Oil & Gas UK

the voice of the offshore industry

Guidance on the Conduct and Management of Operational Risk Assessment for UKCS Offshore Oil and Gas Operations

Issue 1
January 2012

Guidance on the Conduct and Management of Operational Risk Assessment for UKCS Offshore Oil and Gas Operations
Issue 1, January 2012

© The United Kingdom Offshore Oil and Gas Industry Association Limited (trading as Oil & Gas UK), 2011.

Any material within these guidelines that has been reproduced has been done so with the permission of its owners. Contains public sector information licensed under the Open Government Licence v1.0, which can be found at http://www.nationalarchives.gov.uk/information-management/uk-gov-licensing-framework.htm

The information contained herein is given for guidance only. These guidelines are not intended to replace professional advice and are not deemed to be exhaustive or prescriptive in nature. Although the authors have used all reasonable endeavours to ensure the accuracy of these guidelines neither Oil & Gas UK nor any of its members assume liability for any use made thereof. In addition, these guidelines have been prepared on the basis of practice within the UKCS and no guarantee is provided that these guidelines will be applicable for other jurisdictions.

While the provision of data and information has been greatly appreciated, where reference is made to a particular organisation for the provision of data or information, this does not constitute in any form whatsoever an endorsement or recommendation of that organisation.

ISBN: 1 903 003 77 5

PUBLISHED BY OIL & GAS UK

London Office:
6th Floor East, Portland House, Bressenden Place, London, SW1E 5BH
Tel: 020 7802 2400 Fax: 020 7802 2401

Aberdeen Office:
Exchange 2, 3rd Floor, 62 Market Street, Aberdeen, AB11 5PJ
Tel: 01224 577250 Fax: 01224 577251

Email: info@oilandgasuk.co.uk
Website: www.oilandgasuk.co.uk

Contents

Acknowledgements

In publishing this guidance document, Oil & Gas UK gratefully acknowledges the support and contributions from work group representatives drawn from Amec, Apache, BP, Chevron, CNR, Talisman, Taqa, and HTC Human Technologies. We also appreciate draft reviews undertaken by members of the Oil & Gas UK Major Hazards Management Forum and by Inspectors from the Offshore Division of the Health & Safety Executive.

1. Introduction, Objectives and Application

The effective management of major accident hazards (MAH) is an integral feature of safe operations on offshore oil and gas installations. Robust arrangements are in place to identify and evaluate major accident hazards, and to specify measures taken to ensure that major accident risks are controlled to ensure compliance with the relevant statutory provisions and to a level that is as low as reasonably practicable (ALARP). A demonstration that major accident hazards have been identified and that major accident risks are adequately controlled is documented in the installation safety case.

A duty holder's procedures for risk management need to be dynamic such that they accommodate and account for adverse changes in safety-critical element (SCE) provision or other abnormal situations that may potentially increase levels of major accident risk. This dynamic approach to risk management takes a number of forms and has various titles applied to the processes. For the purpose of this guidance, the term Operational Risk Assessment (ORA) is used in a generic sense, and it should be clear from the guidance that it applies equally to other forms of operational risk management typically undertaken by duty holders. Examples of other titles applied to forms of ORA include Safety Critical Risk Assessment (SCRA); Safety Critical Element Impairment Risk Assessment (SCEIRA); and Deviation Control Risk Assessment (DCRA).

A work group managed by Oil & Gas UK developed this guidance in order to help duty holders develop, implement and maintain robust operational risk assessment procedures to manage MAH where impairment* of a safety-critical element (including loss or degradation of a safety-critical component forming a significant part of an SCE) or some other abnormal operational situation may potentially compromise safety and increase major accident risk levels. The guidance is particularly targeted at personnel within duty holder organisations who may:

- develop, communicate and maintain procedures for operational risk management;
- manage the implementation of operational risk management procedures;
- lead or facilitate operational risk assessments; and / or
- monitor, audit or review operational risk management arrangements

The objective of the guidance is to help duty holders develop, maintain and implement ORA procedures that achieve a legally compliant, systematic and effective approach to operational risk management processes such that:

* Note that the terms "impairment" or "degradation" are typically used to describe failed SCE and can generally be taken to mean that the as-found failure results in less than 100% performance of that SCE. Note also that although other forms of "abnormal operations" may require ORA; for simplicity, this guidance will focus primarily on SCE impairment.

- a thorough assessment of major accident hazards associating with SCE impairment or other abnormal operational situations is carried out and risks are identified and evaluated; effective risk control and mitigation measures to manage risks arising from impaired SCE are properly identified, documented, implemented and monitored;
- steps are taken to provide assurance that interdependent SCE or other control measures associating with, or affected by the ORA are adequate, available and fully functional, or being managed under a separate ORA;
- the assessment and documented outputs are reviewed, endorsed and approved by relevant technically competent personnel;
- awareness of the abnormal condition and changes arising from an ORA is maintained and monitored until such time as permanent remediation is completed;
- there is a reliable basis for operational decision making and control;
- permanent remediation of impaired SCE or recovery actions from the abnormal situation are identified, prioritised and tracked to closure in an appropriate time scale; and
- operational risk management processes are managed and executed by suitably competent personnel

This guidance applies primarily to the operational risk assessment of degraded safety-critical elements. The principles and general methodologies described however, lend themselves to application to other forms of abnormal operations (e.g. the temporary loss of logistics support to an installation). The guidance adopts a good practice approach that retains some flexibility in terms of its application to a duty holder's operations and alignment with existing management systems and ORA procedures.

It should also be noted that although the terms major accident hazard and safety-critical element are used throughout this document, the guidance can be taken to apply to operational risk assessment where a significant environmental hazard may be present or where an identified Environmentally Critical Element (ECE) has been found to be degraded.

The guidance is designed for application to UKCS offshore installations but duty holders may also choose to apply the guidance to company-specific ORA procedures in place at onshore major hazard facilities.

It is particularly important to stress that the application of task risk assessment procedures, criteria and guide words focusing on personal injury outcomes only is inappropriate in operational risk assessment.

The Health & Safety Executive Semi Permanent Circular entitled "Safety critical elements good repair and condition" offers a Regulatory view on SCE degradation response. This document can be found at:

http://www.hse.gov.uk/foi/internalops/hid/spc/spcenf175.htm

2. Main Legislative References

The UK legislation referenced below primarily relates to the obligation for effective risk assessment or demonstrations that all major accident hazards have been identified and evaluated and measures taken to control risks.

1. Health and Safety at Work etc. Act 1974
2. Management of Health & Safety at Work Regulations 1999
3. Offshore Installations (Safety Case) Regulations 2005
4. Offshore Installations and Wells (Design & Construction etc.) Regulations 1996
5. Offshore Installations (Prevention of Fire & Explosion, and Emergency Response) Regulations 1995
6. Pipeline Safety Regulations 1996
7. Offshore Installations and Pipeline Works (Management and Administration) Regulations 1995
8. Provision and Use of Work Equipment Regulations 1998

3. Systematic approach to development and implementation of ORA procedures

This section provides guidance to duty holders on the development of company-specific ORA procedures. The guidance prompts procedural alignment with the Health & Safety Executive guidance document HSG65 “Successful Health & Safety Management”. Although not mandatory, this management system approach is commonly used across the UKCS so its application to ORA guidance allows easy harmonisation with wider aspects of a duty holder’s HSE Management System.

Operational risk assessment is one element of a wider suite of management system elements, processes and practices in place to manage major accident hazards. As an example of interdependence, impaired SCE may be revealed by integrity management activities and remediation of the impairment will become part of the maintenance management or action management systems. Figure 1 illustrates those wider system elements and their interrelationship.

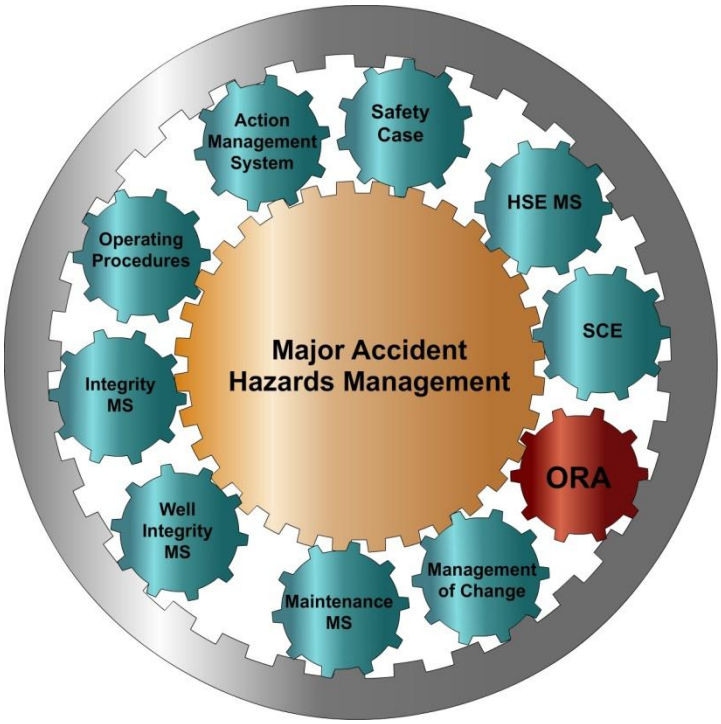


Figure 1. Illustration of relationship of ORA with other elements of MAH management.

Effective ORA arrangements should have characteristics described in the following sections.

3.1 Organisational Factors

The following organisational aspects should be provided for in ORA procedures:

3.1.1 Resources

Organisational capability and staffing arrangements need to be aligned to the effective management of ORA processes. In particular, organisations should take account of the need for the involvement of Technical Authorities, SCE Responsible Engineers and other onshore support personnel in the ORA process. The organization needs to be sized and staffed appropriately to allow for the involvement in the ORA process of all relevant personnel. The ORA procedure should make provision for the non-availability of specialist support personnel (e.g. Technical Authorities) out-of-hours for example, and describe how that absence affects the ORA process. The procedure should set out any constraints that may

apply where not all relevant personnel are available to play their part in the ORA process. In particular actions necessary to manage the abnormal situation where not all appropriate resources are available to conduct, review and approve an operational risk assessment should be defined.

3.1.2 Roles & Responsibilities

The procedure should describe the roles and responsibilities of personnel involved in identifying, planning, leading, participating in, reviewing, endorsing, approving and/or monitoring ORA processes and outputs. Positions that should be specifically accounted for in the procedure may include the following:

- Offshore Installation Manager;
- Offshore discipline Supervisors;
- Offshore HSE Adviser
- Offshore technicians;
- ORA Facilitator / Team Leader;
- Technical Safety personnel;
- Environmental Adviser (onshore)
- Technical Authorities (onshore Engineers)
- SCE Responsible Engineers (onshore Engineers with responsibility for specific SCE – duty holders use various titles for this role);
- Discipline Engineers (onshore);
- Asset / Operations management (onshore);
- Third party specialists / vendors; and
- Independent Verification Body personnel

The particular importance of the role of Technical Authorities and SCE Responsible Engineers (or equivalent titles) in the ORA process should be stressed in duty holder procedures.

Ideally the procedure should identify the various roles of personnel in the management and conduct of ORA using an approach along the lines of that shown in table 1. Duty holder procedures should detail levels of involvement in the process in line with the relative criticality of the major hazard issue being assessed and describe how that is reflected in the table.

This roles and responsibilities tabular approach may be supplemented or replaced by a RACI (Responsible, Accountable, Consulted, Informed) chart in the form of the exhibit provided in appendix 4.1 of this guidance. This example is for guidance purposes only and it will be for duty holders to develop a RACI chart that accurately reflects their specific organisational and procedural arrangements. These should for example align and describe levels of authority and at what point an ORA might be approved by an Asset or Operations Manager rather than the OIM.

Table 1: Typical Roles and responsibilities of personnel involved in ORA.

	I	L	P	R	E	A
OIM	•			•	•	•
Offshore Supervisors		•	•			
Offshore Technicians			•			
Technical Safety		•	•	•	•	
Technical Authorities	•	•	•	•	•	
SCE Responsible Engineers	•	•	•	•	•	
Asset / Operations Management				•	•	•
Third Party Specialists			•	•		

I = Initiate **L** = Lead ORA **P** = Participate **R** = Review **E** = Endorse **A** = Approve

3.1.3 Training & Competence

It is essential that personnel involved in ORA in any capacity are adequately trained and suitably equipped for their specific roles. The distinctive nature of ORA and its linkage to major accident hazards calls for specific training in order to achieve an effective approach to ORA. Duty holders should ensure that they provide sufficient information, instruction, training and supervision to personnel involved in the ORA process. Such personnel should possess or attain necessary attributes, knowledge and skills as follows:

- a thorough understanding of major accident hazards specific to that facility; safety critical elements; and SCE verification and performance standards;
- awareness and understanding of key information documented in the installation Safety Case; main plant isolatable inventories; incident escalation pathways; and prevention, control and mitigation barriers;
- awareness of process safety and integrity management principles, engineering standards and specifications ;
- relevant plant knowledge, understanding of operational status / plant conditions and suitable experience;
- ability to apply ORA process and methodology;
- understanding of any SCE impairment rule sets;
- understanding of specific site emergency response plans and procedures;
- facilitation and communication skills to enable full and active participation by team members; and

- awareness of suitability and limitations of ORA process

3.2 Planning & Implementation

This section describes the operational risk assessment process in terms of:

- identification of circumstances in which ORA is necessary and appropriate;
- rule based approach to SCE management;
- ORA methodology and key considerations in assessing risk;
- considering combined risk and connectivity, including any changes in risk level over the period the abnormal situation is experienced;
- ORA review and approval processes; and
- ongoing management until permanent remediation is effected

Procedures should conform to the broad principles set out in this section, although there is an element of flexibility in relation to specific ORA methodology and assessment tools deployed by individual duty holders. Figures 4.1 and 4.2 illustrate the summarised ORA process and may help duty holders in the development of effective procedures.

3.2.1 When is ORA necessary and appropriate?

An ORA is required where it is intended to operate plant and equipment outside its normal operating (design) envelope, or with protective or monitoring devices, controls or other safeguards not functioning as designed. This includes any changes to organisational capability that may compromise the safe operation of the installation.

The most common trigger for ORA is the identification of non-functioning (unavailable or degraded) safety-critical equipment impairing a safety-critical element. The identification of SCE impairment may result from any of the following circumstances:

- through observation during routine plant operations and maintenance activities;
- whilst conducting SCE assurance routines;
- during ICP witness testing; or
- an unplanned event that reveals SCE impairment;

An ORA is carried out in such circumstances, if the unavailability or degradation of the SCE increases the conditional probability of failure to prevent, detect, mitigate or control a major accident event or impedes evacuation, escape or rescue, or where the potential consequences of an event are increased by SCE impairment.

Duty holder procedures must give clear guidance to personnel on the appropriate application of ORA and should also reinforce that the Offshore Installation Manager is obliged and empowered to take immediate (i.e. pre-ORA) shutdown action where in his judgment he considers the increase in risk arising from SCE impairment to be intolerable.

In the circumstances where plant has been shut down, the ORA can assess the risk of re-starting the affected plant or equipment and support a decision to continue operations with a known, degraded SCE where the assessment outcome shows a tolerable level of safety can be achieved and maintained with mitigation measures in place.

3.2.2 Contingency planning for SCE impairment

Risk management strategies can be supported effectively by contingency planning to identify appropriate responses to SCE impairment. In relation to operational risk management; the adoption of relevant rule sets may aid installation personnel in making sound decisions in potentially testing situations. In terms of SCE impairment, installation based personnel have to respond to dynamic circumstances where the loss or degradation of the SCE may potentially reduce levels of safety on the installation. The immediate response action can be summarised as typically offering installation personnel two options, namely:

- to stop or limit operations to within the limits of remaining barriers; or
- identify and assess any temporary substituted safety system barrier(s) that may be implemented to support continued operation

The first option pursues a precautionary approach and allows the curtailment of an affected operation prior to a formal, structured operational risk assessment being performed. The latter approach would normally result from an ORA that had properly considered the degraded situation and identified and implemented suitable and sufficient actions to enable continued operation until the SCE is fully repaired or replaced.

Decisions to suspend or limit operations can be especially challenging for installation personnel so duty holders should consider the identification and adoption of rules to guide and support robust decision making. These are likely to take the form of discrete situations in which the OIM has a predetermined course of action to follow in the event of certain SCE failures, examples of such failures being:

- an ESDV or its associated control function;
- a pipeline SSIV or its associated control function;
- loss of a well barrier (DHSV);
- non-availability of a fire pump;
- non-availability of a TEMPSC;
- loss of TR integrity; or
- loss of HVAC in an enclosed hydrocarbon processing module

These are examples of reasonably foreseeable SCE failures for which the duty holder should develop and implement operational procedures (rules) to direct or guide OIM response actions. Duty holders should identify the full range of similarly foreseeable failure scenarios and set down rules to guide personnel tasked with managing those scenarios. The rules themselves should be derived and documented from a formal assessment of scenarios by suitably competent people in the duty holder's organisation.

Such contingency planning can co-exist with ORA and may be referred to within the duty holder's ORA procedure or SCE Performance Standard.

3.2.3 ORA methodology and key considerations

This section describes the practical application of the ORA process to help duty holders design and implement effective procedures and protocols, and to develop appropriate ORA methodologies. The descriptions are necessarily general and duty holders should develop detail in their company specific procedures. This sets out key elements of an effective operational risk assessment and provides guidance on key considerations to be made under each heading of the ORA process. This guidance should also aid the development of effective duty holder ORA training and competence arrangements.

The guidance does this by walking through the typical steps of ORA as described below.

(i) Initial Response Actions

On identification of SCE impairment, the OIM should apply the rule sets developed by the duty holder and consult with the relevant Technical Authorities or other support personnel where required to guide initial response actions.

An especially challenging aspect in determining the appropriate initial response – particularly where not all support resources are available – is the assessment of combined risk where the identified SCE impairment may be compounded by other known deficiencies or ORAs in place on the installation. In particular the OIM needs to know if the SCE impairment impacts other ORAs where credit has already been taken for the SCE that is now impaired. The OIM also needs to know what work is taking place on the installation that may exacerbate the abnormal situation. Duty holders should consider developing rules on these aspects to aid decision making and initial response actions. It is suggested that this might take the form of information distilled from the installation Safety Case provided as a check-list to support the initial qualitative assessment of increased risk.

Such information might include:

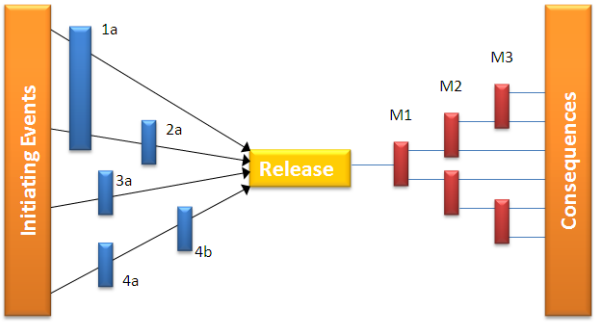
- A list of representative major accident hazard scenarios;
- Summary of main plant isolatable hydrocarbon inventories;
- Predicted hydrocarbon leak frequencies from these inventories or other associated leak frequencies;
- Significant escalation pathways;
- Probability or relative likelihood of escalation for each main inventory; and
- Relative impact / significance of various barriers against immediate or escalated risks

Further check list questions might include:

- What is the impaired system for?
- Under what circumstances would the system be required to work?

- If these circumstances occur, what will be the effects of the impairment?
- What can we do to reduce the potential for these circumstances to occur?
- What measures can we put in place to replace the functionality lost due to impairment?
- How effective are these measures likely to be under the circumstances in which they are most needed?
- Together, are all of these measures sufficient to manage risk effectively, and for how long?

The identification of remaining control measures as part of this initial assessment can be supported by reference to existing hazard management tools such as bow-tie diagrams as illustrated at Figure 2 below.



Prevention / control barrier examples:
- Plant layout
- Construction standards
- Inspection
- Instrument

Mitigation barriers examples:
- Detection system
- ESD
- Active protection
- Passive protection
- EER

Figure 2: Example of a bow-tie diagram (Source: HSE Guidance Sheet 3/2006: Guidance on Risk Assessment for Offshore Installations)

If there is insufficient confidence in answers to the above questions, a precautionary approach should be taken (e.g. affected activities or operations suspended or shut down) until further detailed assessment can be carried out. There is a minimum expectation that clear reasons will exist to support a decision to continue operations and to proceed to ORA rather than to suspend or shut down affected activities or operations.

(ii) Preparation and readiness for conduct of ORA

Having taken any necessary initial response action and identified the need for ORA; an ORA team should be nominated ensuring appropriate levels of competence in relation to the specific risk being assessed. The ORA team make-up will vary according to the initially assessed nature and scale of the issue. Early consideration should be given to the involvement of onshore personnel mentioned

previously (Technical Authorities; SCE Responsible Engineers; Technical Safety Engineers; 3rd party specialists etc. as appropriate).

The person leading the ORA should ensure that involved personnel are fully familiar with the process as the relative infrequency of ORA may mean that participants need a short refresher on the process.

It is critical to stress to all ORA participants that ORA is not simply a mechanism by which continued operation can be justified under any circumstances. Whilst guidance provided by the application of rule sets may not have immediately directed installation personnel to shut down or limit operations, this may still be the eventual outcome of the ORA process. **It is also particularly important to stress to ORA participants that they are undertaking an ORA and not a Task Risk Assessment so they need a major accident mindset rather than a personal injury mindset.**

Necessary supporting documents for the ORA should be assembled and participants familiarised with those documents. Examples of supporting documents may include:

- The ORA reporting and recording pro-forma
- Safety case
- SCE Performance Standard(s)
- Standard operating procedures
- Plant layout diagrams
- P&ID's
- Cause & Effect charts
- Bow-tie or similar hazard analysis outputs as available
- Details of other ORAs in place
- Details of SCE maintenance backlog
- Details of outstanding Written Scheme of Verification inspection and assurance activities
- Relevant LOPA / SIL assessments

The following sub-sections outline practical aspects of the conduct of ORA and highlight some key risk management considerations under each heading. To aid clarity, the descriptions will focus on considerations relating to SCE impairment but these can be taken to apply to other abnormal operations that may be subject to ORA. Duty holder procedures and related pro-forma should provide guidance to involved personnel in relation to the ORA aspects set out in the below sub-sections. In particular however, ORA specific training should ensure that relevant personnel understand the detailed process and its application, and are therefore able to carry out a robust assessment.

(iii) Description of SCE failure and hazard identification

The assessment should provide a clear and sufficiently detailed description of the impaired SCE giving rise to the ORA. Reference should be made to the affected

Performance Standard and describe the nature and extent of SCE degradation. The description should state what plant and equipment is affected by the ORA; what major accident hazard(s) the SCE relates to, and / or the failure gives rise to; and what barrier(s) is /are affected by the failure. Significant effort should be applied to hazard identification at this stage as this provides the basis for all pursuant aspects of the ORA and flawed hazard identification will result in an ineffective ORA output.

This information should be sufficiently detailed to allow onshore personnel to fully understand the nature and extent of the failure or abnormal situation. The team should also justify and document the decision to continue operating with the failed SCE pending the ORA where that is the case (i.e. the ORA is not assessing a situation where equipment has already been shut down in order to determine whether it is safe to re-start). Again, careful consideration must be given to combined hazards resulting from other known defects or other ORAs in place on the installation.

(iv) Risk Evaluation

Having identified relevant major accident hazard(s) associating with the failed SCE; the team should evaluate risks that may stem from the identified major accident hazard. Essentially the ORA is comparing the risk of operating with SCE in a degraded condition against normal operating risk. The evaluation process therefore considers four key factors, namely:

- **Consequence**

The initial stage of risk evaluation should consider the potential consequences associating with the SCE failure. The assessment should identify and list all reasonably foreseeable major accident hazard scenarios linked to that SCE and describe how these are affected by the failure.

This assessment considers the pre-mitigation condition (i.e. the consequences that may result if no additional mitigation is put in place to compensate for the impaired SCE) and should identify the reasonably foreseeable outcome for each identified hazard. The ORA team should have information from the safety case and SCE Performance Standards to support this aspect of the assessment, but they should be especially mindful of any wider impacts of the SCE failure and the combined effect of other ORA already in place on the installation.

A simple example of consequence assessment might be that if the failed SCE is a fire pump then deluge capacity may be reduced leading to an increased risk of serious injuries or fatalities resulting from fire or explosion. Consequence assessment should also consider event escalation potential that may result from a failed SCE. It should be stressed that in ORA, the clear emphasis should be on a determination of the potential consequences of the abnormal situation.

- **Likelihood**

The second aspect of risk evaluation involves an assessment of the likelihood of the identified consequences of the SCE failure being realised. Again this determination relates to the SCE failure without any mitigation measures being in place. In most ORA circumstances this will be a qualitative or semi-quantitative

assessment and the duty holder's procedures should provide clear guidance on likelihood criteria specific to major accident hazards. The assessment of likelihood is most relevant where the impaired SCE is preventive; e.g. ignition prevention. **It should be emphasised that a determination of Low likelihood cannot be used to support continued operations without effective mitigation measures being in place.**

- **Risk estimation**

The properly executed assessment of consequence and likelihood described above enables the assessment team to arrive at a risk estimate which may in qualitative terms assign risks as High, Medium or Low. Duty holders should already have risk criteria for major accident risks and it is essential that the consequence and likelihood criteria are relevant to major accident assessment rather than task related personal injury outcomes. Some duty holders assign numerical values to consequence and likelihood and to their risk ranking matrices to adopt a semi-quantitative approach to risk evaluation, but even these approaches typically result in an extended range of High, Medium and Low risk classifications.

Risk ranking is used to:

- drive the requirement to shut down or limit activities or operations;
- drive the identification and implementation of appropriate mitigation measures;
- ensure appropriate levels of review, endorsement and approval of the ORA;
- identify and prioritise remedial or recovery actions (i.e. SCE time to repair); and
- specify time lines for review, revalidation and/or closure of the ORA

- **Impact on other SCE**

In considering the risks arising from SCE failure, assessors need to be mindful of any interrelationship or dependencies between SCE. These interrelationships and dependencies should be shown in the SCE Performance Standard, so reference should be made to that as a starting point. A simple example is that a failure of gas detection could affect alarm systems, ventilation trips and ESD initiation.

(v) Identification of mitigation measures

Having estimated the risk associated with the degraded SCE, the team should systematically identify and consider control measures designed to mitigate such risk. In making this determination the team should consider the recognised hierarchy of controls and adopt the highest reasonably practicable standard of control. In relation to SCE failure, this hierarchy can be illustrated in descending order as follows:

- hazard elimination by shutting down the affected plant or equipment;
- providing an engineering solution to replace or supplement the degraded SCE;

- implementing procedural controls such as prohibiting certain work activities or tasks in an affected area (e.g. stopping hot work); and
- human intervention in the form of Operator monitoring of a normally automated control function for example

The ORA team should consider **all** available controls and record why any higher standards of control were discounted in deriving mitigation measures. Strict adherence to the hierarchy should be observed and in particular, reliance on human intervention should always be the last resort. **(Note that failure rates associating with reliance on human intervention are typically higher than those for automated process and hence these measures require particular consideration).** The number and range of procedural and human intervention controls required to compensate for SCE subject to ORA should be considered and assurance provided that this is manageable in both steady state and exceptional conditions. This aspect is crucial to successful operational risk management and the team should answer some specific questions along the following lines:

- should the plant or process be shut down?
- is an engineered solution necessary and possible to reduce risk?
- have all available risk reduction measures been identified and properly considered?
- where human intervention has been identified as a mitigation; is there sufficient capacity and no risk of overload to installation personnel?
- is human intervention practical in the event of an emergency?

In establishing that sufficient effective barriers remain in place to justify continued operation, reference should be made to existing documentation such as bow-tie diagrams or similar hazard management tools.

Finally, checks must be made to provide assurance that identified mitigation measures are available and reliable. This may require an SCE assurance routine to be brought forward to gain or increase confidence in the availability and reliability of that SCE in its additional mitigation role.

(vi) Assessment of residual risk & risk determination

The ORA team should make an assessment of residual risk taking account of the risk reduction effect of identified mitigation measures. This should involve each of the identified hazards in the ORA being revisited and risks re-evaluated taking credit for identified mitigation measures. This step should assign new qualitative or semi-quantitative values (high, medium or low) and allow the team to arrive at a determination as to the acceptability of continued safe operation in the impaired state. The duty holder procedure should provide direction as to the tolerable levels of residual risk to enable the ORA team to make a recommendation on shutdown or continued safe operation as appropriate. It should also be emphasised that a lowering of residual risk below that assessed as the original risk level does not necessarily mean that a proposal is acceptable. The focus on consequences referred to at (iv) above should prompt serious consideration of the residual risk level and drive efforts to further reduce risk.

(vii) ORA, ALARP and risk tolerability

The installation safety case includes a demonstration that control of major accident risks complies with the relevant statutory provisions and to a level that is as low as reasonably practicable (ALARP). That compliance and the ALARP demonstration will have taken credit for existing SCE in their fully functional condition. It follows therefore that an impaired SCE condition will temporarily result in a level of risk that is higher than the ALARP level defined in the safety case. The properly executed ORA will arrive at a position where all reasonably practicable risk reduction measures have been implemented, allowing the ORA team to determine if the residual risk is tolerable or intolerable and to make a suitably informed judgment to continue operations or to shut down on that basis. Figure 3 illustrates that concept of applying mitigation to achieve a tolerable level of risk, or alternatively identifying that the risk is intolerable and hence the equipment or operation should be shut down. Note that the Figure 3 graphic shows an exaggerated fluctuation in risk level for illustrative effect only and is not intended to be truly representative.

It should be noted that this is also the initial coarse assessment of tolerability that the OIM has to make in deciding whether an ORA is an appropriate immediate response to SCE impairment rather than a full or partial shutdown to manage increased risk.

Crucial to the ORA approach is the need for strong and continued focus on remedial actions so that the period of reliance on mitigation controls is minimised and appropriate effort and resources are applied to effective restoration of the impaired SCE.

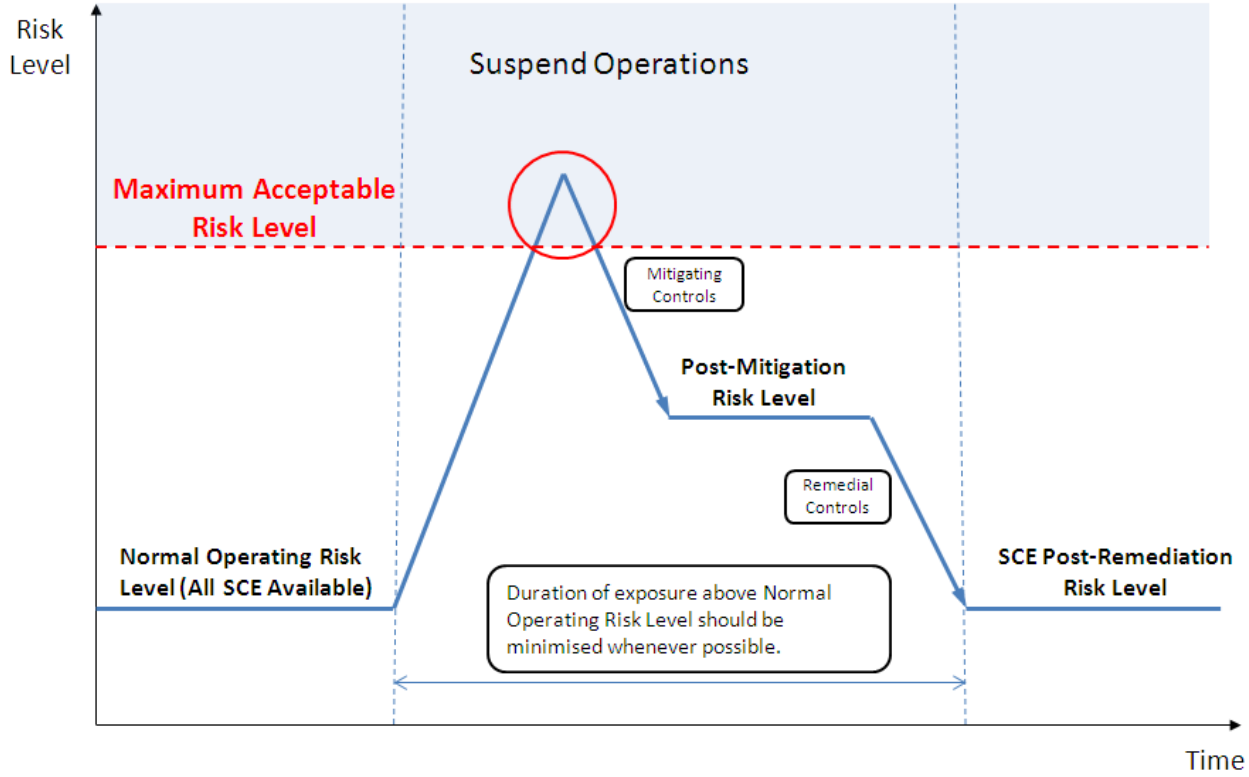


Figure 3. Risk tolerability judgement

(viii) Combined Risk

The ORA team should have an overview of the combined effect of risks arising from SCE failure. The OIM and the ORA team must be aware of other ORA in place on the installation. Other defects such as integrity issues (e.g. temporary repairs), deferred PM or CM routines on SCE and a specific summary of ORA where human controls are in place should also be noted. The team should ensure that the combined effect of SCE impairment remains tolerable and mitigation measures remain manageable. This aspect of the assessment should also particularly consider other demands that may already be placed on SCE affected by the ORA. The assessment should also consider the level of installation activity and the nature and effect of simultaneous operations.

Duty holders should put in place measures to record and ensure visibility of current ORA, degraded SCE and temporary mitigation measures. These measures should enable an offshore and onshore management overview of all ORA in place and the combined effect on major accident hazard management on installations at any given time. The overview may provide information by SCE / barrier; by installation module or process system; or some other common grouping mechanism. It is for duty holders to develop and implement appropriate and effective means of collecting, communicating and reviewing information on ORA status and for the effect of live ORA on the installation risk profile.

(ix) Review, Endorsement and Approval

Clear routes and levels of authority for the review, endorsement and approval of documented operational risk assessments must be specified and adhered to. Levels of authority should reflect and align with levels of assessed risk or relative safety-criticality of the impaired SCE.

(x) Validity Periods

Procedures should define acceptable periods for ORA to remain in force and should cause the ORA review team to specify a validity period during which the impairment situation **must** be rectified. These arrangements should be linked to revised levels of risk, and should ensure timely restoration of the SCE functionality and original level of major accident risk. Renewing ORA and adjusting SCE restoration dates ("re-setting the clock") should be discouraged.

(xi) Recording & Communication of ORA

Procedures should specify the means of recording outputs of the ORA and typically pro forma will be used for that purpose. Although not essential to the process; the use of electronic control of work systems may provide a mechanism for recording and disseminating ORA documentation. It is crucial that relevant personnel are made aware of operational risk assessments and associated changes to SCE. Personnel such as Process Operators, Control Room Operators and Emergency Response Team members should be made aware of changes and any new or additional actions that may be required of them as part of ORA mitigation measures.

These arrangements must pay particular attention to, and specify how visibility is maintained over the life cycle of the ORA, across crew / shift changes for example.

3.2.4 Use of QRA in operational risk assessment

Duty holder ORA procedures should make reference to, and the ORA team consider making use of, the installation quantified risk assessment (QRA) when progressing through the steps described in the preceding section of this guidance. QRA is a powerful tool providing a more formal means of assessing the relationships between initiating events, affected systems and event outcomes, and can be used to support judgments as to the tolerability of residual risk. QRA may be particularly useful for complex risk management situations, or where engineering judgment and more qualitative assessment may not offer enough certainty in relation to risk tolerability. The sensitivity of QRA to relatively small changes that may associate with SCE impairment may be a limiting factor in its use as an ORA tool.

3.3 Monitoring, audit and review

3.3.1 Monitoring

Active monitoring should address key aspects of the ORA process as follows:

- the monitoring of specific risk mitigation measures implemented in response to SCE failure(s) as part of an operational risk assessment. Regular checks should be made to assure the ongoing integrity of such measures in light of installation activity so that acceptable levels of risk are maintained;
- monitoring of combined effects of ORA. Typically this relates to arrangements designed to give visibility to ORA and to allow installation and onshore management to ensure that levels of cumulative risk resulting from multiple ORAs remain tolerable;
- regular monitoring of the ORA process to ensure a) that the process is being applied to appropriate operational situations, and b) that the process is being implemented effectively in line with duty holder procedures;
- assurance that impairment situations are being resolved effectively (e.g. degraded SCE are repaired or replaced within the ORA validity period and time scales are not extended); and
- identification and monitoring of the potential effect on ORA of changes to installation activity sets, and approved engineering or organisational changes.

Duty holders should also implement a mechanism for tracking the number of ORA in place over time on an installation. While the number alone may not translate directly to an overall increase in risk; it may prove useful as an indicator of plant condition and SCE management. Management attention and effort should focus on minimising the number of active ORAs in place at any time.

Reactive monitoring should ensure that any incidents arising from, or associated with the ORA process are investigated thoroughly; causes identified; corrective and preventive measures implemented; and any learning is incorporated into the ORA procedure and properly communicated to affected parties.

3.3.2 Audit

ORA processes should be subject to audit as part of the duty holder HSE Management System assurance regime. The audit should examine the ORA procedure, its implementation and continued adherence to documented measures, to provide reasonable assurance that the procedure and its implementation remains robust. Audit should assess compliance with the procedure and give confidence that the system itself is effective in managing major accident risks in relation to SCE failure or other relevant abnormal situations.

3.3.3 Review

Duty holder HSE Management System review processes should ensure that the ORA process is reviewed as an integral feature of major accident hazard management. This review should provide assurance to duty holder senior management that major accident hazards are well managed and that in particular, operational risk management processes are applied appropriately and effectively. Such review should allow and require senior managers to form a view on the criticality of ORA and potential impacts on major accident hazard management.

The duty holder ORA procedure should also be reviewed periodically and updated as necessary to reflect legislative change, any learning from application of the procedure or incidents associating with the procedure.

4. Appendix

4.1 Example of an ORA RACI chart

Table 2. Example ORA RACI Chart

Phase	ORA Management Process Steps	OIM	Offshore Supervisor	Offshore Technicians	Asset/ Ops Manager	Technical Authority	Technical Safety	SCE Responsible Engineer	ICP/ Third party specialist	Notes
Initiation	Identification of degraded/unavailable SCE or abnormal operating situation	A	R	R	I	R	R	R		Responsibility for identification of scenarios where ORA may be necessary and appropriate lies with all personnel.
	Identify initial response actions	A	C	C	I	C	C	C		Apply pre-defined rule sets. Make initial assessment of cumulative effects of other degraded SCEs or abnormal operations.
	Immediate intervention required?	A R			I					Accountability and responsibility lies with OIM.
	Yes – suspend or limit operations	A	R	I	I	I	I	I		
	No – initiate ORA process	A				A		A		OIM or relevant onshore personnel may call for ORA
	Identify ORA team	A	C			C	C	C		
Execution	Perform ORA as per procedure	A	R	C		C	C	R		Joint responsibility of offshore supervision, technical safety and onshore engineering functions. Responsibility for conduct of ORA will typically lie with assigned ORA team leader
	Describe SCE failure/ abnormal situation	A	R	C		C	C	C		Description must be clear and unambiguous
	Identify hazards related to failure/abnormal situation	A	R	C		C	R	C		Careful consideration must be taken of the combined risk arising where the identified SCE impairment is compounded by other deficiencies or ORAs in place on the installation.
	Evaluate risk (assessing consequences and likelihood)	A	R	C		C	R	C		Consideration should be given to the use of QRA through the remaining steps in this stage of the ORA process.
	Identify mitigating measures	A	R	C		C	R	C		Consideration must be given to ensuring identified mitigation measures are available and reliable, and that combined requirements (if other ORAs are in place) can be managed.
	Assess & determine residual risk	A	R	C		C	R			
	Risk tolerable?	A	R	C		C	R			
	No - suspend or limit operations	A	R	C	I					
	Yes – document ORA output	A	R	C			C	C		ORA must associate with a clear plan and timetable for remediation.
Review & Approval	Review & endorsement	A	R	C	C	R	C	C	I	
	Approval?	A	I	I	I	R	I	I		
	No - suspend or limit operations	A	R	I	I	I	I	I		
	Yes – issue and communicate ORA	A	R	I	I	I	I	I		Ensure that all personnel involved in or affected by mitigation measures are made aware.
Monitor, Audit & Review	Monitor specific risk mitigation measures	A	R	C		C		C		
	Monitor cumulative effects	A	R	C		C	C	C		Of changes in plant/operational status, combined risk of other SCE issues/abnormal situations etc.
	Monitor visibility of ORA and mitigating measures over time	A	C	C		C	C	C		Particular attention must be paid to crew/ shift change.
	Monitor progress of remediation measures	C	C		A	C		R		Formal review process required to track and where necessary expedite progress.
	Close out ORA	A	R	I		I		I		
	Lifecycle audit	A	R	R	I	C	I	R		ORA process must be subject to audit as part of duty holder HSE Management system assurance process.

R	Responsible	The party who does the work to achieve the task. Delegated to by those who are *Accountable*.
A	Accountable	The party ultimately answerable for the correct and thorough completion of the task. *Accountability* and *Responsibility* may lie with the same party, and so no responsible party may be shown for some steps.
C	Consulted	Those whose opinions are sought, and with whom there is two-way communication.
I	Informed	Those who are kept informed and updated on progress.

4.2 Example of ORA process flow as used by one duty holder

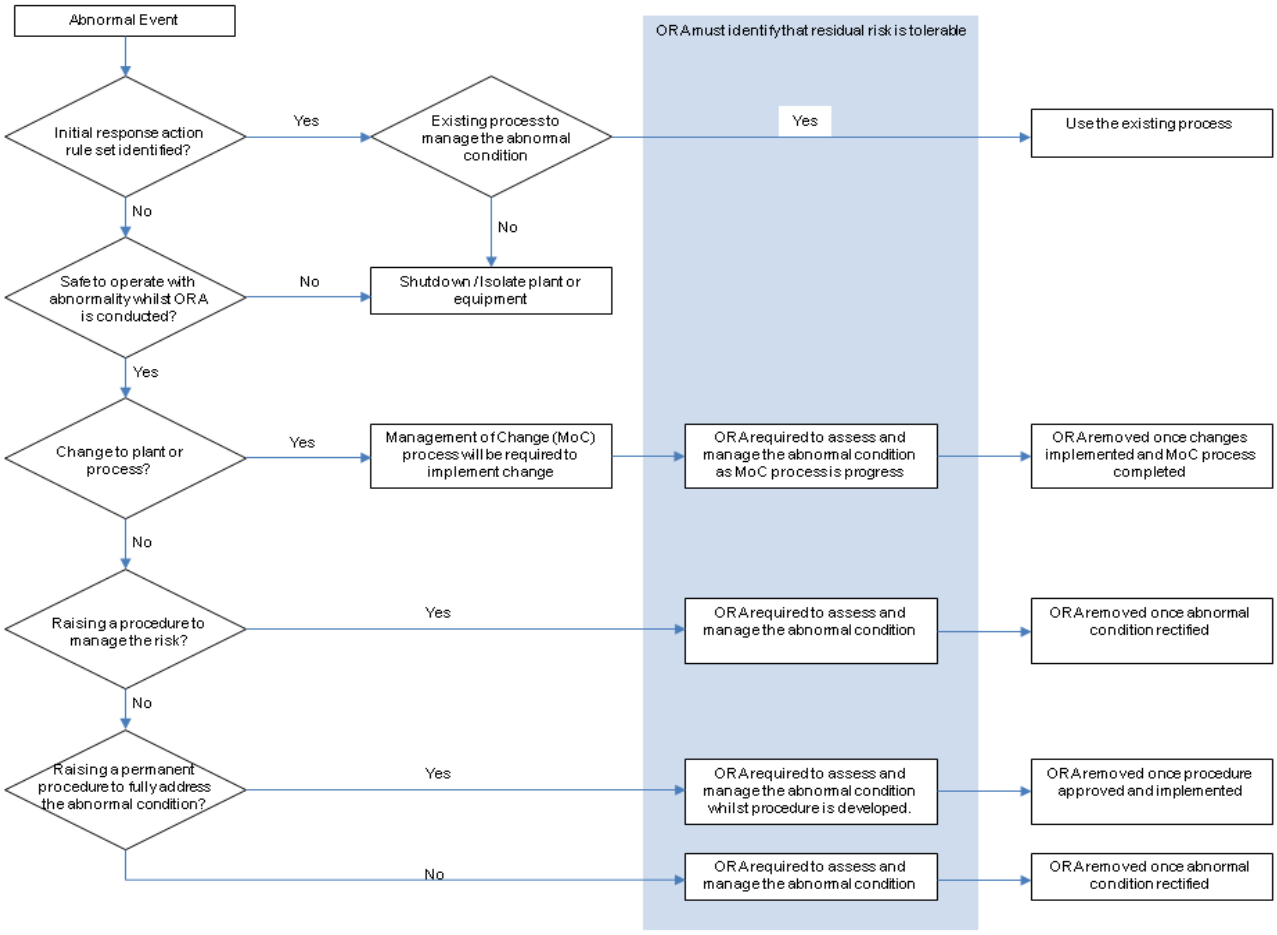


Figure 4: Example ORA process flow

Oil & Gas UK

the voice of the offshore industry