Operational risk assessment

Core concepts

- A facility safety case identifies the control measures necessary to ensure that the risk of major accident events (MAEs) are reduced to as low as reasonably practicable (ALARP).
- The safety case must also specify the performance standards that are used to specify the required performance of systems or items of equipment that are used as a basis for managing the risk of MAEs.
- The operator of a facility has a regulatory obligation to operate their facility within the bounds of the accepted safety case.
- Operating with impaired Safety-Critical Equipment (SCE) and without adequate additional controls may be considered as operating contrary to the safety case 'in force' for a facility.
- Operators should consider stopping activities where controls do not meet requirements specified in the performance standards.
- Operators should have an Operational Risk Assessment (ORA) system in place to assess the risks posed by impaired SCE performance and identify and implement additional temporary controls to cover a period until full functionality of the SCE is restored.
- Some types of SCE impairment can be reasonably anticipated at the design stage or during operations in advance of the impairment occurring. An ORA process can be used for contingency planning to identify appropriate responses to SCE impairment.
- Early implementation of an ORA process for contingency planning is likely to lead to more considered assessments and better safety outcomes, compared with an ORA conducted at the time when SCE impairment has already occurred and where there is likely to be time, resource and production pressures.
- Additional controls identified as part of contingency planning must be reassessed at the time of implementation to consider cumulative risk associated with impairment of more than one SCE.
- An ORA should not be used as a means to justify an operator's intent to continue production.
- Depending on the additional controls identified, the time required, and the change in risk profile until the SCE is restored to full functionality, a revised safety case may be required.
- Including SCE failure contingencies within the facility safety case provides for continued operations during SCE impairment, and therefore will reduce the burden on the operator to revise and resubmit the safety case for NOPSEMA's assessment.
- The facility operator should develop and maintain detailed procedures to ensure that operational risk assessments systematically identify hazards, assess risks and identify additional controls associated with impaired SCE performance to ensure risks are maintained to ALARP.

Table of Contents

Abbreviations and acronyms

ALARP	As low as reasonably practicable
MAE	Major accident event
NOPSEMA	National Offshore Petroleum Safety and Environmental Management Authority
OIM	Offshore Installation Manager
OPGGSA	*Offshore Petroleum and Greenhouse Gas Storage Act 2006*
OPGGS(S) Regs	Offshore Petroleum and Greenhouse Gas Storage (Safety) Regulations 2009
ORA	Operational risk assessment
PIC	Person in charge
SCE	Safety-critical equipment

Key definitions for this guidance note

The following are some useful definitions for terms used in this guidance note. Unless prescriptively defined in the Offshore Petroleum and Greenhouse Gas Storage (Safety) Regulations 2009 (OPGGS(S) Regs [as indicated by the square brackets]) they are a suggested starting point only.

ALARP	*This term refers to reducing risk to a level that is as low as reasonably practicable. In practice, this means that the operator has to show through reasoned and supported arguments that there are no other practicable options that could reasonably be adopted to reduce risks further.*
Control measure	*A control measure is any system, procedure, process, device or other means of eliminating, preventing, reducing or mitigating the risk of hazardous events at or near a facility. Control measures are the means by which risk to health and safety from events is eliminated or minimised. Controls can take many forms, including physical equipment, process control systems, management processes, procedures, emergency response plans, and personnel.*
Formal safety assessment	*A formal safety assessment is an assessment or series of assessments that identifies all hazards having the potential to cause an MAE. It is a detailed and systematic assessment of the risk associated with each of those hazards, including the likelihood and consequences of each potential MAE. It identifies the technical and other control measures that are necessary to reduce that risk to a level that is ALARP [OPGGS(S) Regulation 2.5(2)(c)].*
Hazard	*A hazard is defined as a situation with the potential for causing harm.*
Hazard identification	*Hazard identification is the process of identifying all hazards having the potential to cause an MAE [OPGGS(S) Regulation 2.5(2)(a)], and the continual and systematic identification of hazards to health and safety of persons at or near the facility [OPGGS(S) Regulation 2.5(3)(c)].*
Major accident event	*A major accident event (MAE) is an event connected with a facility, including a natural event, having the potential to cause multiple fatalities of persons at or near the facility [OPGGS(S) Regulation 1.5].*
Performance standard	*A performance standard means a standard, established by the operator, of the performance required of a system, item of equipment, person or procedure which is used as a basis for managing (controlling) the risk of a MAE [OPGGS(S) Regulation 1.5].*
Risk assessment	*Risk assessment is the process of estimating the likelihood of an occurrence of specific consequences (undesirable events) of a given severity.*
Safety-critical equipment	*A technical control measure, the failure of which could cause or contribute to a major accident event (i.e. piece of equipment, control system or protection device including hardware as well as safety-critical computer software for the prevention or mitigation of a major accident event).*
Operational risk assessment	*An aspect of an operator's safety management system dealing with temporary changes to procedures or technical controls to cover a short period of time where safety-critical equipment cannot meet the requirements specified in their performance standard(s).*

1. Introduction

1.1. Intent and purpose of this guidance note

The effective management of MAEs is an integral requirement of safe operations on offshore oil and gas facilities. Robust arrangements must be in place to identify and evaluate MAEs, and to specify control measures required to ensure that MAE risks are reduced to a level that is ALARP. A demonstration that MAEs have been identified and that MAE risks are reduced to ALARP must be adequately documented in the facility safety case.

MAE control measures are identified in the safety case as 'technical' or 'other' control measures. Technical controls are typically identified as SCEs, and other controls are usually administrative controls such as procedures and management systems (e.g. permit to work). The required performance of SCEs to meet the intent of the control are specified in Performance Standards and the performance standards are listed in the safety case.

Further guidance is available in the NOPSEMA guidance note:
"Control Measures and Performance Standards"

A facility operator's procedures for risk management need to be comprehensive such that they accommodate and account for adverse changes in SCE performance, or other abnormal situations that may potentially increase levels of MAE risk. For the purposes of this guidance note, the term operational risk assessment (ORA) is used in a generic sense; the guidance applies equally to other forms of operational risk management (e.g. permitted operations process) typically undertaken by facility operators.

There are many cases where the failure of a SCE can reasonably be foreseen (e.g. failure of an emergency shutdown valve). Considering these potential SCE failures prior to experiencing a failure in the field can help with contingency planning by identifying additional controls that may be required and allowing time for these to be developed before they are needed. NOPSEMA recommends that operators describe these contingencies within their facility safety case, however this is not mandatory.

However, it should be noted that waiting for an SCE failure to occur before conducting an ORA may require a shutdown until the risk has been assessed and any identified controls can be developed and implemented, and may also require the operator to submit a revised safety case to NOPSEMA for assessment. It should also be noted that where operators' change management has been found to be deficient either in terms of process or implementation, NOPSEMA has pursued various forms of enforcement action (e.g. Prohibition Notices, Improvement Notices, Directions and/or requests for a revision of the facility safety case) to ensure the change in risk is adequately addressed by the facility operator.

This guidance note has been prepared to help facility operators develop, implement and maintain robust ORA procedures to manage MAEs where impairment of SCE (including SCE that is damaged, failed or degraded to the extent that it no longer meets its performance standard) or some other abnormal operational situation may potentially compromise safety and/or increase MAE risk.

This guidance is particularly targeted at personnel within the facility operator's organisation 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

- monitor, audit or review operational risk management arrangements.

1.2. Objectives

The objectives of the guidance note are to help facility operators develop, maintain and implement ORA procedures that achieve a systematic and effective approach to operational risk management processes such that:

- a thorough assessment of MAEs associated with SCE impairment or other abnormal operational situations is carried out, hazards are appropriately identified, and risks are appropriately assessed
- effective control (prevention 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 identified by the ORA are adequate, available and fully functional, or being managed under a separate ORA
- operational risk management processes are managed and executed by suitably technically competent personnel, including review, endorsement and approval of the assessment and documented outputs
- 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 consistent and systematic 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 within an appropriate time scale
- consideration of SCE impairment is conducted as a part of contingency planning to allow alternative controls to be developed
- consideration is given to including SCE failure contingencies, where these are reasonably predictable, within the facility safety case. Note: this is not mandatory, however may prevent an operator having to shut down their facility in case of certain SCE impairment.

1.3. Application

This guidance applies primarily to the ORA relating to impaired SCE. 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 a facility). The guidance adopts a good practice approach that retains some flexibility in terms of its application to a facility operator's operations and alignment with existing management systems and ORA procedures.

2. Systematic approach to development and implementation of ORA procedures

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 when SCE are impaired. This includes any changes to organisational capability that may compromise the safe operation of the facility. The most common trigger for ORA is the identification of impaired SCE. The identification of SCE impairment may result from a range of circumstances including:

- through observation during routine plant operations and maintenance activities
- while conducting SCE assurance routines
- during independent competent person witness testing
- an unplanned event that reveals SCE impairment.

An ORA is carried out in circumstances where the impairment of the SCE impacts on the equipment's ability to meet its safety function. That is, where impairment increases the probability of failure to prevent, detect, mitigate or control a major accident event, or impedes evacuation, escape or rescue, or increases the potential consequences of an event.

The facility operator's procedures should give clear guidance to personnel on the appropriate application of ORA, and should also reinforce that the Offshore Installation Manager (OIM) or Person in Charge (PIC) is obliged and empowered to take immediate (i.e. pre-ORA) shutdown action where, in the OIM's/PIC's judgment, the increase in risk arising from SCE impairment is not adequately provided for in the facility safety case.

In the circumstances where plant has been shut down, the ORA can assess the risk of re-starting and support a decision to continue operations with a known, impaired SCE where the assessment outcome shows that mitigations can be implemented to reduce risks to ALARP.

*Refer to NOPSEMA's Guidance Note N-04300-GN0166 **"ALARP"** for further discussion on risk management within an ALARP regime.*

2.1.1. Contingency planning for SCE impairment

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

- stop or limit operations to within the limits of remaining SCE
- identify and assess any temporary substituted procedural or technical control measures 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 ORA being performed. The latter approach would normally result from an ORA that had properly considered the impaired SCE situation and identified and implemented suitable and sufficient actions to enable continued operation until the SCE is fully repaired or replaced.

Operational risk assessment should not be utilised for long-term or permanent SCE impairment; as this would typically be considered a modification triggering a safety case revision in accordance with Regulation 2.30 of the OPGGS(S) Regs.

Decisions to suspend or limit operations can be especially challenging for facility personnel so facility operators should consider the identification and adoption of rule sets 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 impairment. Examples of such impairment include:

- failure of an emergency shutdown valve or its associated control function
- failure of a pipeline subsea isolation valve or its associated control function
- loss of a well barrier
- non-availability of a fire water pump
- non-availability of a lifeboat or fast rescue craft
- loss of temporary refuge integrity
- loss of heating, ventilation and air conditioning (HVAC) in relation to enclosures where there is a potential for hydrocarbon ingress.

These are examples of reasonably foreseeable SCE impairment for which the facility operator should develop and implement operational procedures (rules) to direct or guide the OIM/PIC in relation to response actions. It is recommended that operators of facilities include consideration of these types of SCE failures as part of the development of their facility safety cases, however this is not mandatory. Any consideration should include contingency measures which may be taken in the event of impaired SCE ranging from partial/complete shutdown of operations to other safeguards which may be put in place which may facilitate continued operations in the interim. Facility operators should identify the full range of similarly foreseeable impairment 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 involving suitably competent people in the facility operator's organisation. Such contingency planning can co-exist with ORA and may be referred to within the facility operator's ORA procedure or SCE performance standard.

Depending on the nature of the SCE impairment, e.g. failure on demand, failure triggering a requirement for the emergency response plan to be implemented, etc., there may be a requirement to notify, and provide a written report to, NOPSEMA in relation to a dangerous occurrence in accordance with clause 82 of Schedule 3 to the OPGGS Act.

2.2. Organisational factors

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

2.2.1. 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 organisation needs to be sized and staffed appropriately to allow for the involvement in the ORA process of all relevant personnel. The ORA procedure should, for example, make provision for the non-availability of specialist support personnel (e.g. technical authorities) out-of-hours, and describe how that absence will be managed by 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.

2.2.2. Roles and 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.

The particular importance of the role of technical authorities and SCE responsible engineers (or equivalent position titles) in the ORA process should be stressed in the facility operator's procedures.

The procedure should clearly identify the various roles of personnel in the management and conduct of ORA; one possible approach is along the lines of that shown in **Table 1**. The facility operator's procedures should detail levels of involvement in the process in line with the risk being assessed.

This roles and responsibilities tabular approach may be supplemented or replaced by a RACI (responsible, accountable, consulted, informed) chart. This should 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 or PIC.

Table 1 – Typical roles and responsibilities of personnel involved in ORA

	I	L	P	R	E	A
OIM	X			X	X	X
Offshore supervisors		X	X			
Offshore technicians			X			
Technical safety		X	X	X	X	
Technical authorities	X	X	X	X	X	
SCE responsible engineers	X	X	X	X	X	
Asset / operations management				X	X	X
Third party specialists			X	X		
General members of the offshore workforce	X		X			
I = Initiate, **L**= Lead ORA, **P** = Participate, **R** = Review, **E** = Endorse, **A** = Approve						

2.2.3. Training and 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 MAE hazards calls for specific training in order to achieve an effective approach to ORA. Facility operators 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 including:

- a thorough understanding of MAE hazards specific to the facility, SCEs, and SCE verification and performance standards
- awareness and understanding of key information documented in the facility 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 site-specific emergency response plans and procedures
- facilitation and communication skills to enable full and active participation by team members
- awareness of suitability and limitations of ORA process.

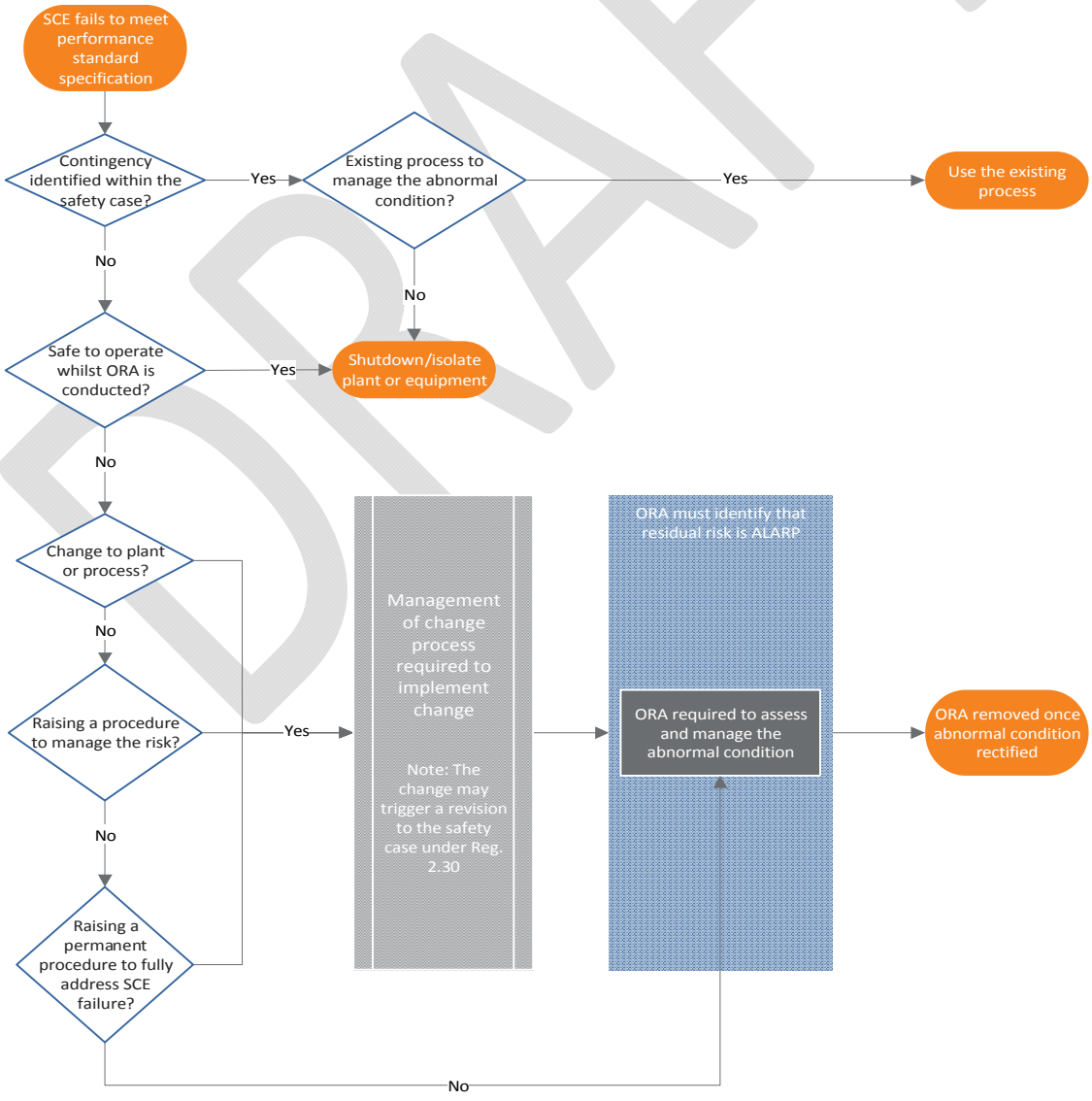
2.3. Planning and implementation

This section describes the ORA process in terms of:

- identification of circumstances in which ORA is necessary and appropriate
- a 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
- ongoing management until permanent remediation is achieved.

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 facility operators. Figure *1* illustrates the summarised ORA process and may help facility operators in the development of effective procedures.

Figure 1 – Example of ORA process flow



Refer to NOPSEMA Guidance Note N-03000-GN0099 ***"Notification and Reporting of Accidents and Dangerous Occurrences"***

2.3.1. ORA methodology and key considerations

This section describes the practical application of the ORA process to help facility operators design and implement effective procedures and protocols, and to develop appropriate ORA methodologies. The descriptions are necessarily general and facility operators should develop detail in their company-specific procedures. This sets out key elements of an effective ORA and provides guidance on key considerations for each stage of the ORA process. This guidance should also aid the development of effective facility operator ORA training and competency arrangements.

The typical steps of ORA are described below.

(i) Initial response actions

On identification of SCE impairment, the OIM should apply the rule sets developed by the facility operator (recommended to be included in the facility safety case) 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 facility. In particular, the OIM needs to know if the SCE impairment impacts other ORAs that are reliant on the SCE that is now impaired. The OIM also needs to know what work is taking place on the facility that may exacerbate the abnormal situation. Facility operators should consider developing rules to aid decision-making and initial response actions. This might take the form of information distilled from the facility safety case provided as a check-list to support the initial qualitative assessment of increased risk.

Such information might include:

- a list of representative MAE hazards
- 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
- relative impact / significance of various barriers against immediate or escalated risks.

Further check-list questions might include:

- What is the impaired system used for?
- What are the circumstances under which the system would 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 bowtie diagrams.

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, and be thoroughly documented, 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 established, 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, third party specialists, etc. as appropriate). The ORA team should also include members of the offshore workforce who need to be aware of the risks and hazards that they may be exposed to from the impaired SCE and any contingencies/mitigations proposed.

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

ORA participants should understand that ORA is not a mechanism by which to justify a predetermined decision to continue operation. While guidance provided by the application of rule sets may not have immediately directed facility personnel to shut down or limit operations, this may still be the eventual outcome of the ORA process.

It is particularly important to stress to those ORA participants who may be more familiar with conducting job hazard assessments, that they are undertaking an ORA and that a major accident event mindset is required.

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
- the safety case
- SCE performance standard(s)
- standard operating procedures
- plant layout diagrams
- piping and instrumentation diagrams
- cause and 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 inspection and assurance activities
- relevant layers of protection analyses or safety integrity level assessments.

The following sub-sections outline practical aspects of the conduct of ORA and highlight some key risk management considerations. 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. Facility operator procedures and related pro-forma should provide guidance to involved personnel in relation to the ORA aspects set out below. In particular, 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(s) 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 event(s) the SCE helps prevent or mitigate and/or the failure gives rise to, and the barrier(s) affected by the failure.

Significant effort should be applied to hazard identification at this stage as this provides the basis for all subsequent aspects of the ORA. Flawed hazard identification will result in an ineffective ORA output.

The description should be sufficiently detailed to allow onshore technical support personnel and other personnel that have input into risk-based decision making 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. Again, careful consideration must be given to cumulative risk resulting from other known defects or other ORAs in place on the facility.

(iv) Risk evaluation

Having identified relevant MAE hazard(s) associating with the impaired SCE, the team should evaluate risks that may stem from the identified MAE. Essentially, the ORA compares the risk of operating with impaired SCE against normal operating risk. The evaluation process therefore considers the four key factors below.

Consequence

The initial stage of risk evaluation should consider the potential consequences associated with the impaired SCE. The assessment should identify and list all reasonably foreseeable major accident event scenarios linked to that SCE and describe how these may be affected by the impairment.

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 impairment and the combined effect of other ORA already in place on the facility.

A simple example of consequence assessment might be that if the impaired SCE is a fire water 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 an impaired SCE. 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 impairment being realised. Again this determination relates to the SCE impairment without any mitigation measures being in place. In most ORA circumstances this will be a qualitative or semi-quantitative assessment. Procedures should provide clear guidance on likelihood criteria specific to MAEs. The assessment of likelihood is most relevant where the impaired SCE is preventive (e.g. ignition prevention).

A determination of 'low' likelihood cannot be used to support continued operations without effective mitigation measures being in place, as the entire major accident event regulatory regime is based around low likelihood, high consequence events.

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.

Facility operators should already have risk criteria for MAE risks and it is essential that the consequence and likelihood criteria are relevant to MAE assessment rather than task related personal injury outcomes. Some facility operators 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 for a number of purposes, including:

- driving the requirement to shut down or limit activities or operations
- driving the identification and implementation of appropriate mitigation measures
- ensuring appropriate levels of review, endorsement and approval of the ORA
- identifying and prioritising remedial or recovery actions (i.e. SCE time to repair)
- specifying time lines for review, revalidation and/or closure of the ORA.

Impact on other SCE

In considering the risks arising from SCE impairment, 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 impaired gas detection could affect alarm systems, ventilation trips and emergency shut-down initiation.

(v) Identification of mitigation measures

Having estimated the risk associated with the impaired 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 impairment, 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 impaired SCE
- implementing procedural controls such as prohibiting certain work activities or tasks in an affected area (for example, stopping hot work and/or stopping work involving breaking into hydrocarbon containment systems)
- human intervention (e.g. operator monitoring of a normally automated control function).

The ORA team should consider all available controls and record why any higher standards of control were discounted in deciding 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 associated 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 impairment 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 ORA 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 facility personnel?
- What systems are in place to support and document the human intervention?
- Is human intervention practical in the event of an emergency?

In establishing that sufficient effective control measures 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 and 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 facility operator's procedure should provide direction as to the acceptable 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 acceptability

The facility safety case includes a demonstration that control of MAE risk complies with the relevant statutory provisions and to a level that is 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 acceptable or unacceptable and to make a suitably informed judgment to continue operations or to shut down on that basis.

Inclusion of contingencies within the safety case

Consideration should be given to including contingencies and mitigation measures to be implemented on impairment of SCE within the safety case where such impairment of SCEs is reasonably predictable. For example, loss or degradation of a fire water pump may lead to restrictions in the operational activities that can be safety undertaken at the facility until full functionality and performance of the fire water pump can be restored.

Safety case revision triggers

The following safety case revision triggers are noted from OPGGS(S) Regs:

- 2.30(1)(b)

  "the operator proposes to modify or decommission the facility, and the proposed modification or decommissioning is not adequately addressed in the safety case"
- 2.30(1)(c)

  "*there are reasonable grounds for believing that a series of proposed modifications to the facility would result in a significant cumulative change in the overall level of risk of major accident event*"
- 2.30(2)(a)

  "*a significant increase in the level of risk to the health or safety of persons at or near the facility*"
- 2.30(2)(b)

  "*a series of increases in the level of risk to the health or safety of persons at or near the facility that, in total, are significant*"

In the context of this guidance note, NOPSEMA defines significant cumulative change as follows:

"*In relation to overall level of risk of major accident events, means a change in the level of risk that is likely to change the basis on which the safety case was accepted.*"

The definitions indicate that a revised safety case is required in any circumstances where the operator does not intend to restore the SCE to meet the performance standard requirements within a reasonable (relatively short) period of time.

Note: A change or removal of a control measure that is likely to change the basis on which the safety case was accepted is also likely to trigger a safety case revision.

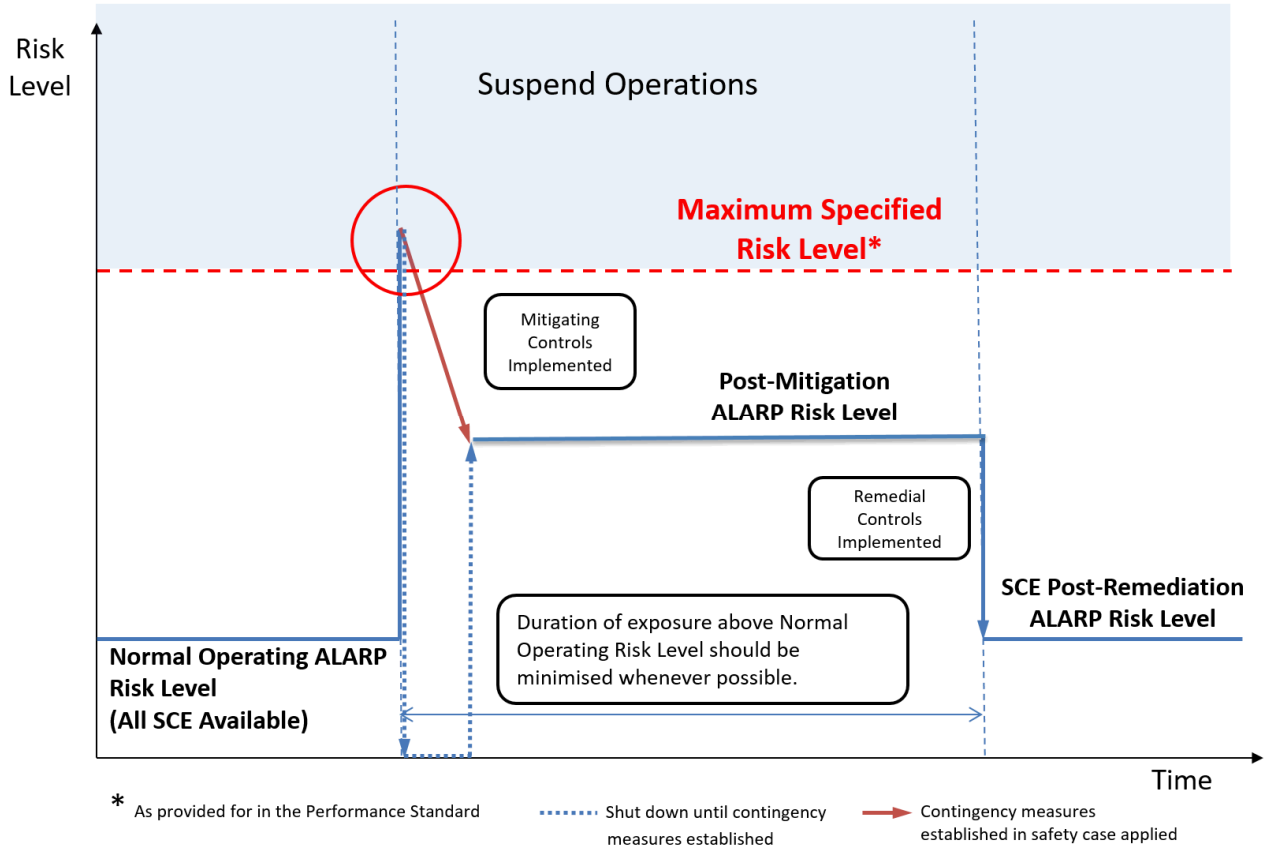
*Refer to the NOPSEMA Guidance Note N-4300-GN0087 **"Safety Case Lifecycle Management"***

Figure 2 illustrates the concept of applying mitigation to achieve a risk that is ALARP, or alternatively identifying that the risk mitigations cannot be implemented and hence the equipment or operation should be shut down. Note that Figure 2 shows an exaggerated fluctuation in risk level for illustrative effect and may not be representative.

It should be noted that this is also the initial coarse assessment of risk level 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 2 – Risk level not provided for by the performance standard



(viii) Combined risk

The ORA team should have an overview of the combined effect of risks arising from SCE failure. The OIM/PIC and the ORA team must be aware of other ORAs in place on the facility. Other defects such as integrity issues (e.g. temporary repairs), deferred preventative maintenance or corrective maintenance 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 risk impact of SCE impairment remains ALARP and mitigation measures remain

manageable. In particular, this aspect of the assessment should consider other demands that may already be placed on SCE affected by the ORA. In addition, the assessment should consider the level of facility activity and the nature and effect of simultaneous operations.

Facility operators 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 MAE hazard management on facilities at any given time. The overview may provide information by SCE/barrier, by facility module or process system, or some other common grouping mechanism. It is for facility operators to develop and implement appropriate and effective means of collecting, communicating and reviewing information on ORA status, and to understand the effect of live ORA on the facility risk profile.

(ix) Review, endorsement and approval

Clear routes and levels of authority for the review, endorsement and approval of documented ORA 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 period

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 MAE risk. Renewing ORA and adjusting SCE restoration dates ("re-setting the clock") is generally is not considered to be acceptable practice or ALARP.

(xi) Recording and 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 members of the workforce exposed to the risk, and or personnel making risk-based decisions are made aware of ORA 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, for example across crew/shift changes.

2.4. Monitoring, audit and review

2.4.1. Monitoring

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

- Monitoring specific risk mitigation measures implemented in response to SCE impairment(s) as part of an operational risk assessment. Regular checks should be made to ensure the ongoing integrity of such measures in light of facility activity so that ALARP levels of risk are maintained.
- Monitoring combined effects of ORA. Typically this relates to arrangements designed to give visibility to ORA so that facility and onshore management can ensure that levels of cumulative risk resulting from multiple ORAs remain ALARP. Regular monitoring of the ORA process to ensure that:
  - the process is being applied to appropriate operational situations
  - the process is being implemented effectively in line with the facility operator's 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).
- Identification and monitoring of the potential effect on ORA of changes to facility activities, and approved engineering or organisational changes.

Facility operators should implement a mechanism for tracking the number of ORAs in place over time on a facility. 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.

2.4.2. Audit

ORA processes should be subject to audit as part of the facility operator's safety 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 event risks in relation to SCE impairment or other relevant abnormal situations.

2.4.3. Review

The facility operator's safety management system review processes should ensure that the ORA process is reviewed as an integral feature of MAE hazard management. This review should provide assurance to the facility operator's senior management that MAE 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 MAE hazard management.

The facility operator's ORA procedure should be reviewed periodically and updated as necessary to reflect legislative change and any learning from application of the procedure or incidents associated with the procedure.

3. Operational risk in a broader change management framework

All changes at a facility are required to be appropriately managed. This is to ensure that the change does not introduce a new hazard or increase the risk from an existing hazard. The change may also provide an opportunity to reconsider the controls in place and re-evaluate if the change facilitates modified controls or additional controls which were not practicable before. Change can come in many forms and may consist of one or more of the following:

- temporary change
- permanent change
- technical change
- organisational change
- procedural change
- administrative change
- hardware change
- software change
- maintenance change
- construction change.

Operating companies typically have a number of systems to manage change depending on the type of change, for example:

- document control
- technical change management
- ORA
- stand-alone risk assessment
- job safety assessment.

The term operational risk is used in this document to refer to aspects of an operator's safety management system dealing with temporary changes to procedures or technical controls to cover a period where SCEs are impaired (cannot meet the requirements specified in their performance standards). Operational risk may therefore be identified as a separate management system or may be included as part of a technical change system typically referred to in industry as 'management of change'. Examples of other titles applied to operational risk assessment include case to operate, deviation control risk assessment, and safety-critical element impairment risk assessment.

4. References and acknowledgements

4.1. Legislation references

- *Offshore Petroleum and Greenhouse Gas Storage Act 2006*
- Offshore Petroleum and Greenhouse Gas Storage (Safety) Regulations 2009

4.2. Acknowledgement

In January 2012, the United Kingdom Offshore Oil and Gas Industry Association Limited (Oil & Gas UK) published "Guidance on the conduct and management of operational risk assessment for UKCS offshore oil and gas operators", ISBN 1 903 003 77 5. The objective of the guideline was 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 abnormal operational situation may potentially compromise safety and increase major accident risk levels.*"

The National Offshore Petroleum Safety and Environmental Management Authority (NOPSEMA) has reviewed the guideline and concluded that the contents of the guidelines are applicable to oil and gas operations within Australian waters. NOPSEMA has received permission from Oil & Gas UK to utilise these guidelines including amendments, where necessary, to reflect the requirements of the Offshore Petroleum and Greenhouse Gas Storage Act 2006 (OPGGSA).

5. Appendices

5.1. Stakeholder Consultation

NOPSEMA has received a number of comments in relation to the draft guidance published on NOPSEMA website in March 2019. NOPSEMA has analysed these comments and categorised these into general categories. These general categories of comment and NOPSEMA's response are included in Table *2* . Refer to NOPSEMA's website for the detailed industry comments.

Table 2 - NOPSEMA responses to stakeholder comment

General Comment	NOPSEMA Response
The workshop identified a number of tangential issues, e.g. Performance Standards and Accidents and Dangerous Occurrences that were not discussed. It is believed that these issues have an impact on ORA.	The topics of Performance Standards, Damage to Safety-Critical Equipment and Operational Risk Assessment are inter-related. NOPSEMA will consider drafting/revising discussion papers and guidance on Performance Standards and Damage to Safety-Critical Equipment in in the 2019/2020 planning cycle. These drafts will be published on NOPSEMA's website and industry will be engaged to seek feedback. As part of the engagement process NOPSEMA will consider holding future workshops on these topics.
Industry has expressed an interest in conducting additional ORA workshops to discuss/explore the description of ORA within the safety case and the inclusion of contingency measures.	Consideration will be given to conducting additional workshops, with increased industry participation, to review case study examples of ORA systems and explore the level of detail that could reasonably be included within a safety case. The priority however is likely to be given to conducting workshops on Performance Standards and Damage to Safety-Critical Equipment.
Concerns have been raised regarding the description of SCE impairment contingencies within the safety case. The overall size and complexity of the safety case could increase representing an administrative burden on the operator.	There is no regulatory requirement to include contingencies within a safety case and therefore inclusion of contingencies within the safety case is not mandatory. The recommendation to consider inclusion of contingencies is intended to avoid situations (that have occurred in the past) where there may be a requirement for an operator to submit a revised safety case on the basis that the contingency measures proposed by the operator were not adequately described in the safety case. This guidance is consistent with the Control Measures and Performance Standards Guidance Note which was published in December 2012. Inclusion of contingencies would reduce the cost and resource burden on the operator for the development of a safety case revision at short notice. It is not the intent that every contingency is included (e.g. a failed smoke or gas detector). The examples provided in section 2.2.2 are examples where a

General Comment	NOPSEMA Response
	failure of the equipment to meet the performance standard increases the likelihood of escalation or increases the potential consequences of an incident. It is anticipated that inclusion of contingencies could be described in a number of paragraphs or a tabulated matrix rather than adding pages to the safety case.