NOPSEMA
Australia's offshore energy regulator

GUIDANCE NOTE

Damage to Safety-Critical Equipment

Document No: N-09000-GN1914 A729008

Date: 01/05/2020

1. Introduction

Clause 82(1) of Schedule 3 to the *Offshore Petroleum and Greenhouse Gas Storage Act 2006* (OPGGSA) requires that operators give NOPSEMA notice of a dangerous occurrence. Regulation 2.41(2) Item 8 of the Offshore Petroleum and Greenhouse Gas Storage (Safety) Regulations 2009 (OPGGS(S)) describes 'Damage to safety-critical equipment' as a dangerous occurrence; however the regulations do not provide a definition of ***damage to safety-critical equipment***.

Therefore, the purpose of this guidance is to provide a definition of ***safety-critical equipment*** and ***damage to safety-critical equipment*** so that operators are able to notify NOPSEMA consistently, as required by the Act.

2. Determination of Damage to Safety-Critical Equipment

Safety-critical equipment means the physical parts of the facility associated with the technical and other control measures described in regulation 2.5(2)(c) of the OPGGS(S):

a) the failure of which could cause or contribute to a major accident event; or
b) the purpose of which is to prevent, or mitigate the effect of, a major accident event.

Damage to safety-critical equipment means an impairment of safety-critical equipment that could:

a) cause or contribute to a major accident event, or
b) limit its ability to prevent or mitigate a major accident event.

The performance standards[1] specified in the safety management system[2], provide the criteria to assess whether an impairment can lead to a) or b). Therefore, any impairment to ***safety-critical equipment*** that prevents it (or its associated system) from meeting its performance standard is ***damage to safety-critical equipment*** and therefore a ***dangerous occurrence***.

An operator must, in accordance with the Clause 82(1) of the OPGGSA and regulation 2.41(2) of the OPGGS(S), give notice of any damage to safety-critical equipment such that it (or its associated system) is unable to meet its performance standard.

[1] Performance Standards are defined in regulation 1.5
[2] The requirement for performance standards is described in regulation 2.5(3)(i)

Users of this guidance should note that performance standards can define the performance of a safety-critical 'system'. Damage to an item of safety-critical equipment (e.g. gas detector), may not necessarily prevent the system (e.g. fire and gas system) from meeting its performance standard.

- Refer to Appendix A for the relevant clauses and regulations of the OPGGSA and OPGGS(S).
- Refer to Appendix B for examples of ***damage to safety-critical equipment***.

Appendix A – Associated Legislative References

OPGGSA – Notifying and Reporting Accidents and Dangerous Occurrences

Cl. 82(1) *If, at or near a facility, there is:*

c) a dangerous occurrence;

*the operator must, in accordance with the regulations, give NOPSEMA notice of the accident or **dangerous occurrence**.*

OPGGS(S) – Regulations – Definition of Performance Standards

Reg 1.5 ***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 the risk of a major accident event.*

OPGGS(S) – Regulations – Control Measures

Reg 2.5(2) *The safety case for the facility must also contain a detailed description of the formal safety assessment for the facility, being an assessment, or series of assessments, conducted by the operator that:*

*i) identifies the technical and other **control measures** that are necessary to reduce that risk to a level that is as low as reasonably practicable.*

OPGGS(S) – Regulations – Performance Standards

Reg 2.5(3) *The safety case for the facility must also contain a detailed description of the safety management system that:*

j) specifies the performance standards that apply.

OPGGS(S) Regulations – Dangerous Occurrences

Reg 2.41(2) *For the definition of **dangerous occurrence** in clause 3 of Schedule 3 to the Act, an occurrence, at a facility, that is specified in the following table is a dangerous occurrence.*

*Item 8. **Damage to safety-critical equipment**.*

Appendix B – Examples of Damage to Safety-Critical Equipment

The examples listed in Table 1 are for illustrative purposes only. Actual designs, conditions and performance standards may vary from those described below.

Table 1 – Examples of Damage to Safety-Critical Equipment

Safety-Critical Equipment	Impairment	Performance Standard	Impairment Notifiable (OPGGSA Cl 82.1)	Clarifications and Exceptions (Defined in Performance Standard)
Fire Water Pumps	One (1) of two (2) x 100% Firewater pumps fails to start during a weekly test.	2 x 100% pumps must be available at all times to ensure the reliability of the Fire Water system. *Comment: The impairment means the performance standard cannot be met. The impairment should be reported to NOPSEMA.*	Yes	The unavailability of one (1) of two (2) x 100% pumps during planned maintenance (provided the maintenance is completed in reasonable time and in accordance with a recognised standard e.g. NFP 25) is not a breach of the Performance Standard, provided this clarification is described and justified in the performance standard. The performance standard must also describe the conditions of the exception, such as maximum allowable time to maintain.

Safety-Critical Equipment	Impairment	Performance Standard	Impairment Notifiable (OPGGSA Cl 82.1)	Clarifications and Exceptions (Defined in Performance Standard)
Process Shutdown Valve (SDV)	An SDV fails to close during a demand on the associated safety instrumented function (SIF) or during a proof test.	SDV is required to close on demand and within the process safety time, to ensure the process is maintained in a safe condition. The performance requirement for the SIF and SDV is specified in the Safety Requirement Specification – IEC 61511-1) *Comment: The impairment means the performance standard cannot be met. The impairment should be reported to NOPSEMA.*	Yes	This may not be a breach of the performance standard if the operator is able to demonstrate full compliance with IEC 61511, including the collection and analysis of reliability data, and demands on the system. The operator has proof tested the device at a frequency specified in the SRS and periodically reviewed the test frequency.
Blowdown Valve (BDV)	The blowdown valve failed to open on demand, or opened too slowly during an ESD event, such that the performance standard blowdown time could not be met (e.g. 690 kPag in 15 minutes).	The blowdown systems must be able to de-pressure vessels containing pressurised hydrocarbon to less than 690 kPag within a time specified in the Performance Standard. *Comment: The impairment means the performance standard cannot be met. The impairment should be reported to NOPSEMA.*	Yes	

Safety-Critical Equipment	Impairment	Performance Standard	Impairment Notifiable (OPGGSA Cl 82.1)	Clarifications and Exceptions (Defined in Performance Standard)
Gas Detectors	One (1) gas detector is discovered to have failed dangerously (Note 1) during periodic testing.	The performance standard allows for up to one 'dangerous failure' (Note 1) per fire zone because the system has been designed with redundancy, such that one failure does not reduce the reliability below design requirements. *Comment: The failure of one gas detector is allowed for by the performance standard. This does not need to be reported to NOPSEMA.*	No	The performance standard must clearly describe the redundancy that is designed into the system, such that a single failure does not reduce system reliability below acceptable levels. If there is no redundancy described, a single dangerous failure detected during testing is a breach of the performance standard and should be notified to NOPSEMA as a dangerous occurrence.
Note 1. A failure which impedes or disables a given safety action (IEC 61511-1, cl. 3.2.11).				