STAY LIVE
Electrical Industry Health & Safety Group

Electrical Industry

Guideline for Safety Critical Elements

Revision 1, Issued 1 June 2018

Role	Name	Company	Signature	Date
Author	David Lynch	Genesis Energy		13/06/2018
Reviewer	Tim Syme	Mercury		1/06/2018
Reviewer	Mathew Staddon	Contact Energy		6/06/2018
Reviewer	Alan Mudie	Contact Energy		6/06/2018
Reviewer	Charlie Noakes	Transpower		12/06/2018
Reviewer	Ian Gardiner	Meridian Energy		18/6/2018
Approver	Neil Gregory	Meridian Energy		18/6/2018

Contact Trust power Mercury meridian genesis Pioneer energy

eea Electricity Engineers' Association nova energy TRANSPOWER Tuwharetoa Geothermal Kawerau

Page intentionally left blank

Contents

1 Purpose

This document aims to provide a guideline for the definition and use of the term **Safety Critical Element** (SCE) within the New Zealand Electricity Generation and Distribution industry. It intends to:

- clarify the definition of an SCE
- outline a process for identifying SCEs within a facility
- suggest practices for the management of SCEs.

2 Background

The Health and Safety at Work Major Hazard Facilities (MHF) Regulations 2016 introduces the term Safety Critical Element.

Safety Critical Elements are items of equipment or control systems that warrant an increased level of oversight due to their critical role in preventing harm, or in mitigating the effects of a major incident.

The MHF Regulations apply only to facilities where specified hazardous substances are present in quantities exceeding prescribed thresholds. Consequently, the Regulations apply to some, but not all electricity industry facilities.

The Process Safety Working Group (reporting to StayLive), recognises the existence of other hazards which could cause significant events at sites not covered by the MHF Regulations. These other hazards include high voltage electricity, high pressure steam, large volumes of stored water and rotating machinery.

The Process Safety Working Group believes there is value in aligning with and applying certain principles of the MHF Regulations to contribute to good management of all electricity industry facilities regardless of whether they are designated MHF status or not. In particular, a common approach to the definition and treatment of Safety Critical Elements will:

- support the legislated requirements that must be met by MHF sites, and
- allow consistent (albeit optional) application of principles for non-MHF sites.

Within the MHF Regulations, items classified as Safety Critical Elements are subject to several specific requirements, including:

- independent verification of Safety Critical Elements to ensure they are suitable and remain in good repair for the life of the facility
- independently verified performance standards to ensure the effectiveness of the control is tested and maintained
- formal notification to WorkSafe of incidents where damage to or failure of a Safety Critical Element has occurred, requiring intervention to ensure it will operate as designed.

3 Scope

The application of SCEs should apply to all workplaces and all equipment which have the potential to cause a major incident, where a major incident is commonly regarded as:

> *"An uncontrolled event that exposes multiple persons to a serious risk to their health or safety"*

Note: Electricity companies need to set their own definition of a major incident. They may choose to align with their company risk matrix and include financial, environment, and other factors in the definition of a major incident.

4 Definition of a Safety Critical Element

A **Safety Critical Element** is defined as:

> *"Any part of the facility or its plant (including a computer program):*
>
> - *That has the primary purpose of preventing, or limiting the effect of a major incident,* ***AND***
> - *The failure of which could cause or substantially contribute to a major incident"*

For the purposes of this guideline, the term Safety Critical Element is limited to physical equipment and control systems, thus, Safety Critical Element does not include processes, procedures and documents and is generally analogous to Safety Critical Equipment.

This guideline aligns with the MHF-based definition to provide a refined focus on a smaller group of critical devices. It recognises that other Major Incident Control Measures (barriers) may exist at some facilities, and while these will not be managed under the governance of Safety Critical Elements, operators may elect to have a second tier of governance.

Note: From contributors' experience, application of this definition typically results in approximately 1–10% of an asset catalogue being tagged as an SCE. A traditional SCE definition (using **OR** rather than **AND**) originated from the oil and gas industry and leads to a broader application of the term SCE (20–30% of asset catalogue).

5 SCE Selection Process

The following outlines key steps for determining what items of equipment or control systems are to be defined as safety critical.

Step	Action	Notes
1	Define risk context, appetite, and key definitions including: • major incident • substantially contribute • major incident control groups.	Refer to Appendix 1 for suggested groups.
2	Identify major incident hazards and major incident events.	
3	Identify threats that can lead to each major incident.	Use a process such as HAZOP, HAZID, etc.
4	Identify control measures or barriers.	
5	Assign relevant control groups to barriers (as defined in Step 1) to assist with management and reporting.	Everything defined to this point (equipment, processes, and procedures) is now considered a Major Incident Control Measure; Safety Critical Elements are a subset of this group.
6	Develop Bowtie diagrams.	This can be carried out in parallel with 3 and 4.
7	Apply SCE selection criteria.	Refer to 'SCE Selection Criteria' below.
8	Identify SCEs on Bowties and in the equipment register.	Eg, functional location in CMMS.
9	Develop and implement performance standards.	

6 SCE Selection Criteria

From the definition, SCEs are any element:

> *That has the purpose* of preventing, or limiting the effect of a major incident,* ***AND***
>
> *The failure of which could cause or substantially contribute* to a major incident"*

There are two points (*) of this definition that operators still find ambiguous; each is further clarified below:

- **Purpose:** Is the primary purpose of all components of the control to prevent or limit the effect of a major incident? Elements which are designed for routine process control or process function, such as basic process controllers and mechanical primary containment, are not included; however independent shutdown systems and safety features of the primary containment would be expected to be included.
- **Substantially Contribute:** A *"failure of which could cause or substantially contribute"* is interpreted as a failure to fulfil its purpose, as defined above, to a specified performance requirement. Operators need to determine their own specified performance requirements; however, a suggestion is:

  > *Controls, which when functional provide an order of magnitude reduction in risk. To achieve this they must have high reliability, ie, Probability of Failure on Demand less than 0.1 (<10^{1}) and the control must be a 'suitable' control measure, eg, a safety valve is sized correctly for the incident*

Additions: At times an item may not clearly meet the requirements outlined above, however, may warrant classification as an SCE when considering the following points (at the discretion of the business and subject-matter expert):

- Is this the only plant control for the scenario, and the level of governance of Major Incident Control Measure is deemed insufficient?
- Has the control been deemed Safety Critical by the subject-matter expert (this may be due to including other definitions such as dam safety, or other factors, such as the control provides limited protection but across many scenarios)?

7 Major Incident Control Measure Equipment Grouping

For reporting purposes and alignment of performance standards it can be beneficial to group Major Incident Control types.

An example equipment grouping for Major Incident Control classification is provided in Appendix 1. Note that this is not a list of equipment which is safety critical – equipment is only classified as SCE if deemed so by the definition and process outlined above.

8 SCE Performance Standards

It is suggested that a performance standard is developed for each SCE group.

Performance standards can contribute to maintaining the effectiveness of SCEs. They can be developed for each SCE group to ensure effectiveness of that control is maintained to a defined tolerance.

Performance standards ensure any failure or degradation in performance is identified and corrected as a preventative measure. The overall effectiveness of a control can be measured by monitoring compliance against the standard.

9 References/Links

Health and Safety at Work (Major Hazard Facilities) Regulations 2016

Good Practice Guidelines: Major Hazard Facilities – Safety Assessment

StayLive website – Process Safety Working Group

10 Definitions

Term	Definition
Control	A measure which either helps to prevent an undesirable event or helps to mitigate the consequences.
Barrier	Refer 'Control'.
Industry Process Safety Working Group (IPSG)	A working group of StayLive with the purpose of collaborative improvement of process safety management systems and controls to reduce process safety risks in the electrical industry.
Major hazard facility (MHF)	A facility where specified hazardous substances are present (or potentially present) in quantities exceeding certain thresholds, as prescribed in the MHF Regulations.
StayLive	A New Zealand industry group with the goal of driving material and sustainable improvement in health and safety for employees, contractors and members of the public across the electricity industry.

11 Revision History

Rev	Date	Comment	By	Reviewed	Approved
1.0	1/06/2018	Issued for Use	David Lynch (Genesis Energy)	• Tim Syme (Mercury) • Mathew Staddon (Contact) • Alan Mudie (Contact) • Charlie Noakes (Transpower) • Ian Gardiner (Meridian)	Neil Gregory (Meridian)

Appendix 1 – Suggested Major Incident Control Groups

Passive Protection: Protected System	1	Civil Assets
	2	Pressure Containment Systems
Active Protection: Protected Systems	3	Critical Systems
	4	Lifting and Transportation Equipment
Protective devices – Detect	5	Critical Instrumentation
	6	Alarm Systems
Protective devices – Compute	7	Critical Control Systems
Protective devices – Act	8	Emergency Backup Supplies
	9	Main Protection Systems
	10	Protective Systems/Devices (these are self-actuating)
	11	Electrical Systems Protective Systems/Devices
Recovery	12	Fire Systems
	13	Environmental Containment Systems
	14	Emergency Planning Infrastructure and Equipment