Electrical Industry

Guideline for Development of Major Incident Bowtie Diagrams

StayLive Electrical Industry Health and Safety Group

Controlled Document

This is a controlled document. Printed copies may not be up to date. Check the StayLive website for the current version.

Document Control

Document name	Guideline for Development of Major Incident Bowtie Diagrams	
Document location	StayLive	
Document status	Issued for use	
Version number	Version 1.1	
Issue date	November 2023	
Validity period	Two years	
Next review date	November 2025	
Assigned Responsibilities	Author	John Lilly (Contact Energy)
	Reviewer	John Donnelly (Snowy Hydro)
	Reviewer	Nathaniel Janke-Gilman (Meridian)
	Reviewer	Tim Syme (Manawa Energy)
	Reviewer	Kent Mahon (Mercury)
	Reviewer	David Lynch (Genesis)
	Reviewer	Shane Minty (Origin)
	Reviewer	Bevan Lange (Eastland)
	Approver	Mark Utley (Contact Energy)

Record of Amendments

Version	Issue Date	Summary of Key Changes
1.0	August 2023	Draft issue
1.1	November 2023	First issue

Contents

1 Purpose

The purpose of this document is to provide a guideline for the definition and use of the term "major incident" for facilities not designated major hazard facilities (MHFs) and the development of major incident bowtie diagrams within the Electricity Generation and Distribution Industry. It intends to:

- define major incident for facilities not designated MHFs;
- outline a process for identifying major incident scenarios at a facility; and
- provide a framework for the development of major incident bowtie diagrams.

2 Background

Major Incident Definition

The New Zealand Parliament passed the Health and Safety Reform Bill into law in 2015 establishing the Health and Safety at Work Act 2015 (HSWA) [Ref. 1]. The HSWA is accompanied by a suite of supporting regulations to manage workplace health and safety in New Zealand, including the Health and Safety at Work (Major Hazard Facilities) Regulations 2016 (MHF Regulations) [Ref. 2].

The MHF Regulations introduces the term “major incident”, which is defined as:

(1) an uncontrolled event at a major hazard facility that:

(a) involves, or potentially involves, specified hazardous substances; and

(b) exposes multiple persons to a serious risk to their health or safety (including a risk of death) arising from an immediate or imminent exposure to—

(i) 1 or more of those substances as a result of the event; or

(ii) the direct or indirect effects of the event.

(2) Without limiting subclause (1), an uncontrolled event includes any of the following:

(a) escape, spillage, or leakage of a substance;

(b) implosion, explosion, or fire.

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

The StayLive Process Safety Working Group [Ref. 6] recognises the existence of other hazards which could cause significant consequence 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 robust major incident risk management at all electricity industry facilities regardless of whether they are designated MHF status or not. In particular, a common approach to the definition of major incidents and development of major incident bowtie diagrams will allow consistent (albeit optional) application of principles for non-MHF sites across industry.

Bowtie Diagrams

The Process Safety Working Group seeks to establish a common approach to major incident bowtie diagram development across industry that is aligned with international good practice standard guidance developed by the American Institute of Chemical Engineers in collaboration with the Center for Chemical Process Safety and Energy Institute (*Bowties in Risk Management: A Concept Book for Process Safety*: 2018) [Ref. 4].

The intent is to standardise bowtie diagram development in accordance with the standard guidance to:

- reduce complexity and increase understanding of the interrelationship between major incident scenarios, associated threats/hazards and barriers.
- prevent the false indication of the number of barriers and layers of protection in a threat line through the development of barrier criteria requirements and removal of degradation factors and controls that are represented as independent barriers.
- allow for bowtie and barrier ownership, accountability and management at the most effective level.
- support identification and classification of major incident control measures (MICMs) and safety critical elements (SCEs).
- facilitate major incident risk management through bowties being more actively and effectively used in the ongoing assurance management of barriers and their condition, performance and effectiveness.

While there is general agreement on the aligned bowtie development approach, the Process Safety Working Group recognises that there may be some differences between members and makes allowances for these within the guideline where noted.

Note: the standard guidance does not need to be followed to the letter, but should be closely adhered to as good practice. Aspects can be adapted to make bowtie diagrams suitable for a particular participant's purposes.

3 Major Incident Definition

The StayLive Process Safety Working Group has adopted the following broader definition of a major incident for non-MHF sites that has been developed for the identification of major incident scenarios and creation of major incident bowtie diagrams.

At facilities that are not designated MHFs, a major incident hazard means a hazard that has the potential to cause a major incident:

(1) Major incident means an uncontrolled event at a facility that:

(a) is associated with the physical operational processes related to the generation of electricity or energy supply and excludes occupational health and safety hazards; and

(b) exposes multiple persons to a serious risk to their health or safety (including a risk of death) arising from an immediate or imminent exposure to the direct or indirect effects of the event.

(2) An uncontrolled event includes any of the following:

(a) escape, spillage, or leakage of a substance;

(b) implosion, explosion, or fire;

(c) loss of control of operational equipment/facilities;

(d) catastrophic failure of plant;

(e) loss of containment of energy.

This definition of major incident:

- closely aligns with that defined in the MHF Regulations and uses similar terminology (i.e. uncontrolled events that expose multiple persons to a serious risk to their health and safety).
- broadens the scope through application to all facilities and by removing the specific requirement for events to involve a specified hazardous substance.
- provides clarification that major incident uncontrolled events are those directly related to the physical operational processes of the power plant related to the generation of electricity or energy supply, with the focus placed on process safety events and occupational health and safety hazards specifically excluded. This allows other uncontrolled events with potentially significant consequences associated with high voltage electricity, high pressure steam, large volumes of stored water and rotating machinery to be defined as major incidents.

Note: This major incident definition is specific to safety consequence related hazards and incidents. Participants will need to set their own definition of a major incident; they may choose to completely align with the definition provided above or broaden the scope of the major incident definition to include asset damage, financial impact, reputational damage, environmental damage, and/or other factors in line with their specific requirements. Where this is the case, additional impact qualifications for what constitutes an asset, financial, reputational, or environmental major incident can be added to the definition provided (with the safety related aspects of the definition remaining consistent).

4 Bowtie Diagram Development Criteria

Bowtie diagrams are a diagrammatical representation of a hazardous incident that assist with visualisation and understanding of a potential hazardous incident risk and its associated threats/hazards, consequences, and control barriers and the interrelationships between these.

Bowtie Level of Detail

Each participant will need to determine at what level their major incident bowties will be based/structured to meet their intended purposes (e.g. company/group/station wide, or unit specific). This is required to assist with the framing of major incident scenarios and major incident bowtie diagrams.

The creation of station specific major incident bowties is recommended as this allows for:

- major incident scenarios and bowtie diagrams to be developed that are specific to each station and its plant/equipment/controls and environment.
- station ownership of major incidents and barrier condition, performance and effectiveness management at their sites.
- incorporation of bowtie reviews into station risk review processes.
- allocated ownership of bowtie threats to station personnel that are most familiar with the plant/equipment, barriers and their associated assurance activities, and who have the ability to take effective action.
- a reduced number of major incident bowtie diagrams to manage, review and revise.

Note: participants may decide to create:

- more general company or group-wide bowties only;
- unit specific bowties where there are significant or unique differences requiring unit level bowties; or
- include generic company or group-wide bowties in addition to station specific bowties.

Bowtie Terminology and Structure

Bowtie diagram development and structure is aligned with international good practice standard guidance developed by the American Institute of Chemical Engineers in collaboration with the Center for Chemical Process Safety and Energy Institute (*Bowties in Risk Management: A Concept Book for Process Safety*: 2018) [Ref. 4].

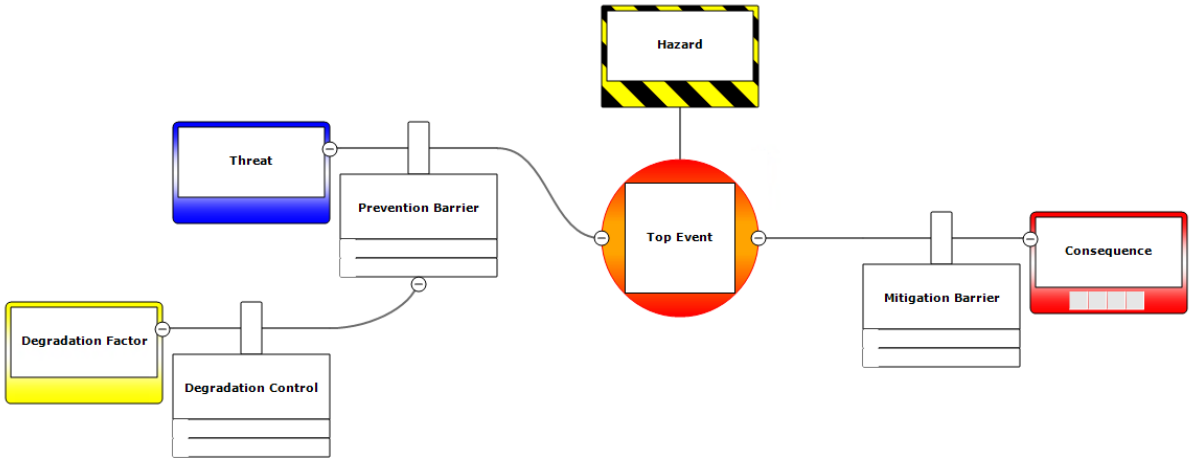

Figure 1: Bowtie Structure

The following terminology, definitions, criteria and methodology should be used to develop and structure the bowtie diagrams:

- **Hazard** – Describes the hazard in a controlled state and is linked to equipment/asset system for bowtie context/scope definition.
- **Top Event** – Describes how/what control is lost from the equipment/asset system and the hazard in an uncontrolled state.
- **Consequence** – Describes release of hazards in an uncontrolled state/nature of the risk and potential subsequent consequences, severity of impact and escalation potential. Separate consequence lines should be developed for each potential consequence (e.g. kinetic energy/projectiles, fire/explosion, toxic gas release).

  Note: potential consequences may include asset damage, financial impact, reputational damage, environmental damage, and/or other factors in line with the definition of a major incident used.
- **Threats** – Describes a possible initiating event that can result in a loss of control or containment of a hazard (i.e. the identified Top Event). Threats should be specific and every credible threat must be included. Separate threat lines should be created where required to ensure barriers directly relate to the threat and do not give a false sense of layers of protection. Threat lines with identical/similar barriers should also be combined where possible.

  Threats typically fall into one of the following categories:

  - Specific major incident scenario bowtie threats:
    - Operating condition deviations (e.g. overpressure/overspeed/overflow).
    - Physical equipment/component/mechanical failure related to primary equipment/systems that are part of the process.
  - Common (shared) major incident bowtie threats:
    - Natural events (e.g. seismic, extreme weather, lightning, volcanic, flooding, subsidence).
    - External impact hazards (e.g. vehicles/mobile plant, dropped objects, structural collapse, excavation).

- Escalation hazards (e.g. major plant fire).
- Sabotage/vandalism/terrorism (external/internal/cyber).

Note: common (shared) bowtie threats (i.e. that are applicable to all or multiple bowtie diagrams) may be hidden from a bowtie to focus on only the specific major incident scenario threats.

- **Prevention Barriers** – Describes a control measure that can prevent a threat from turning into a top event. Prevention barriers cannot only reduce the probability of a top event; they must have the capability on their own to prevent a top event occurring. They do not need to be 100% reliable but they must be effective, independent, and auditable.
    - "Effective" means the barrier is capable to perform the intended function when demanded and to the standard intended.
    - "Independent" means can independently prevent the top event and removes common mode failures/dependencies between barriers. Where these exist in the same threat line then barriers are removed (e.g. same operator response action required to alarms).
    - "Auditable" means that the barrier can be performance monitored and assessed.

  To align with the standard guidance, barriers in the bowtie diagram should be intuitively placed in time sequence of their effect (i.e. where the barrier delivers its function). As the last line/s of defence, identified safety critical element prevention barriers should be located as the last barrier/s closest to the "Top Event" at the centre of the bowtie diagram.
- **Mitigation Barriers** – Describes a measure that may only mitigate, not prevent, a consequence. Mitigation barriers should also intuitively be placed in time sequence of their effect.
- **Degradation Factor** – Describes a condition that can reduce the effectiveness of the barrier to which it is attached (e.g. power failure, operator or maintenance error, instrument/control failure, wear and tear).
- **Degradation Control** – Do not meet the criteria for a Barrier (effective, independent and auditable). But they can help defeat the degradation factor. Degradation controls are frequently human and organisational factors concerned with management of risk and barrier assurance (e.g. engineering standards, training and competency, contractor management, management of change, permit to work, quality assurance and control, design reviews).

  Degradation factors and controls should be used sparingly. In line with the standard guidance, it is recommended that critical degradation factors (e.g. physical barrier wear and tear, instrument/control protection or software failure, operator/maintenance error, power failure) and controls remain displayed in bowties:
    - to ensure staff understand the barriers, the degradation factors that threaten them, and the degradation controls relied upon to maintain barrier effectiveness.
    - since degradation factors may also be major incident hazards (threats) and failure of degradation controls still have the potential to lead to failure of a barrier which may subsequently result in the Top Event.
    - so that critical degradation controls can be performance monitored, managed and reviewed like all other major incident control measures.

- because degradation controls assist with identification of critical tasks (e.g. specific operator actions, or inspection, testing and maintenance activities) and linking of these to training and competency requirements or the need for establishment of further measures.

Note: degradation factors and controls generally apply to multiple barriers. Participants may choose to display them against all applicable barriers, remove them, or display them only once in each bowtie diagram and reference them where applicable elsewhere to ensure they are captured, but to reduce clutter and limit the size of bowtie diagrams.

- **Barrier Types** – Identify the main characteristic of the barriers. Includes barrier types that can be physical or non-physical/procedural. The use of five barrier types is suggested by the standard guidance and these are listed below in sequence of effectiveness, giving a hierarchy of control:
  - Passive hardware (the barrier works by virtue of its presence)
  - Active hardware (all elements of the barrier are solely executed by technology)
  - Active hardware + human (the barrier is a combination of human behavior and technological execution)
  - Active human (the barrier consists of human actions, often interacting with technology)
  - Continuous hardware (the barrier is always operating)

  Active barriers must be able to detect-decide-act (i.e. 'detect' a change in condition or what is going wrong, 'decide' what action is required to rectify and 'act' to stop the threat from progressing further). A barrier can only be "Active hardware" if all three aspects of detect-decide-act are hardware.

  Note: These barrier type categories are recommended by the standard guidance for clarity and understanding. However, different barrier type categories/terminology can be used by participants.

- **Safety Critical Element** – means any part of a facility or its plant (including a computer program):
  a) that has the purpose of preventing, or limiting the effect of, a major incident; and
  b) the failure of which could cause or contribute substantially to a major incident.

  Refer to the StayLive *Guideline for Safety Critical Elements* for further guidance criteria used in the identification of safety critical elements [Ref. 5].

Participants may decide to take a staged approach to bowtie development and incorporation of aspects of the standard guidance to ensure bowtie development and use is practicable for each participant, e.g.:

- Bowties include specific major incident threat lines and barriers only;
- Bowties include barriers and there is company or group-wide reporting on macro degradation factors/controls and common threats;
- Bowties include degradation factors and controls tied to individual barriers.

5 Major Incident Scenario and Bowtie Diagram Development Process

The following outlines key steps for determining what uncontrolled events are to be defined as major incidents and provides a recommended framework for the development of major incident bowtie diagrams.

Step	Action	Notes
1	Bowtie development personnel	- Hazard identification, risk assessment and bowtie diagram development should be led by an experienced facilitator knowledgeable in bowtie methodologies and risk assessment techniques, and with the technical expertise to understand the plant/process or operation being analysed to guide the process and ensure the required outcomes. Typically senior engineers with strong communication and facilitation skills. - Workshop teams should be multi-disciplinary and comprise experienced and competent personnel who are familiar with the site management, design, operation and maintenance of the facilities (including relevant engineering, subject matter experts, production, and generation ops/controller/technician representation as appropriate). In particular, it includes those most familiar with the plant operations, assets/equipment, controls, maintenance and risks associated with the hazards being discussed.
2	Develop definition of major incident for non-MHF sites	- Completely align with the definition provided or broaden the scope to include asset damage, financial impact, reputational damage, environment damage, and/or other factors in the definition of a major incident. - Use existing bowties (if available) to screen and group major incident scenarios as per the adopted major incident definition.
3	Determine the scope of the bowties	- Decide what level the bowties will be based/structured (e.g. company/group/station wide, or unit specific).

Step	Action	Notes
4	Conduct site wide hazard identification and risk assessment studies as the first part of the safety assessment process	- Hazard identification and risk assessment studies may include HAZID, HAZOP, LOPA etc. - Risk assess all hazards using a risk assessment matrix with defined likelihood and consequence criteria to establish the risk. - Collate and validate HAZIDs/HAZOPs for those sites where this analysis has already been completed.
5	Identify major incident hazards	- Major incident hazards are those that have the potential to cause an uncontrolled event that has been risk assessed to have a people safety consequence severity that results in multiple serious injuries or fatalities. - Must be hazards associated with the physical operational processes of the power plant related to the generation of electricity or energy supply. - Excludes occupational health and safety hazards. - May include asset damage, financial impact, reputational damage, environment damage, and/or other factors depending on the definition of a major incident used.
6	Screen and group major incident hazards to identify major incident scenarios	- Hazards are grouped based on related plant operational processes and asset/equipment. - Major incident scenario description should include the event, hazardous substance/energy, associated equipment/asset and consequence.
7	Develop a Major Incident Hazard Register	- Major Incident Hazard Registers should define each major incident scenario, and comprehensively document all associated major incident hazards, prevention and mitigation control measures (not required to be independent), consequences and escalation potential.
8	Develop a draft major incident bowtie diagram for each major incident scenario	- Major incident bowtie diagrams should be a mirror of the major incident scenarios identified in the Major Incident Hazard Register. - Major incident bowtie diagrams should only include prevention barriers that can be demonstrated to be independent layers of protection (i.e. have the capability on their own to prevent a top event). They do not need to be 100% reliable, but must be effective and auditable.

Step	Action	Notes
9	Remove degradation factors and controls from each bowtie diagram threat's prevention barriers for which they do not meet the requirement of a barrier (as defined above)	- Degradation Factor – is a condition that can reduce the effectiveness of the barrier to which it is attached. - Degradation Control – do not meet the criteria for a barrier (effective, independent and auditable). But they can help defeat the degradation factor. - Determine how and which degradation factors and controls may remain displayed in the bowtie diagrams attached to barriers. - Note: the Major Incident Hazard Register should still comprehensively document all major incident hazards and associated major incident control measures that are not included in the bowtie diagrams (e.g. warning signage, behavior and value controls such and life saving rules, incident reporting etc.).
10	Conduct Major Incident Hazard Register and bowtie review workshop	- Workshop review of the draft Major Incident Hazard Register and major incident bowtie diagrams. - Provides a forum for appropriate workforce engagement and participation in major incident bowtie diagram development as part of the safety assessment process. - Document the process and finalise the Major Incident Hazard Register and major incident bowtie diagrams.
11	Finalise the bowties and incorporate into risk management processes	- Finalise the bowties and handover ownership to the appropriate allocated person/s responsible for management and review of bowties. - Incorporate bowties into enterprise risk management tool/software and risk management and review processes so that they can be actively used in the management of risk through assessment of barrier condition, effectiveness and performance. - Ensure bowties are stored and managed appropriately as controlled documents.

Step	Action	Notes
12	Identify safety critical elements barriers	- Use the bowtie diagrams for assistance in the identification of safety critical elements. Under the MHF Regulations, a safety critical element means any part of a facility or its plant (including a computer program): *a) That has the purpose of preventing, or limiting the effect of, a major incident;* and *b) The failure of which could cause or contribute substantially to a major incident* - Refer to the StayLive *Guideline for Safety Critical Elements* for further guidance criteria used in the identification of safety critical elements [Ref. 5].

6 Definitions

Term	Definition
Major Hazard Facility	A facility where specified hazardous substances are present (or potentially present) in quantities exceeding certain thresholds, as prescribed in the MHF Regulations [Ref 2].
Process Safety Working Group	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.
Safety Critical Element	A safety critical element means any part of a facility or its plant (including a computer program): a) that has the purpose of preventing, or limiting the effect of, a major incident; and b) the failure of which could cause or contribute substantially to a major incident. Refer to the StayLive *Guideline for Safety Critical Elements* for further guidance criteria used in the identification of safety critical elements [Ref. 5].
StayLive	An 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 [Ref 6].

7 References/Links

1. *Health and Safety at Work Act 2015*, Public Act No 70, September 2015
2. *Health and Safety at Work (Major Hazard Facilities) Regulations 2016*, February 2016
3. Good Practice Guidelines, *Major Hazard Facilities: Safety Assessment*, July 2016, WorkSafe New Zealand
4. *Bowties in Risk Management: A Concept Book for Process Safety*, American Institute of Chemical Engineers, 2018
5. *Guideline for Safety Critical Elements*, StayLive – Electrical Health and Safety Group, Version 1.1, April 2022
6. StayLive website – Process Safety Working Group