<th>Availability</th>
<th>Reliability</th>
<th>Survivability</th>
<th>Interdependence</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESD System (Logic Solver and Outputs)</td>
<td>- Functionality (reference to Cause &amp; Effects) - Location and diversity of control points - ESD valve closure time and seat leakage rates - Failure modes for valve and associated controls</td>
<td>- High availability target required for overall ESD system availability (XX.X%) - Provision of control functions and status indication within Temporary Refuge</td>
<td>- Safety Integrity Levels (SIL) to be identified (test intervals to ensure SIL levels are achieved)</td>
<td>- Ingress Protection (IP) rating for field instrumentation - Fire Safe ESD valves and actuators - Operation on loss of main power supplies (duration)</td>
<td>- Fire &amp; Gas Detection initiates ESD on confirmed detection - UPS provides back-up power supply following loss of main power - ESD System initiates Blowdown - Certified electrical equipment ensures field equipment is suitable for use in a hazardous area</td>
</tr>
<tr>
<td>Pressure Relief, Flare and Blowdown Systems</td>
<td>- System overpressure limits - Certification of relief valves - Flare system purge (to prevent air ingress) - Blowdown rate (pressure vs. time) - Failure modes for valve and associated controls - Position/Interlock of relief and blowdown system isolation valves</td>
<td>- High availability target required for overall blowdown system availability (XX.X%) - Provision of control functions and status indication within Temporary Refuge</td>
<td>- Safety Integrity Levels (SIL) to be identified (test intervals to ensure SIL levels are achieved)</td>
<td>- Fire Safe rating of Relief valves, Blowdown valves and actuators - Dropped object resistance/protection Blast resistance</td>
<td>- Drains remove flammable liquids from below vessels and rotating equipment in the event of a leak. This is mitigation against pool fires. - Liquids from the blowdown/flare system are pumped to the drains system - Passive Fire Protection to flare system pipework, vessels and supports</td>
</tr>
<tr>
<td>High Integrity Pressure Protection Systems</td>
<td>- System overpressure limits - Logic Solver voting - HIPPS valve closure times</td>
<td>- High availability target required for overall HIPPS system availability (XX.X%)</td>
<td>- Safety Integrity Levels (SIL) to be identified (test intervals to ensure SIL levels are achieved)</td>
<td>- Fire rating for field cables - Ingress Protection (IP) rating for field devices - Fire rating of HIPPS valves - Operation on loss of main power supplies (duration)</td>
<td>- HIPPS system interacts with ESD to initiate further levels of plant trips - Certified electrical equipment ensures field equipment is suitable for use in a hazardous area</td>
</tr>
<tr>
<td>Drilling Well Control (BOP, Mud and Cement)</td>
<td>- BOP closure time - Condition - External leakage; Visible damage - Capacity of BOP accumulator System (number of operations) - Capacity of mud / cement systems - Location and diversity of control points</td>
<td>- BOP system to be available at all times when drilling</td>
<td>- Testing regime in accordance with API RP 53 (Recommended Practice for Blowout Prevention Equipment Systems for Drilling Wells)</td>
<td>- Dropped object protection/resistance - Pool and jet fire resistance - BOP control hoses to be certified fire resistant - Operation of loss of main power supplies (duration)</td>
<td>- UPS power provided to control consoles in the event of loss of main power - HVAC required for the mud/cement systems to operate (safe area pressurisation) - Certified electrical equipment ensures field equipment is suitable for use in a hazardous area - Well Examination Scheme to confirm design of pressure envelope</td>
</tr>
<tr>
<td>Ventilation and HVAC</td>
<td>- HVAC air change rates (open areas, turbine compartments) - Location of inlet/outlets (relative to haz. areas) - HVAC Fan and damper status indication (what &amp; where) - Operation of instrumentation to monitor area pressurisation / flow rates - HVAC damper operation, closure time and position indication</td>
<td>- Availability of Temporary Refuge HVAC system to match TR Impairment Frequency (TRIF)</td>
<td>- HVAC dampers on the Temporary Refuge boundary should meet SIL 2 (PFD of 10-2 to 10-3) - Safety Integrity Levels (SIL) to be identified for dampers on other areas and instrumentation that monitors HVAC operation (pressurisation and flow alarms, interlocks etc.)</td>
<td>- TR boundary dampers to have sufficient fire rating/blast protection to meet endurance period</td>
<td>- Fire &amp; Gas detection controls fans and dampers. Isolates non-certified electrical equipment on loss of pressurisation - HVAC provides pressurised atmosphere within Temporary Refuge - Certified electrical equipment ensures field equipment is suitable for use in a hazardous area</td>
</tr>
<tr>
<td>Drains</td>
<td>- Mechanical strength/integrity - Limits for corrosion, erosion, fatigue, coating breakdown, mechanical damage, water ingress to insulation, security of supports etc. - Sizing - Segregation (e.g. open/closed systems) - Bunded areas unobstructed and clear of debris</td>
<td>- Availability target should align with target production efficiency for plant</td>
<td>- Safety Integrity Levels (SIL) to be identified for drains tank level controls and indication (test intervals to ensure SIL levels are achieved)</td>
<td>- Dropped object resistance/protection - Blast resistance - Pool and jet fire resistance - Environmental criteria - Segregation (e.g. between fire zones)</td>
<td>- Drains remove flammable liquids from below vessels and rotating equipment in the event of a leak. This is mitigation against pool fires. - Liquids from the blowdown/flare system are pumped to the drains system - UPS provides power to drain pumps and instrumentation following loss of main power - Certified electrical equipment ensures field equipment is suitable for use in a hazardous area</td>
</tr>
<tr>
<td>Ballast Systems</td>
<td>- Pump sizing and performance - Corrosion protection/resistance - Ballast tank level control - Operation and accuracy of loading computer - Failure mode (valves) - Remote tank level indication - Tank internal coatings and corrosion resistance - Cathodic protection systems</td>
<td>- Availability target should align with target production efficiency for plant - Arrangements for alternative (back-up) loading computer</td>
<td>- Safety Integrity Levels (SIL) to be identified for ballast tank level controls and indication (test intervals to ensure SIL levels are achieved)</td>
<td>- Provision of ballast system isolation to allow system operation following collision damage - Operation of loss of main power supplies</td>
<td>- Hull provides secondary containment for liquid product. Isolates liquid product in the event of breach. - Emergency power to operate ballast pumps following loss of main power</td>
</tr>
</tbody>
</table>
## CONTROL SECE Barrier table (continued)

<table>
<thead>
<tr>
<th>SECE Example</th>
<th>Functions</th>
<th>Availability</th>
<th>Reliability</th>
<th>Survivability</th>
<th>Interdependence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Marine Inert Gas Systems</td>
<td>- Sizing</td>
<td>- Inert Gas supply required during offload operations</td>
<td>- Safety Integrity Levels (SIL) to be identified for failure of IG supply/quality to trip (test intervals to ensure SIL levels are achieved)</td>
<td>- Environmental criteria</td>
<td>- Certified electrical equipment ensures field equipment is suitable for use in a hazardous area</td>
</tr>
<tr>
<td></td>
<td>- Failure mode (valves)</td>
<td>- Supply rate to be in excess of offloading rate</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Control of inert gas generation (O2 content)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Pressure/Vacuum breaker location/functionality</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Pressure/Vacuum breaker liquid levels and glycol content</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Flame arrestors</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dynamic Positioning/Heading Control System</td>
<td>- Maximum excursion</td>
<td>- Emergency power supplies ensure system availability following loss of main power supplies</td>
<td>- Safety Integrity Levels (SIL) to be identified for system (test intervals to ensure SIL levels are achieved)</td>
<td>- Environmental criteria</td>
<td>- UPS provides emergency power following loss of main supply</td>
</tr>
<tr>
<td></td>
<td>- Monitoring and alarms (turret position, off-station, mooring tension etc.)</td>
<td></td>
<td></td>
<td></td>
<td>- Provides protection to and monitoring of Mooring System integrity</td>
</tr>
<tr>
<td></td>
<td>- Manual and automatic operation of thrusters</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Operation and condition of thrusters</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Condition of hydraulic supplies to thrusters</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Position/heading reference data (gyro compass/GPS etc.)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Condition/operation of turret bearing (including hydraulic systems)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ignition Prevention</td>
<td>- Selection and condition of 'Ex' certified electrical equipment</td>
<td>- Ignition prevention functionality to be available while electrical equipment in hazardous areas is energised. Power supplies to be isolated in non-hazardous areas on confirmed gas detection or loss of pressurisation</td>
<td>- Sample sizes for 'Ex' equipment inspections to be reviewed in accordance with IEC 60079-17</td>
<td></td>
<td>- Ex' Electrical Equipment is not required to survive a fire or explosion in the area where ignition will already have occurred.</td>
</tr>
<tr>
<td></td>
<td>- Sizing, condition and continuity of anti-static devices, grounding and bonding</td>
<td></td>
<td></td>
<td></td>
<td>- HVAC maintains safe areas by pressurisation and limits flammable gas accumulations within hazardous area atmospheres</td>
</tr>
<tr>
<td></td>
<td>- Location and condition of insulation to limit surface temperatures</td>
<td></td>
<td></td>
<td></td>
<td>- Fire &amp; Gas system isolates non-certified electrical equipment in the event of gas detection / loss of pressurisation</td>
</tr>
<tr>
<td></td>
<td>- Condition and security of spark and flame arrestors</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### MITIGATION SECE Barrier table

<table>
<thead>
<tr>
<th>SECE Example</th>
<th>Functions</th>
<th>Availability</th>
<th>Reliability</th>
<th>Survivability</th>
<th>Interdependence</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Fire Water Pumps</strong></td>
<td>- Methods and operation of manual and automatic initiators</td>
<td>- Sufficient water supply to meet demand scenarios identified in fire risk analysis</td>
<td>- Pump diversity to meet demand</td>
<td>- Dropped object resistance/protection</td>
<td>- UPS supply to fire pump starting and control systems</td>
</tr>
<tr>
<td></td>
<td>- Operation of firepump starting systems (electric, mechanical, pneumatic etc.)</td>
<td></td>
<td></td>
<td>- Blast resistance</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Remote status indication</td>
<td></td>
<td></td>
<td>- Pool and jet fire resistance</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Operation of firepump starting logic (duty, stand-by etc.)</td>
<td></td>
<td></td>
<td>- Environmental criteria</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Condition of drive (diesel) engine and ancillaries (fuel, coolant, ventilation etc.)</td>
<td></td>
<td></td>
<td>- Fire rating for control cables</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Operation of diesel engine protection (overspeed, low lube oil etc.)</td>
<td></td>
<td></td>
<td>- Operation of start system on loss of main power supplies (duration/number of diesel engine starts)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Pump delivery performance (flow rate, delivery pressure)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Fire Water Distribution and Monitors</strong></td>
<td>- Condition of ring main pipework and supports</td>
<td>- Sufficient water supply to meet demand scenarios identified in fire risk analysis required</td>
<td>- By design: Operational target not appropriate</td>
<td>- Isolation valves on the firemain allow damaged sections to be isolated in MAH</td>
<td>- Fire Pumps to supply firewater</td>
</tr>
<tr>
<td></td>
<td>- Operation of ring main isolation valves</td>
<td></td>
<td></td>
<td>- Pool and jet fire resistance</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Condition of monitors</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Operation of monitor oscillation and locking devices</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Monitor Spray patterns</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Operation of interface with cooling water systems (actuated crossover valves)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Ringmain pressure monitoring (to initiate fire/ jockey pump)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Deluge and Foam Systems</strong></td>
<td>- Operation of manual and automatic initiators</td>
<td>- Sufficient water supply to meet demand scenarios identified in fire risk analysis required</td>
<td>- Safety Integrity Levels (SIL) to be identified for deluge valve operation (test intervals to ensure SIL levels are achieved)</td>
<td>- Isolation valves on the firemain allow damaged sections to be isolated in MAH</td>
<td>- Fire Pumps and Firewater distribution system (ringmain) to supply firewater</td>
</tr>
<tr>
<td></td>
<td>- Deluge valve failure mode</td>
<td></td>
<td></td>
<td>- Deluge valves located outside protected areas</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Reaction time to water delivery</td>
<td></td>
<td></td>
<td>- Pool and jet fire resistance</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Spray patterns (blocked nozzles)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Flow rate and delivery pressure (at most hydraulically remote nozzle)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Coverage (areas, flow rate, fluid density)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Cleanliness of foam proportioners</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Quality of stored and produced foam (% concentration)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Condition of foam storage tanks and distribution pipework</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Helideck Firefighting Equipment</strong></td>
<td>- Operation of manual and automatic initiators</td>
<td>- Sufficient water supply to meet demand scenarios identified in fire risk analysis required</td>
<td>- Safety Integrity Levels (SIL) to be identified for deluge valve operation (test intervals to ensure SIL levels are achieved)</td>
<td>- Shelf life of foam concentrates</td>
<td>- Process Containment to prevent loss of helifuel</td>
</tr>
<tr>
<td></td>
<td>- Quality of stored and produced foam (% concentration)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Reaction time to foam delivery</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Operation of foam monitor oscillation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Duration of foam supply</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Effective helideck coverage and throw</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Gaseous Fire Protection Systems
- Operation of manual and automatic initiators
- Condition and rating of fusible loops
- Operation of firing system (failure modes)
- Duration and concentration level of suppressant required in protected space
- Remote status indication
- Pre-release warning alarms, time delays and warning signage
- Sufficient quantity of suppressant
- Retention of extinguishing agent in protected area (damper, bulkhead penetrations, turbine enclosure etc.)
- Condition and cleanliness of discharge nozzles
- Quantities of suppressant required to achieve required concentration level
- Condition of protected space boundaries (doors, bulkhead penetrations, turbine enclosure etc.) to retain suppressant
- Operation of ventilation dampers at boundary of protected space
- Safety Integrity Levels (SIL) to be identified for system activation device (test intervals to ensure SIL levels are achieved)
- Location of suppressant storage outside protected space
- HVAC to operate boundary dampers on demand and monitor pressurisation of protected area (remote alarm if doors left open)

### Sprinkler Systems
- Operation of manual and automatic initiators
- Remote status indication
- Frangible bulb condition and temperature rating
- Minimum delivery pressure and flow rate
- High availability target required
- Safety Integrity Levels (SIL) to be identified for flow and pressure monitoring instrumentation (test intervals to ensure SIL levels are achieved)
- By design - No survivability criteria for ongoing suitability
- Fire & Gas detection system to initiate sprinkler and indicate activation
- Fire Pumps and Firewater distribution system to supply firewater

### Manual Firefighting Equipment
- Operability of Hydrants
- Condition and availability of valve couplings
- Quantity, condition and location of hoses
- Condition and availability of in-line pressure regulating device
- Quantity and location of wheeled and portable extinguishers
- Certification of wheeled and portable extinguishers
- Manual firefighting equipment to be provided ready for immediate use at their designated location (Safety Equipment Layout drawings)
- No specific reliability target for this Safety Critical Element (SECE)
- By design - No survivability criteria for ongoing suitability
- Fire Pumps and Firewater Distribution to supply firewater
- Personal Survival Equipment to provide appropriate PPE for emergency response team personnel

### Passive Fire Protection (PFP)
- Protected areas
- Limits of degradation - bonding breakdown, exposed areas, 'coat-back' on attachments to protected areas
- Vent paths adjacent to blast walls unobstructed
- Fitment of PFP jackets on (riser) ESD valves
- PFP to be available at all times during normal operations
- No specific reliability target for this Safety Critical Element (SECE)
- Design criteria (fire suitable rating) for survival time of protected areas
- Limits for blast overpressures (X mBar)
- Primary structures that require protection
### EMERGENCY RESPONSE SECE Barrier table

<table>
<thead>
<tr>
<th>SECE Example</th>
<th>Functions</th>
<th>Availability</th>
<th>Reliability</th>
<th>Survivability</th>
<th>Interdependence</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Temporary Refuge (TR)</strong></td>
<td>- Space for entire POB to muster</td>
<td>- Availability target for Temporary Refuge to match TR Impairment Frequency (TRIF)</td>
<td>- High reliability target for HVAC dampers on the TR boundary (SIL 2)</td>
<td>- TR to prevent an ingress of flammable gas to smoke (i.e. retain a positive pressurisation) for a period of X minutes.</td>
<td>- Topside Structures provide support and survivability for the TR</td>
</tr>
<tr>
<td></td>
<td>- Condition of boundary doors and seals</td>
<td></td>
<td>- High reliability target for instrumentation that monitors HVAC operation (pressurisation and flow alarms, interlocks etc.)</td>
<td>- TR to survive all hydrocarbon oil fires for a period of X minutes (by design)</td>
<td>- HVAC systems (initially) provide a safe, breathable atmosphere with the TR</td>
</tr>
<tr>
<td></td>
<td>- Condition of other bulkhead penetrations</td>
<td></td>
<td>- Provision of battery-backed emergency lighting in muster and command &amp; control areas (duration)</td>
<td>- TR to survive blast overpressure of X mbar (by design)</td>
<td>- Passive Fire Protection protect the TR from the effects of fire and explosion</td>
</tr>
<tr>
<td></td>
<td>- TR leakage rate - Integrity of enclosure to retain positive pressure for survival period (may be expressed in air changes per hour)</td>
<td></td>
<td></td>
<td>- Provision of battery-backed emergency lighting to mitigate effects of smoke (duration)</td>
<td>- Active fire protection systems provide emergency command and control facilities through provision of manual firewater pump start and remote release facilities for deluge and extinguishing systems within the TR</td>
</tr>
<tr>
<td></td>
<td>- Number of air changes during normal operations ()</td>
<td></td>
<td></td>
<td></td>
<td>- ESD System provide emergency process control and shutdown initiation facilities within the TR</td>
</tr>
<tr>
<td></td>
<td>- Pressurisation during normal operations ()</td>
<td></td>
<td></td>
<td></td>
<td>- Fire &amp; Gas Detection monitors presence of fire or potentially flammable atmospheres that could impair the TR</td>
</tr>
<tr>
<td></td>
<td>- Location of inlets/outlets (relative to haz. areas)</td>
<td></td>
<td></td>
<td></td>
<td>- UPS and emergency generator provide emergency power to command and control systems within the TR</td>
</tr>
<tr>
<td></td>
<td>- HVAC Fan and damper status indication (what &amp; where)</td>
<td></td>
<td></td>
<td></td>
<td>- Emergency Communications inform personnel of the need to muster and/or evacuate</td>
</tr>
<tr>
<td></td>
<td>- Operation of instrumentation to monitor area pressurisation / flow rates</td>
<td></td>
<td></td>
<td></td>
<td>- Emergency Communications provide communication facilities with aircraft, shipping (including the Emergency Response &amp; Rescue Vessel) and external rescue agencies</td>
</tr>
<tr>
<td></td>
<td>- HVAC damper operation, closure time and position indication</td>
<td></td>
<td></td>
<td></td>
<td>- Personal Survival Equipment provides personnel in the TR with protective equipment</td>
</tr>
<tr>
<td><strong>Escape Routes</strong></td>
<td>- Dimensions</td>
<td>- Duration of escape lighting (escape routes, muster and embarkation areas)</td>
<td>- By design: operational target not appropriate</td>
<td>- Blast resistance</td>
<td>- Topside Structures to provide adequate support and aid survivability of escape routes</td>
</tr>
<tr>
<td></td>
<td>- Visibility and limits for degradation of markings</td>
<td></td>
<td></td>
<td>- Pool and jet fire resistance</td>
<td>- Passive Fire Protection to protect escape routes from the effects of fire/explosion</td>
</tr>
<tr>
<td></td>
<td>- Condition of non-slip surfaces</td>
<td></td>
<td></td>
<td>- Provision of battery-backed emergency lighting to mitigate effects of smoke (duration)</td>
<td>- Personal Survival Equipment to provide equipment to assist personnel to escape to a place of safety</td>
</tr>
<tr>
<td></td>
<td>- Obstructions on walkways and access/egress points</td>
<td></td>
<td></td>
<td></td>
<td>- Emergency Communications to control alert personnel of the need to muster and advise routes/areas to avoid</td>
</tr>
<tr>
<td></td>
<td>- Obstructions in evacuation and escape embarkation areas</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Obstructions affecting access to emergency response or escape equipment</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Condition and closure of doors at pressurised areas/air-locks</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Intensity of escape lighting</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Signage at changes of direction</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>TEMPSC</strong></td>
<td>- Condition of canopy, hull/stem glands, doors and seals</td>
<td>- HSE guidance identifies 150% design capacity</td>
<td>- High reliability target for launch readiness (engine starting etc.)</td>
<td>- Independent air system allows use in smoke filled or toxic atmospheres</td>
<td>- Topside Structures to support lifeboat davits</td>
</tr>
<tr>
<td></td>
<td>- Condition and (fixed time) replacement of fall wires</td>
<td>- Sufficient capacity to enable all persons to evacuate to a place of safety to be provided at all times</td>
<td>- High reliability target for release gear (fail to release and fail open) to be considered</td>
<td>- Deluge system provide protection from radiated heat</td>
<td>- Emergency Communications provides an electronic location beacon and voice communication with CCR/radio room/stand-by vessel</td>
</tr>
<tr>
<td></td>
<td>- Davit load test certification</td>
<td>- High target required for TEMPSC availability (e.g. 98% = 7 days downtime per year for maintenance and testing).</td>
<td>- Location of TEMPSC allows embarkation from Temporary Refuge</td>
<td>- TEMPSC protected from explosion overpressures by location (by design)</td>
<td>- Heading Control System to provide a sheltered (lee) area for the TEMPSC to launch from floating installations</td>
</tr>
<tr>
<td></td>
<td>- Condition of davits and deck connections (NDT examination)</td>
<td>- Size of embarkation areas and illumination by battery-backed escape lighting</td>
<td>- Provision for persons who cannot access the TR in MAH</td>
<td></td>
<td>- Ballast System prevents heel or trim angles which could prevent TEMPSC launch from floating installations</td>
</tr>
<tr>
<td></td>
<td>- Operation of clutch and steering</td>
<td>- Status of batteries and charging systems (fixed time battery replacement)</td>
<td></td>
<td></td>
<td>- Tertiary Escape Systems provide alternative means of escape in the event of TEMPSC unavailability</td>
</tr>
<tr>
<td></td>
<td>- Security and condition of harneses</td>
<td>- Pressurisation air (charge pressure and bottle certification)</td>
<td></td>
<td></td>
<td>- Escape Routes to ensure that embarkation areas are unobstructed and adequately illuminated</td>
</tr>
<tr>
<td></td>
<td>- Operation of interior lighting</td>
<td>- Operation of radio communication (with CCR, Radio Room, Stand-by vessel)</td>
<td></td>
<td></td>
<td>- Emergency Response and Recovery (Stand-by Vessel) provides a ‘place of safety’</td>
</tr>
<tr>
<td></td>
<td>- Fuel tank level and quality (water contamination)</td>
<td>- Deluge system provide protection from radiated heat</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Status of batteries and charging systems (fixed time battery replacement)</td>
<td>- Provision for persons who cannot access the TR in MAH</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Descent rate (laden or unladen)</td>
<td>- TEMPSC allows embarkation from Temporary Refuge</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Engine starting (via diverse systems)</td>
<td>- Size of embarkation areas and illumination by battery-backed escape lighting</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Security and condition of harneses</td>
<td>- Provision for persons who cannot access the TR in MAH</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Operation of interior lighting</td>
<td>- Status of batteries and charging systems (fixed time battery replacement)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Fuel tank level and quality (water contamination)</td>
<td>- TEMPSC allows embarkation from Temporary Refuge</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Status of batteries and charging systems (fixed time battery replacement)</td>
<td>- Size of embarkation areas and illumination by battery-backed escape lighting</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Descent rate (laden or unladen)</td>
<td>- Provision for persons who cannot access the TR in MAH</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Engine starting (via diverse systems)</td>
<td>- TEMPSC allows embarkation from Temporary Refuge</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Security and condition of harneses</td>
<td>- Size of embarkation areas and illumination by battery-backed escape lighting</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Operation of interior lighting</td>
<td>- Provision for persons who cannot access the TR in MAH</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Fuel tank level and quality (water contamination)</td>
<td>- TEMPSC allows embarkation from Temporary Refuge</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Status of batteries and charging systems (fixed time battery replacement)</td>
<td>- Size of embarkation areas and illumination by battery-backed escape lighting</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Descent rate (laden or unladen)</td>
<td>- Provision for persons who cannot access the TR in MAH</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Engine starting (via diverse systems)</td>
<td>- TEMPSC allows embarkation from Temporary Refuge</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Security and condition of harneses</td>
<td>- Size of embarkation areas and illumination by battery-backed escape lighting</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Operation of interior lighting</td>
<td>- Provision for persons who cannot access the TR in MAH</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Fuel tank level and quality (water contamination)</td>
<td>- TEMPSC allows embarkation from Temporary Refuge</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Status of batteries and charging systems (fixed time battery replacement)</td>
<td>- Size of embarkation areas and illumination by battery-backed escape lighting</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Descent rate (laden or unladen)</td>
<td>- Provision for persons who cannot access the TR in MAH</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Engine starting (via diverse systems)</td>
<td>- TEMPSC allows embarkation from Temporary Refuge</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Security and condition of harneses</td>
<td>- Size of embarkation areas and illumination by battery-backed escape lighting</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Operation of interior lighting</td>
<td>- Provision for persons who cannot access the TR in MAH</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Fuel tank level and quality (water contamination)</td>
<td>- TEMPSC allows embarkation from Temporary Refuge</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Status of batteries and charging systems (fixed time battery replacement)</td>
<td>- Size of embarkation areas and illumination by battery-backed escape lighting</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Descent rate (laden or unladen)</td>
<td>- Provision for persons who cannot access the TR in MAH</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Engine starting (via diverse systems)</td>
<td>- TEMPSC allows embarkation from Temporary Refuge</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Security and condition of harneses</td>
<td>- Size of embarkation areas and illumination by battery-backed escape lighting</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Operation of interior lighting</td>
<td>- Provision for persons who cannot access the TR in MAH</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Fuel tank level and quality (water contamination)</td>
<td>- TEMPSC allows embarkation from Temporary Refuge</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Status of batteries and charging systems (fixed time battery replacement)</td>
<td>- Size of embarkation areas and illumination by battery-backed escape lighting</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Descent rate (laden or unladen)</td>
<td>- Provision for persons who cannot access the TR in MAH</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## EMERGENCY RESPONSE SECE Barrier table (continued)

<table>
<thead>
<tr>
<th>SECE Example</th>
<th>Functions</th>
<th>Availability</th>
<th>Reliability</th>
<th>Survivability</th>
<th>Interdependence</th>
</tr>
</thead>
</table>
| Personal Survival Equipment | - Location and quantities (relative to POB)  
- Cabin grab bag contents  
- Inspection/Recertification date (SOLAS/LSA Code requirements)  
- Condition and accessibility of storage cabinets  
- Defined life replacement  
- Design/construction standard of equipment  
- Capacity of breathing apparatus  
- Tools and PPE for Emergency Response Team and Helideck crews | - Location of equipment (relative to muster + other areas)  
- Provision within the Temporary Refuge  
- Provision for persons who cannot access the TR in MAH | - By design: operational target not appropriate  
- Design/construction standard of equipment | - Location of equipment (fire/blast protection)  
- Equipment design rating | - Emergency Response and Recovery (Stand-by) Vessel provides a “place of safety” and facilities to rescue evacuees from the sea |
| Tertiary Escape Systems | - Location and quantities (relative to POB)  
- Design/construction standard of equipment  
- Inspection/Recertification date (SOLAS/LSA Code requirements)  
- Condition and accessibility of storage cabinets  
- Defined life replacement  
- Operation of winch brakes and release mechanism  
- Davit load test certification  
- Condition of davits and deck connections (NDT examination)  
- Condition and (fixed time) replacement of fall wires (liferafts)  
- Condition and certification of descent device anchor points  
- Condition of escape to sea ladders | - Location of equipment (relative to muster + other areas)  
- Provision within the Temporary Refuge  
- Provision for persons who cannot access the TR in MAH | - By Design: Equipment Designed/constructed to SOLAS/LSA Code standards | - Location of equipment (fire/blast protection)  
- Equipment design rating | - Temporary Refuge provides a safe environment to collect and don personal survival equipment  
- Structural integrity ensures escape to sea ladders remain suitable and provides support to davits  
- Escape Routes enable access to personal survival equipment  
- Emergency Response and Recovery (Stand-by) Vessel provides a “place of safety” and facilities to rescue evacuees from the sea |
## Appendix 4

### Examples of Verification Benefits

### Example 1

1. **Provide a single sentence summarising the relevant System and Issue**

   ICP identifies significant improvements to Duty Holder’s SECE Assurance Process.

2. **Describe the problem and how Verification identified this**

   **Issue**
   
   Through a robust Operational Verification Scheme, the ICP was instructed to thoroughly scrutinise the SECE Assurance Process for all identified SECEs. Through this process, the ICP identified several areas where the SECE Assurance Process was not suitable and as a result escalated the issue by combining the individual issues and raised a high level Finding that allowed the Duty Holder to investigate and implement an Effective Solution.

   **Examples**
   
   **Fire Fighting (Automatic and Manual) and Life Saving Apparatus Assurance Process** was not suitable due to:
   - Poorly defined Performance Standards
   - Assurance activities did not assure against the Performance Standard
   - Vendor had no visibility of Performance Standard
   - Vendor Assurance records were poor and not visible in Duty Holder’s Maintenance Management System (MMS)
   - Follow-up of Safety Critical Remedial work was not auditable

   **Hazardous Area Electrical Equipment Assurance Process** was not suitable due to:
   - Poor HAE Strategy
   - Poorly managed inspections: Equipment not being inspected as per plan
   - Variable Competency
   - Exact Quantity of HAE items unknown
   - Poor recording of newly installed equipment
   - Resourcing not well managed to execute workload

   **Improvements made**
   
   **Fire Fighting (Automatic and Manual) and Life Saving Apparatus Assurance Process**:
   - Performance Standards improved
   - Assurance activities aligned to Performance Standards
   - Assurance activities embedded in Duty Holder’s MMS
   - Communication with Vendor improved
   - History of Assurance activities improved
   - Remedial work clearly recorded in Duty Holder’s MMS

   **Hazardous Area Electrical Equipment Assurance Process**:
   - New HAE Philosophy written and issued
   - Duty Holder site audits implemented to assess effectiveness and competency of inspections
   - Specific HAE onshore resource appointed
   - Complete review and rescheduling to aid efficient inspections
   - Manning levels better understood

   **Benefits**
   
   - HAE inspections being competently inspected in the most efficient manner, resulting in confidence of HAE Integrity
   - Cost saving as retrospective campaigns to liquidate backlog avoided
   - Cost saving as Integrity issues identified early and potentially resolved within normal outages, thus avoiding potential shutdowns for replacement of critical equipment
   - Legal Compliance maintained
   - Reputation secured

3. **Explain the potential consequences which may have arisen should Verification not have identified the Issue**

   - HAE integrity would have been compromised and therefore the potential for ignition resulting in a Major Accident and potentially leading to fatalities would increase
   - Improvement Notice from HSE
   - Potential for shutdown until SECEs were compliant, resulting in loss of production
Examples of Verification Benefits

**Example 2**

1. **Provide a single sentence summarising the relevant System and Issue**

   For Engineering Changes, the Duty Holder was unable to demonstrate that suitable Assurance Processes were in place to manage SECEs and their associated Performance Standards.

2. **Describe the problem and how Verification identified this**

   **Issue**
   
   Assurance Process by the Engineering Contractor (EC) did not suitably show SECEs and their associated Performance Standards had been assured. This resulted in SECEs not meeting their Performance Standards.
   
   Through the Activities documented in the Verification Scheme for Projects and Modifications, the ICP identified several instances where SECEs were not meeting their Performance Standards. Examples were:
   
   - Emergency Lighting designed / procured and tested for 90 min duration when Performance Standard was 120min
   - HVAC designed to 6 air changes/hr when Performance Standard was 12 air changes/hr
   - Electrical Cabling designed / procured and installed to incorrect fire protection rating
   
   No Technical Deviations were raised by the EC.
   
   ICP escalated the issue by combining the individual issues and raised a high level Finding that allowed the Duty Holder to investigate and implement an effective solution.

   **Improvements made**
   
   - Improvements to EC Assurance Process so that SECE Performance Standards were clearly assured at Design, Procurement, Construction, Commissioning and Handover. For example:
     
     1) Design Engineers signing to confirm they had met the identified SECE Performance Standards for each Modification / Project
     2) Commissioning identifying all the SECE Performance Standards up-front, and documenting which Offshore Test Procedures would assure that Performance Standard

   **Benefits**
   
   - Increased confidence that SECEs will work as intended when required
   - It is more cost effective to meet the Performance Standard before handover than to retrospectively engineer solutions to meet the Performance Standard
   - Legal compliance maintained
   - Reputation secured

3. **Explain the potential consequences which may have arisen should Verification not have identified the Issue.**

   - SECEs would not have been effective during a Major Accident resulting in an escalation of the event and potentially leading to fatalities
   - Improvement Notice from HSE
   - Potential for shutdown until SECEs were compliant, resulting in loss of production
Examples of Verification Benefits

Example 3

1. Provide a single sentence summarising the relevant System and Issue

ICP identifies significant fault in a SIL 3 rated Safety Critical system in which overpressure of an interfield pipeline was possible.

2. Describe the problem and how Verification identified this

Issue

During function testing of an Interfield pipeline Over Pressure Protection System (OPPS), it was noted by the Verifier that there was a fault with one of the pipeline pressure sensor control system cards for the OPPS. On investigation of the internal cards it was found that the analogue input card in slot 1 was indicating a fault signified by a Light Emitting Diode (LED) “1” flashing. The card was also showing a green healthy LED as per the other cards installed in slots 2 and 3 which are for the other 2 pressure sensors. The fault state was not transmitted to either the matrix panel or Integrated Control Safety System (ICSS), screens for operator attention, therefore for some unknown period of time the OPPS had been operating at a lower integrity, 2 out of 2, (2oo2) voting system.

If there are no methods by which to inform the Control Room Operators on the ICSS or the matrix panel then it is possible that 2 of the 3 cards may be in fault but the system would still be operating at a 2oo3 voting system. This has catastrophic potential as all 3 PTs could be showing overpressure but the Emergency Shutdown (ESD) System would only see the 1oo3 overpressure signal and no executive actions would be taken. The cards were located on a normally unmanned installation which made the ad-hoc discovery of the fault more unlikely.

Improvements made

• New cards provided by manufacturer which allow voting to be decreased to 1oo2 should there be any equipment failure, thus maintaining the integrity of the system
• Regular inspection of the lamps on the control panel in which the control cards are located. PM frequency amended to ensure more regular checks completed
• Remote alarm warning system implemented to allow the status of the cards to be monitored from the control room which is on a manned platform several kilometres away

Benefits

• Performance Standard availability and reliability remains assured and therefore legal compliance maintained
• Integrity of SIL rated system now much more robust
• Reduction in risk of overpressure situation arising undetected
• Reputation secured

3. Explain the potential consequences which may have arisen should Verification not have identified the Issue.

• Overpressure situation within Interfield pipeline causing catastrophic event at unmanned platform. Multiple fatalities a possibility
• Huge environmental situation which is very hard to control due to ruptured subsea pipeline. Far reaching and large scale pollution
• Large Production loss
• Worldwide media, public scrutiny and criticism
Appendix 5

An example of how sample size for Verification activities can be defined

The level of examination conducted by the Verifier must be defined within the Verification Scheme. One way of determining the level of examination is to determine a sample size for each SECE by using examination levels linked to the criticality of the equipment; criticality being a combination of the consequence of failure, risk associated with failure and level of redundancy.

**Examination Level 1**: Equipment with high consequence of failure and little or no levels of redundancy. Failure during normal operation is likely to result in, or initiate, a MAH.

**Examination Level 2**: Equipment with a significant consequence of failure and at least one level of redundancy. Failure during normal operations is unlikely to result in a MAH but is likely to contribute towards escalating an event.

**Examination Level 3**: Equipment with a low consequence of failure and multiple levels of redundancy. Failure during normal operations would not cause a MAH but may contribute towards escalating an event.

The percentage of equipment or routines to be examined per year for each Verification activity can then be defined, e.g.

<table>
<thead>
<tr>
<th>Examination Level</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Offshore examination visual / witness</td>
<td>40-100%</td>
<td>20-40%</td>
<td>10-20%</td>
</tr>
<tr>
<td>Onshore review of records</td>
<td>60-100%</td>
<td>40-60%</td>
<td>20-40%</td>
</tr>
</tbody>
</table>

Note that care should be taken when applying this approach to the individual Verification activities because it would not be possible for the Verifier to visually inspect 40% of pipework or ‘Ex’ equipment. Process audits on how the SECEs are managed can be defined and used to supplement the activity.

<table>
<thead>
<tr>
<th>Prevention</th>
<th>Examination Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process containment</td>
<td>1</td>
</tr>
<tr>
<td>Well integrity</td>
<td>1</td>
</tr>
<tr>
<td>Jacket / hull integrity</td>
<td>1</td>
</tr>
<tr>
<td>Tops side structures</td>
<td>1</td>
</tr>
<tr>
<td>Mooring system</td>
<td>1</td>
</tr>
<tr>
<td>Ignition prevention</td>
<td>2</td>
</tr>
<tr>
<td>Lifting equipment</td>
<td>2</td>
</tr>
<tr>
<td>Hazardous area ventilation</td>
<td>1</td>
</tr>
<tr>
<td>Fire &amp; gas detection</td>
<td>3</td>
</tr>
<tr>
<td>ESD system (Inputs)</td>
<td>2</td>
</tr>
<tr>
<td>ESD system (logic solver and outputs)</td>
<td>1</td>
</tr>
<tr>
<td>Pressure relief, flare and blowdown</td>
<td>2</td>
</tr>
<tr>
<td>High integrity pressure protection systems</td>
<td>1</td>
</tr>
<tr>
<td>Drilling well control</td>
<td>1</td>
</tr>
<tr>
<td>Non-hazardous ventilation</td>
<td>2</td>
</tr>
<tr>
<td>Ballast systems</td>
<td>1</td>
</tr>
<tr>
<td>Marine inert gas systems</td>
<td>2</td>
</tr>
<tr>
<td>Dynamic positioning / heading control system</td>
<td>1</td>
</tr>
<tr>
<td>Hazardous drains</td>
<td>2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Prevention</th>
<th>Examination Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Passive fire protection (PFP)</td>
<td>2</td>
</tr>
<tr>
<td>Fire water pumps</td>
<td>2</td>
</tr>
<tr>
<td>Deluge and foam systems</td>
<td>3</td>
</tr>
<tr>
<td>Fire water monitors</td>
<td>3</td>
</tr>
<tr>
<td>Gaseous fire protection systems</td>
<td>3</td>
</tr>
<tr>
<td>Helideck firefighting</td>
<td>3</td>
</tr>
<tr>
<td>Sprinkler systems</td>
<td>3</td>
</tr>
<tr>
<td>Manual firefighting equipment</td>
<td>3</td>
</tr>
<tr>
<td>Temporary refuge (TR)</td>
<td>2</td>
</tr>
<tr>
<td>Escape routes</td>
<td>3</td>
</tr>
<tr>
<td>TEMPS</td>
<td>3</td>
</tr>
<tr>
<td>Tertiary escape systems</td>
<td>3</td>
</tr>
<tr>
<td>Personal survival equipment</td>
<td>3</td>
</tr>
<tr>
<td>Emergency communications</td>
<td>3</td>
</tr>
<tr>
<td>Helicopter facilities</td>
<td>3</td>
</tr>
<tr>
<td>Emergency response and rescue vessel (ERRV)</td>
<td>3</td>
</tr>
</tbody>
</table>