WORKSAFE
Mahi Haumaru Aotearoa

HSWA

TECHNICAL BULLETIN

June 2026

When to notify WorkSafe New Zealand about safety-critical element failures or damage

This technical bulletin helps operators of major hazard facilities and petroleum installations understand when they must notify WorkSafe about damage to or failure of a safety-critical element (SCE).

Introduction

Operators of major hazard facilities and petroleum installations have a duty to notify WorkSafe when a safety-critical element is damaged or fails and needs intervention to operate as designed.

There has been some uncertainty about exactly when notification is required, especially when the system includes redundancies or the SCE is still partly working.

This technical bulletin clarifies when operators are required to notify WorkSafe of damage to or failure of an SCE, and provides examples.

The examples in this guidance are for illustration only. What counts as an SCE can vary between facilities. These examples are not exhaustive and do not replace an operator's judgement or their legal obligations.

What is intervention?

In the context of SCEs, intervention means taking action to change or restore a system so it operates as designed. This could include:

- adjusting equipment
- repairing equipment
- replacing the SCE or its components
- putting a fix in place to improve how the system operates.

What the regulations say

A notifiable incident under section 24(3) of the Health and Safety at Work Act 2015 (HSWA) includes any unplanned or uncontrolled event that could expose a worker or another person to serious risk, even if no one is injured. This includes situations where potential exposure to risk arises from SCE failures or damage.

Operators must notify WorkSafe as soon as possible if an SCE is damaged or fails and needs intervention to operate as designed. This is a requirement under:

- regulation 33(c) of the Health and Safety at Work (Major Hazard Facility) Regulations 2016 (MHF regulations)
- regulation 70(f) of the Health and Safety at Work (Petroleum Exploration and Extraction) Regulations 2016 (PEE regulations).

Operators also need to meet requirements found in:

- schedule 5 of the MHF regulations
- schedule 2 of the PEE regulations.

These schedules explain what is expected for monitoring major incidents or accident control measures. Operators must:

- have a safety management system that includes performance standards for all control measures
- clearly define the criteria used to monitor whether control measures are operating as designed.

WSNZ_5082_JUN 26

Why collecting information on SCE notification matters

WorkSafe collects information on SCE notification matters to:

- better understand the types of notifiable incidents occurring at MHF and petroleum installations
- improve the quality of our data and insights
- identify and share common themes across the industry
- support operators by providing targeted guidance and promoting good practices.

Sharing these insights with operators helps create a safer and more informed industry.

How performance standards determine notification requirements

If an operator classifies a control measure as an SCE and it is damaged or fails, they must notify WorkSafe if intervention is needed to operate it as designed.

Performance standards provide the basis for determining whether an SCE is operating as designed. Clear, detailed performance standards support consistent, evidence-based decisions about whether a damaged or failed SCE requires notification.

Performance standards should specify the criteria such as functionality, availability, reliability, survivability, and interactions that define how the SCE must operate. They should also explicitly define any redundancy built into the SCE system.

An SCE may be degraded but still operate as designed, provided the performance standard contains sufficient detail to show that the system continues to meet all required criteria even with the damaged or failed component. The performance standard should clearly show how the system still meets its requirements, not just say that it does.

If a performance standard does not contain enough detail to clearly demonstrate that the SCE continues to operate as designed, then the damage or failure must be notified. For example, if the performance standard does not specify what is acceptable versus unacceptable failures, operators should err on the side of notifying.

In summary, clear and robust performance standards support consistent and transparent notification decisions. Vague or incomplete performance standards reduce consistency and result in more uncertainty about when notification is required.

When notification is required

These examples show failures where the performance standard does not have enough detail to show the SCE is still operating as designed.

Note: This guidance explains notification requirements for SCE failures. It is not performance standard guidance, and the examples are simplified and must not be used as templates. Other resources, including guidance from the Energy Institute or international regulators, provide more detailed information.

EXAMPLE:
FIREWATER PUMP FAILURE

What happened

One of two firewater pumps fails to start during testing.

What the performance standard says

The performance standard:

- states system design requires two 100% firewater pumps (one running and one on standby)
- specifies pump delivery expectations, including pump outlet pressure, flowrate, and may reference pump curve characteristics
- specifies two 100% firewater pumps should always be available.

Notify WorkSafe?

Yes. The performance standard says two pumps should be available 'at all times', but it does not allow for any downtime or maintenance.

If the performance standard allows one pump to be taken out of service for maintenance or testing, it should specify the maximum downtime allowed and reference a recognised standard.

EXAMPLE:
HIGH-HIGH LEVEL TRANSMITTER FAILURE

What happened

During testing, a high-high level transmitter was out of calibration and could no longer activate the emergency shutdown system at the correct set point.

What the performance standard says

The performance standard:

- states that high-high level transmitters are on tanks that activate the emergency shutdown system
- specifies a requirement for the system to respond at a specific high-high level set point (this set point may be defined in another document)
- includes maintenance processes, which are based on a recognised standard.

Notify WorkSafe?

Yes. The transmitter was outside the acceptable limits and needed fixing to work properly.

When performance standards may avoid notifications

These examples show failures where detailed performance standards clearly show the SCE system is still operating as designed.

EXAMPLE:
SHUTDOWN VALVE ACTIVATION

What happened

An emergency shutdown valve was activated. However, no component damage occurred that required intervention to restore the valve to operate as designed.

What the performance standard says

The performance standard:

- states that the emergency shutdown system includes a fail-safe shutdown valve
- specifies the need to shut on demand, the time to shut, and timing requirements
- defines availability requirements and maintenance processes.

Notify WorkSafe?

No, if the emergency shutdown valve was classified as an SCE and it operated as designed (met the performance standard) with no intervention required.

Otherwise, notify WorkSafe.

EXAMPLE:
GAS DETECTOR FAILURE

What happened

A single gas detector failed in a system with redundancy.

What the performance standard says

The performance standard:

- describes the gas detector system including number and locations of detectors
- describes the area the detector covers, the types of gases they detect, the alarm set points and executive actions (may reference coverage calculations that account for various weather conditions)
- specifies the availability requirements that take into account redundancy as shown in the coverage study
- defines repair timeframes and maintenance processes.

Notify WorkSafe?

No, if:

- redundancy is confirmed by the coverage study, and
- availability criteria are met.

Otherwise, notify WorkSafe.

EXAMPLE:
LIGHT BULB FAILURE IN AN EMERGENCY LIGHTING SYSTEM

What happened

One light bulb failed in an emergency lighting system designed with redundancy.

What the performance standard says

The performance standard:

- describes the emergency lighting system including number of lights, coverage and locations
- sets out how much light coverage the whole system needs and what each individual light must provide
- describes design, which includes built-in redundancy, such as allowing the system to keep working even if one light fails (for example, each light might be required to have 90% availability)
- defines repair timeframes and maintenance processes.

Notify WorkSafe?

No, if:

- redundancy is confirmed by the coverage study, and
- availability criteria are met.

Otherwise, notify WorkSafe.

Key points to remember

Operators must comply with requirements in:

- the MHF regulations – regulation 34 and parts 1 and 2 of schedule 4, or
- the PEE regulations – regulation 71 and parts 1 and 2 of schedule 9.

The root cause analysis required in each regulation's part 2 should be proportionate to the severity/ complexity of the SCE failure.

Operators must notify regardless of how the failure was discovered. It does not matter whether the failure was safe, revealed or found during testing – only whether the damaged or failed SCE needs intervention to operate as designed.

Redundancy must be documented in your performance standard, not merely asserted. You cannot rely on other equipment that is not part of that SCE system to provide redundancy.

Keep records of SCE issues you do not notify. WorkSafe needs to understand the link to your performance standards during inspections.

Not sure whether to notify?

Contact us for advice:

- hhu.mhf@worksafe.govt.nz or
- hhu.petroleum@worksafe.govt.nz

Where can you find more information?

For more information on managing SCEs and performance standards, see:

- Energy Institute, Guidelines for management of safety-critical elements (SCEs), third edition January 2020, ISBN 978 1 78725 155 7.
- UK Health and Safety Executive, Verification that safety-critical elements are 'suitable' at the commencement of a verification scheme SPC/Enforcement/174
- NOPSEMA Guidance Note N-09000-GN1914 A729008 and WA guidance Damage to Safety-Critical Equipment

The international guidance in the materials listed above is provided to give examples of good practice only. Operators must make sure they are compliant with all relevant New Zealand laws and regulations, which may differ from the international guidance.

For more detailed WorkSafe guidance on managing SCEs and performance standards, see:

- Notifying a rupture disk activation when classified as a SCE
- Reporting notifiable incidents for failure of pressure safety valves when identified as safety critical elements at Major Hazard Facilities
- Verification that safety-critical elements are suitable and effective at a major hazard facility or petroleum installation
- Major accident prevention policy and safety management systems