



Purpose

This discussion paper extends ideas already presented in existing NOPSEMA guidance documentation and proposes to provide further clarity with respect to the notification and reporting of damage to safety-critical equipment.

This paper seeks facility operator comment on the concepts presented.

Issues and opportunities

Consistent notification of damage to safety-critical equipment (DSCE) amongst operators enables comparative analysis and the identification of trends that may be predictive of changes in safety with respect to specific operators' facilities or to the industry as a whole. There is also a need to minimise unnecessary regulatory burden on the offshore petroleum industry by reducing the requirement for notifications that do not provide predictive or analytical value with respect to occupational health and safety (OHS) or major accident event risk. This discussion paper intends to address both these issues by providing a definition of DSCE and guidance as to its interpretation.

Contents

Purpose.....	1
Issues and opportunities	1
1. Introduction.....	2
2. Acronyms.....	2
3. Glossary of terms.....	3
4. Definition of "Damage to safety critical equipment"	3
5. Operator guidance for "Damage to safety-critical equipment" under sub-regulation 2.41(2)	4
6. Common failure scenarios and performance standards	5
6.1. Failure of spare or redundant equipment.....	5
6.2. Detection of safety-critical equipment failure during periodic testing.....	6
6.3. Failure of fire and gas detectors.....	8

1. Introduction

Sub-regulation 2.41(2) Item 8 of the Offshore Petroleum and Greenhouse Gas Storage (Safety) Regulations 2009 (OPGGS (Safety) Regulations) describes **Damage to safety-critical equipment** as a dangerous occurrence, and clause 82(1) of Schedule 3 to the *Offshore Petroleum and Greenhouse Gas Storage Act 2006* requires that operators give NOPSEMA notice of a dangerous occurrence. The Act and its regulations do not define “damage to safety-critical equipment”. Evidence from facility inspections and notifications of dangerous occurrences indicates that operators do not share a common definition of DSCE and hence do not notify NOPSEMA of damage to safety-critical equipment consistently.

Consistent notification of damage to safety-critical equipment (DSCE) amongst the operators enables comparative analysis and the identification of trends. These trends may be predictive of changes in safety with respect to specific operators’ facilities or to the industry as a whole; however there is also a need to minimise unnecessary regulatory burden on the offshore industry, by reducing the requirement for notifications that do not provide predictive or analytical value. This discussion paper addresses both these issues by providing a definition of DSCE and guidance as to its interpretation.

The guidance provided in this discussion paper links the definition of DSCE to the performance standards required under sub-regulation 2.5(3) of the OPGGS Regulations. This shifts the focus of ensuring consistent notification from the definition of DSCE to the development of the performance standards. The NOPSEMA regime is goal based and not prescriptive and so the content of performance standards is not prescribed by NOPSEMA; however, there are common types of safety-critical equipment employed in the Australian offshore petroleum industry. NOPSEMA is therefore in the position to identify common shortcomings in the formulation of performance standards. Section 5 discusses a selection of common issues that have led to inconsistent notification of DSCE and attempts to provide guidance.

2. Acronyms

ALARP	As low as reasonably practicable
DSCE	Damage to safety-critical equipment
ESD	Emergency shutdown
MAE	Major accident event
MTBM	Mean time between maintenance
MTTF	Mean time to failure
MTTM	Mean time to maintain
MTTR	Mean time to repair
NOPSEMA	National Offshore Petroleum Safety Environment Management Authority
OPGGS	Offshore Petroleum and Greenhouse Gas Storage
PFD	Probability of failure on demand
RBI	Risk-based inspection
SIS	Safety instrumented systems

3. Glossary of terms

Term	Definition
<i>Dangerous detected failure/fault</i>	A failure of a device (or equipment) that the operator can automatically detect via diagnostic tests and output (e.g. alarms). The device has failed in such a way that if a dangerous condition were to occur (e.g. excessively high pressure), the condition would either not have been detected by the device (e.g. pressure transmitter) or the equipment (e.g. shutdown valve, firewater pumps) would not have responded to restore the facility to a safe condition.
<i>Dangerous undetected failure/fault</i>	A failure of a device (or equipment) that the operator is <u>not</u> able to detect without periodic testing. The device has failed in such a way that if a dangerous condition were to occur (e.g. excessively high pressure), the condition would either not have been detected by the device (e.g. pressure transmitter) or the equipment (e.g. shutdown valve, firewater pumps) would not have responded to restore the facility to a safe condition. The failure remains undetected until the next proof test.
<i>Safe detected failure/fault</i>	A safe failure of a device that the operator can detect by diagnostic tests. The device fails in such a way that does not prevent the detection or correct response to a dangerous condition. E.g. a pressure transmitter reads high, leading to an early detection of a dangerous condition, or a valve fails closed to put the process in a safe condition, even though the dangerous condition did not exist. The diagnostics associated with the device has detected the failure, so that the operator can repair it within a reasonable time frame.
<i>Safe undetected failure/fault</i>	A safe failure of a device that the operator cannot detect by diagnostic tests. The device fails in such a way that does not prevent the detection, or correct response, to a dangerous condition. The failure remains undetected until the next proof test.

4. Definition of “damage to safety critical equipment”

Sub-regulation 2.5(1)(b) of the OPGGS (Safety) Regulations requires that the **technical and other control measures**, identified as a result of the formal safety assessment, be described in the safety case. Table 1 lists typical categories of control measures.

Table 1 - Types of control measures

	Types of control measure	Examples of control measures
i)	Equipment (including computer programmes) that prevents, or mitigates the effect of, a major accident event (MAE).	Firefighting systems, instrumented protective system.
ii)	Systems or procedures that assure the integrity of equipment, the failure of which could cause or contribute to a MAE.	Inspection, maintenance and repair (associated equipment could include pressure vessels, pressure piping, cranes).
iii)	Systems or procedures that prevent, or mitigate the effect of, a MAE.	Operating procedures, emergency response plan.

iv)	Systems or procedures that if implemented incorrectly, could lead to a MAE.	Confined space entry procedures.
-----	---	----------------------------------

Safety-critical equipment refers to the physical parts of the facility associated with the control measures described in i) and ii) of Table 1. Therefore safety-critical equipment can be defined as:

“Safety-critical equipment means such parts of a facility and such of its plant (including computer programmes), or any part of those—

- a) the failure of which could cause or contribute to a major accident; or*
- b) a purpose of which is to prevent, or limit the effect of, a major accident.”*

(adapted from the UK Offshore Installations (Safety Case) Regulations 2005)

Therefore “damage” in the context of “damage to safety-critical equipment” can be described as an impairment which leads to a failure as described in part a), or to an inability to prevent or limit the effect of a major accident as described in b).

5. Operator guidance for “Damage to safety-critical equipment” under sub-regulation 2.41(2)

Sub-regulation 2.5(3) requires that “The safety case for the facility must also contain a detailed description of the safety management system that: (i) specifies the **performance standards** that apply”. Performance standards are defined in regulation 1.5 as “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 the risk of a major accident event”. N-04300-GN0271 (section 5) states that “The performance standards are the parameters against which MAE controls are assessed to ensure they reduce risk to ALARP”.

It is through regulations 2.5(3) and 1.5, and guidance note N-04300-GN0271 that we establish that performance standards describe the criteria that safety-critical equipment must meet to ensure that they reduce the risk of an MAE to ALARP. It therefore follows that damage to safety-critical equipment would be an event that prevents it from meeting the performance criteria defined in the performance standards. Guidance note N-03000-GN0099 provides the following example of a dangerous occurrence which is useful as generic guidance for “damage to safety-critical equipment”:

“An acute or chronic occurrence resulting in the inability of a control measure (identified as being necessary to reduce the risk of one or more MAEs to ALARP) to meet its performance standards”.

Therefore an operator only needs to consider whether the damage to safety-critical equipment prevents it from meeting its performance standard to determine whether the event is notifiable to NOPSEMA, under regulation 2.41(2), item 8.

Recommendation one

Update section 6 (assurance of control measures) of guidance note N-04300-GN0271 to include the following guidance for “damage to safety-critical equipment”:

“An acute or chronic occurrence resulting in the inability of a control measure (identified as being necessary to reduce the risk of one or more MAEs to ALARP) to meet its performance standards.”

6. Common failure scenarios and performance standards

The guidance given in section 3 depends heavily on the performance standards prepared by the operators. For notifications of damage to safety-critical equipment (DSCE) to be meaningful, and to be able to identify industry and operator trends, there needs to be some measure of consistency in the general content of performance standards across operators. NOPSEMA therefore provides the following guidance on performance standards for specific issues where there is evidence of inconsistent or incorrect reporting, including:

- Failure of spare or redundant equipment;
- Detection of safety-critical equipment failure during periodic testing; and
- Failure of fire and gas detectors.

6.1. Failure of spare or redundant equipment

Whether the failure of spare or redundant safety-critical equipment is DSCE, and therefore notifiable, may not be immediately obvious. To demonstrate the point, it is useful to consider the common example of fire water pumps which are typically installed with redundancy, whereby one out of two, or two out of three pumps can meet the maximum design load case. At face value it would appear that a loss of one pump in either of these configurations should not constitute a failure to meet the performance standard; however redundancy or sparing in this situation is typically required to ensure system reliability, so that the probability of the system being able to perform its safety function on demand is sufficient.

When one pump from a spared fire water pump arrangement fails, the overall probability that the fire water pumps can meet the total design load, on demand, has reduced. This is because there is the possibility that one of the remaining pumps could also fail on demand. In reality, however, it must be accepted that pump failures do occur and that a failure does not necessarily represent a problem with the design or lack of maintenance, provided that the rate of failure is within expected limits.

Similarly, to ensure reliability, the operator must maintain the fire water pumps; therefore it follows that for the period that the pump being maintained is offline, the probability of failure on demand of the system has increased. As in the case of the failed pump, it must be accepted that pumps need to be maintained and provided the frequency and duration of that maintenance is within expected limits, this should not be considered a failure to meet the performance standard.

To assess whether an event should be considered a failure to meet the performance standard, the following must be considered:

1. The probability of failure on demand (PFD) or mean time to failure (MTTF) of each pump based on historical failure rate data;
2. The mean time to repair (MTTR) a pump in the event of failure;
3. The mean time between maintenance (MTBM); and
4. The mean time to maintain (MTTM).

In the case of maintenance, provided the MTTM and the MTBM is within accepted industry norms, pump maintenance should not be outside the performance standard and would not be notifiable to NOPSEMA as DSCE.

In the case of a pump failure, MTTF and MTTR can be defined in the performance standard, meaning that a failure wouldn't always need to be notified to NOPSEMA; however because the actual MTTF, compared to the performance standard MTTF, depends on the historical rate of failure at the facility, each failure would need to be analysed in the context of historical failures to determine if it is outside the MTTF defined in the performance standard. NOPSEMA inspectors have rarely observed that operators complete this at the time of the incident, but it is sometimes assessed on a periodic basis to determine if testing frequency is sufficient. For this reason, **all failures of spare or redundant safety-critical equipment should be reported to NOPSEMA as DSCE**, even if the actual MTTF and MTTR is within accepted industry norms.

NOPSEMA inspectors should verify that the operator has been monitoring safety-critical equipment reliability over extended time periods, to ensure the equipment reliability is adequate to reduce risks at the facility to ALARP.

Recommendation two

Update section 5.1.12 (five year revisions) of guidance note N-04300-GN0106 (safety case content) to provide guidance on the need for operators to monitor failure rates for safety-critical equipment and to ensure that the associated risks at the facility continue to be ALARP.

Recommendation three

Update section 5.1.4 (reliability) of guidance note N-04300-GN0271 to provide specific guidance on how operators should treat spared or redundant equipment from a performance standard perspective.

6.2. Detection of safety-critical equipment failure during periodic testing

Safety-critical equipment that is required to function on demand in the event of a hazard (e.g. fire) must be proof tested on a periodic basis to ensure that its reliability is sufficient to reduce to risk to ALARP. The goal of the test is to reveal faults that have been undetected since the last test, and which may have prevented the equipment from performing its safety function. This type of fault is a dangerous undetected fault. The frequency of the proof test depends on the historical reliability of the equipment and the level of risk reduction that is required (e.g. should successfully prevent the MAE 9 times out of 10, or say 99 times out of 100). Examples of equipment which operators test periodically to reveal dangerous undetected faults, include:

- Safety instrumented system (SIS) devices (e.g. sensors, emergency shutdown valves);
- Fire water pumps; and
- Fire dampers.

Dangerous undetected faults revealed during proof testing is damage to safety-critical equipment, as defined in section 3. However, NOPSEMA experience is that operators are frequently not reporting such faults as a dangerous occurrence, under regulation 2.41(2).



A common example is emergency shutdown (ESD) valves which the operator will lubricate, stroke and put back in service, following a failed proof test, without notification to NOPSEMA.

Failures detected during periodic testing will represent an unacceptable risk if the historical failure rate is higher, or the mean time to repair is greater, than the operator has planned for in demonstrating that the risk has been reduced ALARP. To account for this possibility, the operators should be able to demonstrate that they have monitored the rates of failure, the time to repair, and made adjustments to their inspection and maintenance programme if required. This is becoming increasingly relevant as there is an increasing trend of operators who are moving towards risk-based inspection (RBI) approaches for assurance of technical integrity without having first established a baseline reference.

Given that dangerous undetected failures, revealed only during periodic testing, do not necessarily represent an unacceptable increase in risk, should NOPSEMA insist that operators report all dangerous occurrences discovered during routine testing, under sub-regulation 2.41(2) to the Act?

The problem lies in the fact that personnel at the facility are required to report the dangerous occurrence as soon as practicable after the first occurrence, or detection, of the event (regulation 2.42 to the OPGGS (Safety) Regulations). To restrict the notification requirement to only those events which represent an unacceptable increase in risk, would require engineering analysis on a per-event basis, for the operator to be able to demonstrate to NOPSEMA that the rate of failure is within (or outside) planned expectations described in the safety case. This would be an unreasonable burden on the operators. Typically such analysis is completed periodically (e.g. annually) not on a per-event basis. Therefore **operators should notify NOPSEMA of all damage that prevents safety-critical equipment from meeting its performance standard, including damage detected during periodic testing.**

Table 2 – Examples of dangerous undetected failures (revealed during periodic testing)

Fault Type	Example
Dangerous undetected (<i>must be notified to NOPSEMA</i>)	<ul style="list-style-type: none"> • A firewater pump fails to start during a weekly “no-flow” test • A fire damper fails to close during a monthly proof test • An ESD valve fails to close during a 12 monthly proof test, does not close in the required time, or does not meet the leak rate requirement, defined in the safety requirement specification • The engine in a totally enclosed motor propelled safety craft (TEMPSC) fails to start during a 12 monthly test.

Recommendation four

Update section 6 of guidance note N-04300-GN0271 and N-03000-GN0099 to clarify that operators must notify NOPSEMA, under regulation 2.41(2), of dangerous and undetected damage to safety-critical equipment, detected during routine testing.

6.3. Failure of fire and gas detectors

There is a perception within NOPSEMA and industry that there are too many notifications of failures of fire and gas detectors under the category of DCSE and that these notifications are not valuable. However, the majority of notifications to NOPSEMA relating to fire and gas detection come under category “Unplanned event – implement emergency response plan” as the spurious trip of a fire and gas detection system typically initiates a general alarm and a muster.

There are relatively few genuine incidents of damage to fire and gas detectors that are damage to safety-critical equipment under the definition provided in section 3. The majority of events reported to NOPSEMA in relation to the failure of fire and gas detectors are safe failures. There are four types of failure that a fire or gas detector can experience, these are:

- safe detected*;
- safe undetected*;
- dangerous detected*; and
- dangerous undetected*.

*See glossary of terms section 2 for a description.

Safe detected and undetected failures are not damage to safety-critical equipment, under the definition, and do not need to be notified to NOPSEMA as damage to safety-critical equipment.

An example of a safe failure is a calibration error that resulted in the device detecting fire or gas earlier or quicker than necessary to be safe. The failure may be inconvenient for the operator as it may cause an unnecessary general alarm and muster, but it is not unsafe. Safe failures of fire and gas detectors typically represent ~ 80% of all failures (i.e. dangerous and safe).

Dangerous detected failures are the type of failure that the operator detects instantly due to diagnostics; however the failure has rendered the device unable to perform its function as safety-critical equipment.



An example of a dangerous detected failure is a gas detector that is under reporting the actual flammable gas concentration (i.e. reading low), but the internal diagnostics of the device has detected the fault and is reporting this back to the control system as a fault. The operator can detect this type of failure quickly, and the operator can implement the repair soon after detection and, provided the repair is completed within a reasonable time, the increase in risk is lower than for a dangerous undetected fault.

An operator can only discover a dangerous undetected failure during periodic testing or in the case of a genuine demand (e.g. fire or gas leak). It is therefore possible that a device could have failed for a period up to the testing frequency (e.g. 12 months) during which the device would have failed to act on demand. Failures of this type are expected, and the average rate of failure determines the testing frequency so that the overall probability of failure on demand (PFD) is within acceptable limits. However, the operator needs to be able to demonstrate that the actual rate of failure on the facility is in line with the expected rate of failure and any safety integrity level (SIL) verifications that the operator may have performed.

In section 5.1 the case was made that operators should notify NOPSEMA of all dangerous failures of spare or redundant equipment; however fire and gas detectors typically operate in a network to provide coverage over an area. The requirement to report a dangerous detected or undetected fault of a fire or gas detector, depends on the fault tolerance of the system. The operator can describe the fault tolerance in the performance standard, so that the determination of whether there is damage to the network of detectors, such that the network cannot meet its performance standard, depends on the tolerance to faults, while still meeting the required probability of failure on demand (PFD) for the system as a whole.

The determination of whether the operator should notify NOPSEMA of damage to safety-critical equipment for dangerous detected or undetected faults, therefore depends on the actual fault tolerance of the system, and whether the operator has accurately described this in the performance standard.

The operator should therefore notify NOPSEMA of damage to safety-critical equipment for all occurrences of dangerous detected or undetected faults of devices within the fire and gas system, unless the operator can:

- a. **demonstrate that there is a level of redundancy in the system, such that the failure of the device has not significantly reduced the overall reliability of system; and**
- b. **show that this is adequately described in the performance standard.**

The performance standard needs to provide sufficient detail to describe the level of redundancy and clarify the zones that it applies, where relevant. **The operator needs to report any exceedance of the redundancy, defined in the performance standard, as damage to safety-critical equipment.**

Recommendation five

Update guidance note N-04300-GN0271 and N-03000-GN0099 to clarify that the operator does not need to notify NOPSEMA of DSCE, for dangerous failures to fire and gas detectors, unless the failure exceeds the device redundancy described in the performance standard.