Major Incident Bowtie Diagrams

18th July 2024

Rachelle Meijer- Senior Fleet Engineer

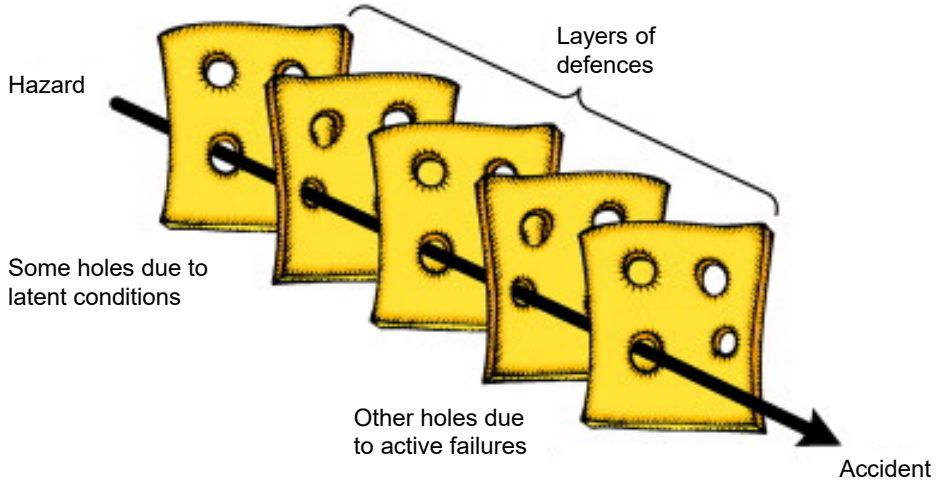
What are Bowtie Diagrams?

Diagram to help visualise a risk with one easy to understand picture.

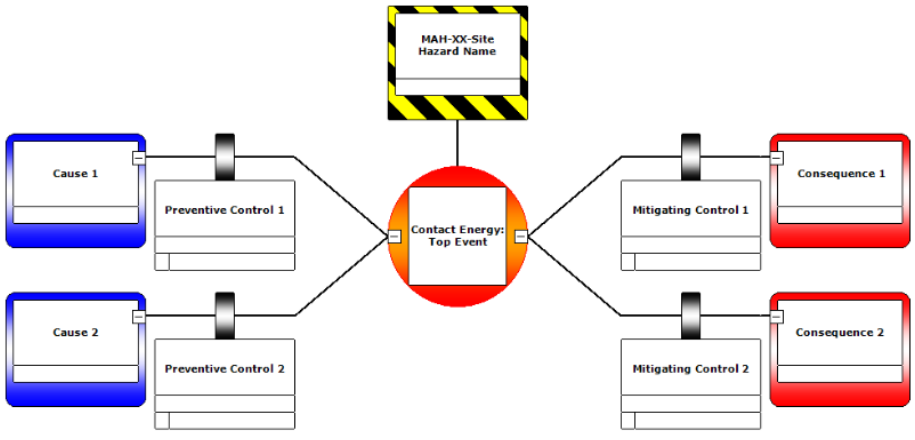
Threats, Consequences and key Control and Mitigation barriers are depicted in time sequence so anyone looking at the diagram can easily understand potential Events and how they are prevented.

Contact Energy use these to support understanding of Process Safety.

Swiss Cheese Model



Bowtie Diagram



Key Bowtie Terminology

Hazard
Describes hazard in controlled state linked to equipment/asset system for bowtie context/scope definition.

Top event
Describes how/what control is lost from equipment/asset system and hazard in uncontrolled state.

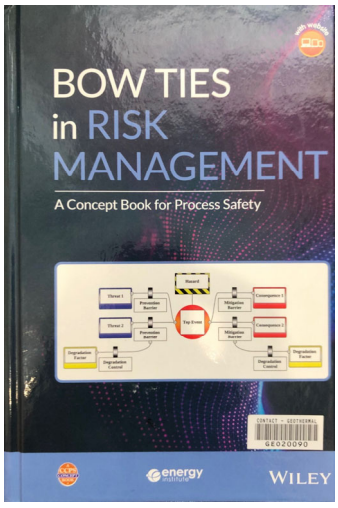
Consequence
Describes release of hazards in uncontrolled state/nature of risk and potential subsequent consequences, severity of impact and escalation potential.

Threats
Describes a possible initiating event that can result in a loss of control or containment of a hazard.

Prevention Barriers
Describes a control measure that can prevent a threat from turning into a Top Event by itself.

Mitigation Barriers
Describes a measure that has lower performance than prevention barriers in that they may only mitigate, not prevent, a consequence.

Bowtie in Risk Management Standard



- Published 2018
- Provides current industry good practice standard guidance from Center for Chemical Process Safety (CCPS) and Energy Institute.
- Not followed to the letter, but closely adhered to as good practice. Have adapted aspects to make bowties suitable for Contact's purposes (some degree of judgement is required as stated in the guidance).

6

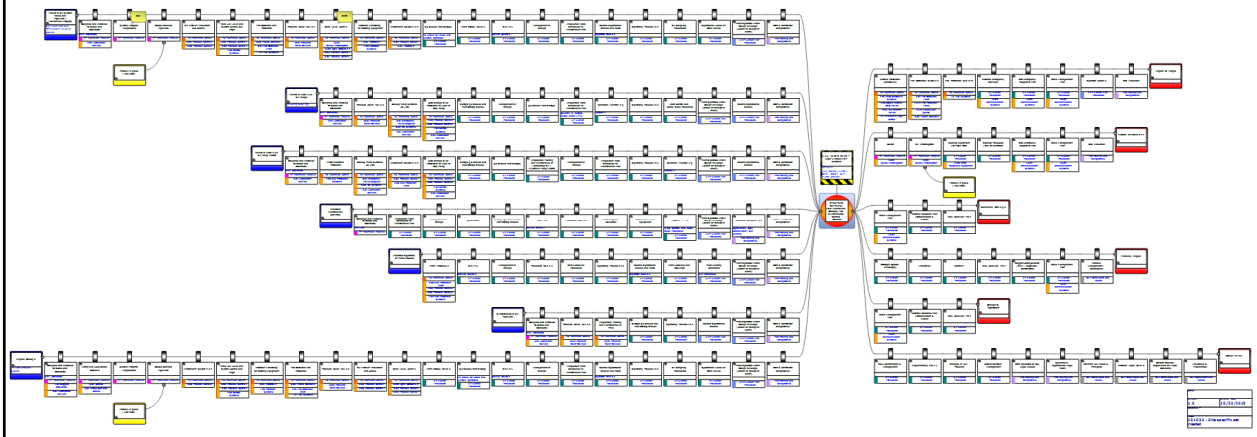
Bowtie History- Starting Point

- Used to manage risk and were created during the OSIP program started in 2014.
- Based around events with a risk rating of high and above.
- Great for getting SME's into a room to ensure that events had been raised and had measures in place to prevent them.
- Reviews of the bowties were carried out on an annual basis.

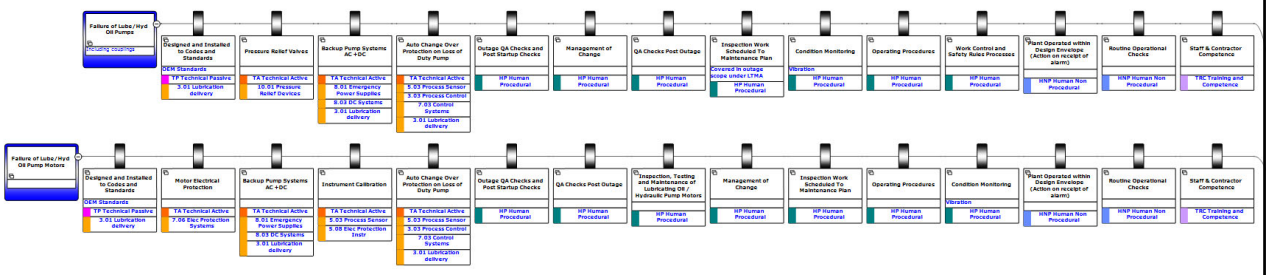
Summary of Bowties

Hazard Name	Top Event
BOP - Aux Boiler incl Tubes, Headers - Gas, SHP Steam	LOC: Explosion, Fire, Structural Failure
BOP - Backup Electrical Systems (DC and UPS)	Failure: Mechanical Damage, Fire, Explosion, LD, Electric Shock, Electrolyte Burns
BOP - Bulk Storage - Supply System - Water, Chemical	LOC: Environmental, Chemical Burns
BOP - Compressed Air System - Air	LOC: Projectile, HP Pressure, Steam supply, LD
BOP - Fire Systems - CO2	LOC: Suffocation
BOP - Fuel Supply System - Gas	LOC: Fire, Explosion, Environmental, Loss of Energy Supply to Fonterra
Civil Engineering - Cooling Tower	Collapse / Fire /Legionella Outbreak
Dropped Objects (damage to plant)	LOC/Damage to Plant:: fire, explosion, projectiles, steam release, damage to critical plant
Electrical Systems - AC Electrical - Cable Systems, Switchgear, Bus, Reactors, Earth System	Electrical Fault: Fire, Explosion, Arcing, Chemical Release, Earth Potential Rise on Earth System
Electrical Systems - Oil Filled HV Transformers - Network Transformers, 400V Auxiliary Transformers	LOC: Fire, Explosion, Electrical, Oil Discharge, Environmental
Feed System - Feedwater/Condensate Systems - Hot Water, Steam	LOC: Burns, Projectile, Steam Contamination
GT - Air Intake	Mechanical Failure: Major Damage to All Equipment, Fire, Projectile
GT - Combustion System - Gas	LOC: Explosion, Fire, Projectile
GT - Compressor Blades and Vanes	Mechanical Failure: Major Damage to All Equipment, Fire, Projectile
GT - Diesel Start System - Diesel	LOC: Fire, Explosion, Environmental
GT/HRSG/Auxiliary Boiler - Exhaust / Stacks	Structural Mechanical Failure: Major damage, fire, projectile, environmental

Bowtie History



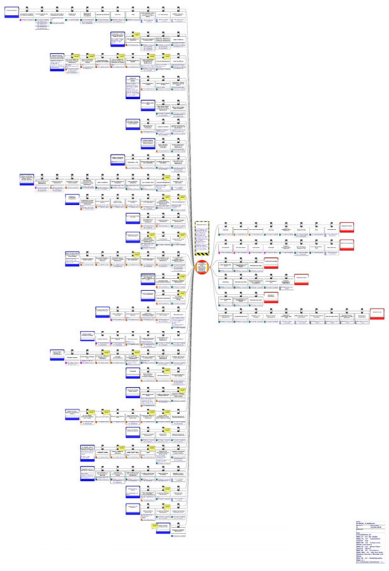
Bowtie History

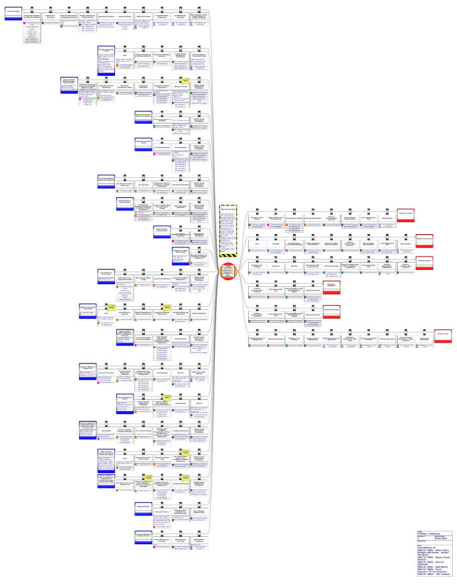


Bowtie History- Issues

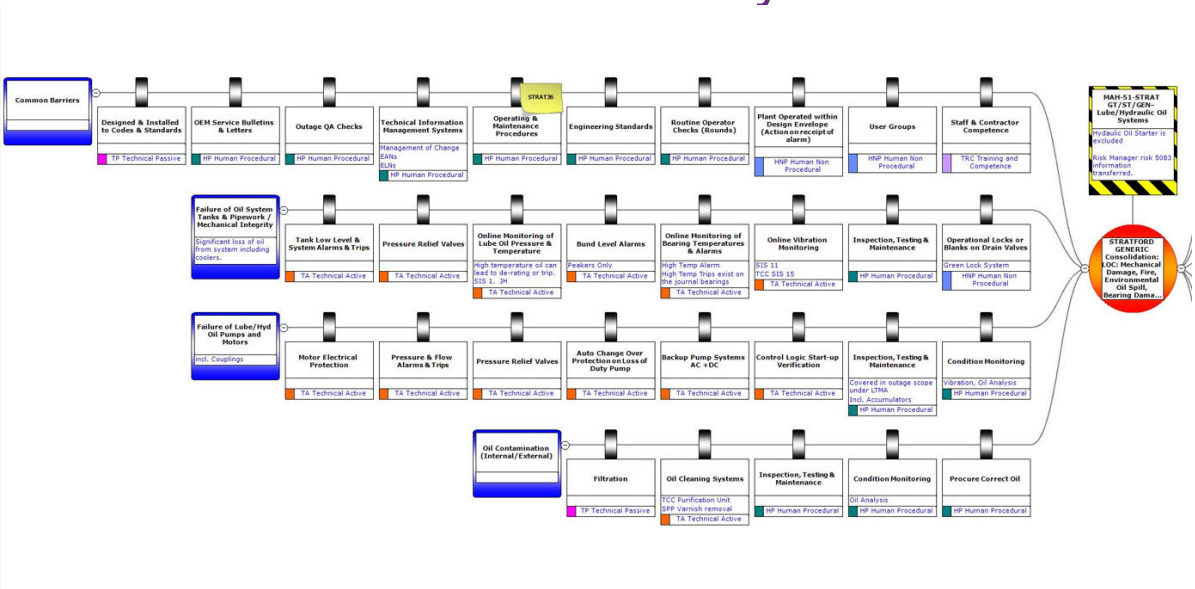
- No clear definition of what constituted a major incident, barrier or threat. Inconsistent language leading to confusion.
- No ownership or accountability for the process.
- Huge quantity of bowties and barriers taking time to review leading to large amounts of actions and a false sense of security.
- Personnel on sites not engaging with the process or having a clear understanding of the key risks or barriers in place.

Bowtie History





Bowtie History



STAY LIVE
Electrical Industry Health & Safety Group

Electrical Industry

Guideline for Development of Major Incident Bowtie Diagrams

Staylive Process Safety Working Group

STAY LIVE
Electrical Industry Health & Safety Group

Questions

- What is a Major Incident?
- How do we intend to use Major Incident bowties?
- What is the level of detail (e.g. company general/group/station/unit)?
- How will reviews of Bowties be conducted?

What is a Major Incident?

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 of the power plant 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.

16

How Bowties are Utilised

- Visual summary outlining the process safety major incidents and threats.
- Support identification and classification of Major Incident Control Measures (MICMs), Safety Critical Equipment (SCEq) and Safety Critical Elements (SCEs).
- Active, ongoing assurance management of barriers and their condition, performance and effectiveness.
- Feed into further risk management tools and post incident learnings (LOPA, SOFAIRP, etc)

Bowties Level of Detail

- Fuel Type/ Station Specific Approach (Hydro, Natural Gas, Diesel, Pentane, Steam)
- Scenarios and bowtie diagrams are specific to each station and its plant/equipment/controls and environment.
- Asset Manager ownership of the review process and drives the management of barrier condition, performance and effectiveness at their sites.

Bowtie Development Process

Step	Action	Notes
1	Develop definition of major incident for non-MHF sites	- Use existing bowties to screen and group major incident scenarios as per the adopted major incident definition above for each station
2	Conduct station wide hazard identification and risk assessment studies	- Hazard identification studies may include HAZID, HAZOP, etc. - Risk assess all hazards using a risk assessment matrix with defined likelihood and consequence criteria to establish the risk - Collate/validate HAZIDs/HAZOPs for those sites where this analysis has been completed
3	Identify major incident hazards	- Hazards that have the potential to cause an uncontrolled event that has a people safety consequence that results in multiple serious injuries or fatalities - Hazards associated with the physical operational processes of the power plant related to the generation of electricity or energy supply

19

Bowtie Development Process

Step	Action	Notes
4	Screen and group major incident hazards to identify major incident scenarios	- Hazards are grouped based on related plant operational process and asset/equipment - Major incident scenario description should include the event, hazardous substance/energy, associated equipment/asset and consequence - Refer to suggested major incident scenarios for thermal facilities (Stratford) as an example
5	Develop a Major Incident Hazard Register for each station	- Major Incident Hazard Register should define each major incident scenario, and comprehensively document all associated major incident hazards, prevention and mitigation control, consequences and escalation potential

20

Examples of Major Incident Scenarios

MI Scenario #	Major Incident Scenario Description	Top Event	Consequence
MI-01	Loss of containment from fuel gas systems (pipework, hot water boiler, fuel gas peaker compressors) with subsequent ignition resulting in fire/ explosion Notes: 1. Includes all associated equipment from delivery point (ESD interface point) of the gas yard up to the fuel gas manifolds in the gas turbine machine and peaker fuel gas compressors.	Loss of containment of natural gas from fuel gas systems (pipework, hot water boiler, compressors)	Loss of containment of natural gas from fuel gas systems (pipework, HW boiler, compressors) under pressure and generation of a flammable vapour cloud leading to: - Immediate ignition - jet fire; - Delayed ignition - flash fire burning back to jet fire; or vapour cloud explosion (VCE) burning back to jet fire; with the potential for multiple serious injuries/fatalities Potential escalation of fire onsite resulting in cumulative fires/explosions and equipment damage
MI-02	Catastrophic failure of turbine (steam and gas) and release of kinetic energy/loss of containment of high pressure steam or fuel gas with subsequent ignition resulting in fire/ explosion	Catastrophic failure of turbine and release of kinetic energy/loss of containment of high pressure steam or fuel gas	Release of kinetic energy/projectiles and loss of containment of high pressure steam or fuel gas under pressure and generation of a flammable vapour cloud leading to: - Immediate ignition - jet fire; - Delayed ignition - flash fire burning back to jet fire; or vapour cloud explosion (VCE) burning back to jet fire; with the potential for multiple serious injuries/fatalities and equipment damage Potential escalation of fire onsite resulting in cumulative fires/explosions and equipment damage
MI-03	Catastrophic failure of generator and release of kinetic energy and electrical energy resulting in fire/explosion	Catastrophic failure of generator and release of kinetic and electrical energy	Release of kinetic energy/projectiles and electrical energy resulting in fire/explosion with the potential for multiple serious injuries/fatalities and equipment damage Potential escalation of fire onsite resulting in cumulative fires/explosions and equipment damage

21

Examples of Major Incident Scenarios

MI Scenario #	Major Incident Scenario Description	Top Event	Consequence
MI-04	Electrical fault and release of Electrical Energy from Electrical Systems (inc. Cable Systems, Switchgear, Reactors, Earth System, Battery, UPS, inverters) resulting in fire/explosion, arcing, chemical release, livening of earth system	Electrical fault and release of Electrical Energy from Electrical Systems	Fire/explosion, electrocution and/or toxic gas release with the potential for multiple serious injuries/fatalities and equipment damage Potential escalation of fire onsite resulting in cumulative fires/explosions and equipment damage
MI-05	High voltage transformer fire (oil filled and dry type)	Transformer fire	Fire/explosion with the potential for multiple serious injuries/fatalities and equipment damage Potential escalation of fire onsite resulting in cumulative fires/explosions and equipment damage
MI-06	Loss of containment from water cycle systems (excluding GT and ST) and release of high pressure/temperature steam/water/flue gas Notes: 1. Includes heat recovery steam generator, piping and equipment up to steam turbine.	Loss of containment of high pressure/temperature steam/water/flue gas from water cycle systems	Release of high pressure/temperature steam/water/flue gas with the potential for multiple serious injuries/fatalities and equipment damage
MI-07	Loss of containment of hydrogen with subsequent ignition resulting in fire/explosion Notes: 1. Includes generator H2 containment, storage (bottles/tank) and pipework.	Loss of containment of hydrogen from generator H2 containment, storage (bottles/tank) and pipework	Fire/explosion with the potential for multiple serious injuries/fatalities and equipment damage Potential escalation of fire onsite resulting in cumulative fires/explosions and equipment damage

22

Major Incident Hazard Register

- MIH Register comprehensively documents all major incident scenarios and associated major incident hazards, prevention and mitigation controls (not required to be independent), consequences and escalation potential (draft example below).

STRATFORD MAJOR INCIDENT HAZARD REGISTER

Dated: March 2023

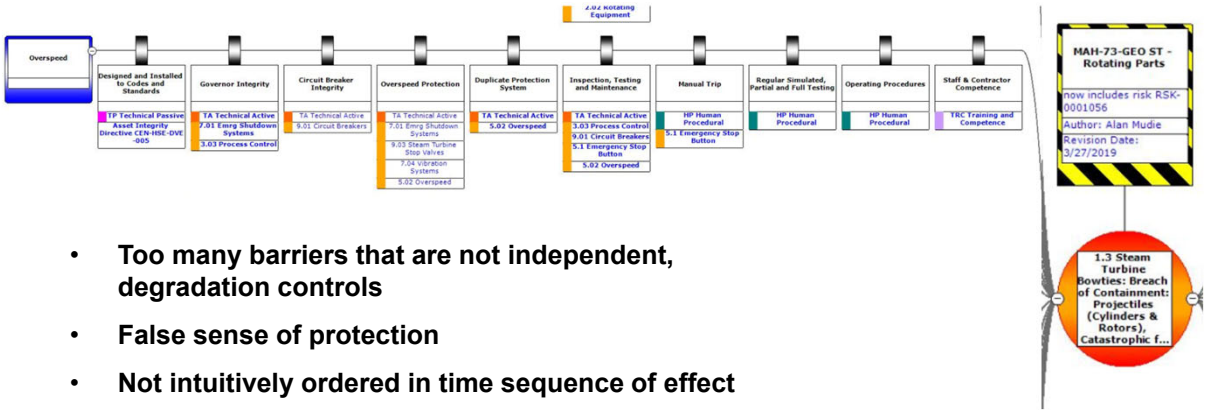
Revision: 1

MI ID #	Major Incident Scenario	Major Incident Hazard (Threat)	Prevention Controls (Threat Barriers)	Consequence	Mitigation / Escalation Controls (Recovery Measures)
MI-01	Loss of containment from fuel gas systems (pipework, hot water boiler, peaker fuel gas compressors) with subsequent ignition resulting in fire/ explosion Notes: 1. Includes all associated equipment from delivery point (ESD interface point) of the gas yard up to the fuel gas manifolds in the gas turbine machine and peaker fuel gas compressors.	Overpressure	- Designed and installed to codes and standards - Gas pressure reducing station - Overpressure protection (high pressure, high high pressure, trip?, with alarm?) - Pressure relief valves - Inspection, testing and maintenance - Operating and maintenance procedures - Staff and contractor training and competence	Loss of containment of natural gas from fuel gas systems (pipework, hot water boiler, peaker fuel gas compressors) under pressure and generation of a flammable vapour cloud leading to: - Immediate ignition - jet fire; - Delayed ignition - flash fire burning back to jet fire; or vapour cloud explosion (VCE) burning back to jet fire; with the potential for multiple serious injuries/fatalities Potential escalation of fire onsite resulting in cumulative fires/explosions and equipment damage	- Fire and gas detection - Emergency shutdown valves - Earthing and bonding - Hazardous area zoning and ignition source controls: · Electrical installation design meets AS/NZ standard requirements · Restricted access and designated traffic routes for vehicles onsite · Plant equipment spaced in accordance to design spacing requirements · Hot work permit · Procedures around personal electronic equipment on-site - Manual fire call points (initiates fire alarm) Manually activated ESD pushbuttons (control room and site) - Manual firefighting equipment (fire extinguishers) - Fire monitors and fire supression system - Personal Protective Equipment - Site emergency siren - Site Emergency Response Plan - Fire and Emergency New Zealand response - Business Continuity Plan/ Disaster Recovery Plan/ Crisis Management Plan
		External Corrosion	- Designed and installed to codes and standards (with corrosion allowance) - Protective coatings (paint) - External visual inspections - Cathodic protection on buried pipelines - Inspection and maintenance		
		Internal Corrosion	- Designed and installed to codes and standards - Dry natural gas with minimum specifications in place for water content - Filter separators - Inspection and maintenance (inc. regular thickness testing)		
		Latent failure conditions (material or installation defects)	- Designed and installed to codes and standards - Quality assurance/control process - Project Safety Reviews (HAZOP, constructability, design reviews) - Hydrostatic testing during commissioning to prove integrity of pipeline - Inspection and maintenance		
		Pipework/equipment failure (e.g. degradation)	- Designed and installed to codes and standards - Support structures, spring hangers - Inspection and maintenance		

Bowtie Diagrams

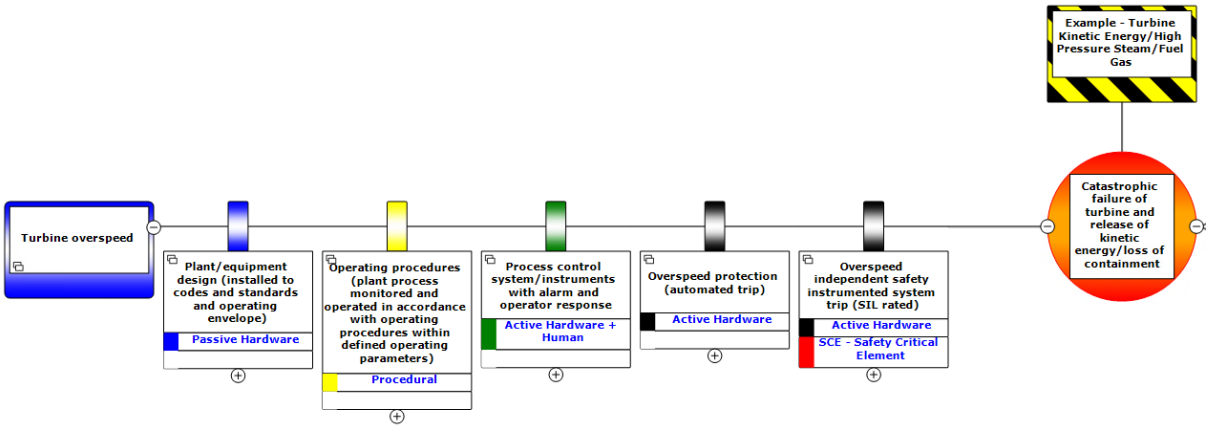
Step	Action	Notes
6	Develop a major incident bowtie diagram for each station major incident scenario	- Station major incident bowtie diagrams should be aligned with the station Major Incident Hazard Register. - Major incident bowtie diagrams should only include prevention control measures/barriers that 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.
7	Remove degradation factors and controls from each bowtie diagram initiating hazard/event's prevention control/barriers for which they do not meet the requirement of a prevention control/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. - Degradation factors and controls are dependent on the initiating hazard/event

Old Bowtie Turbine Overspeed Threat Line

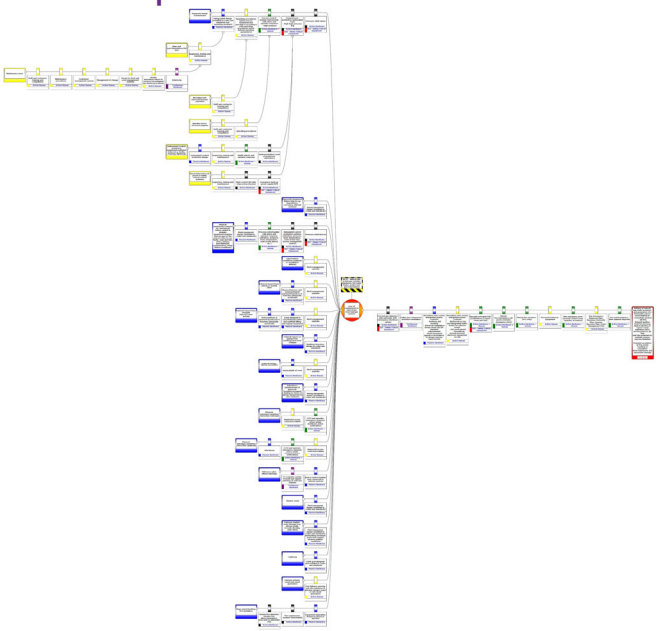


- **Too many barriers that are not independent, degradation controls**
- **False sense of protection**
- **Not intuitively ordered in time sequence of effect**

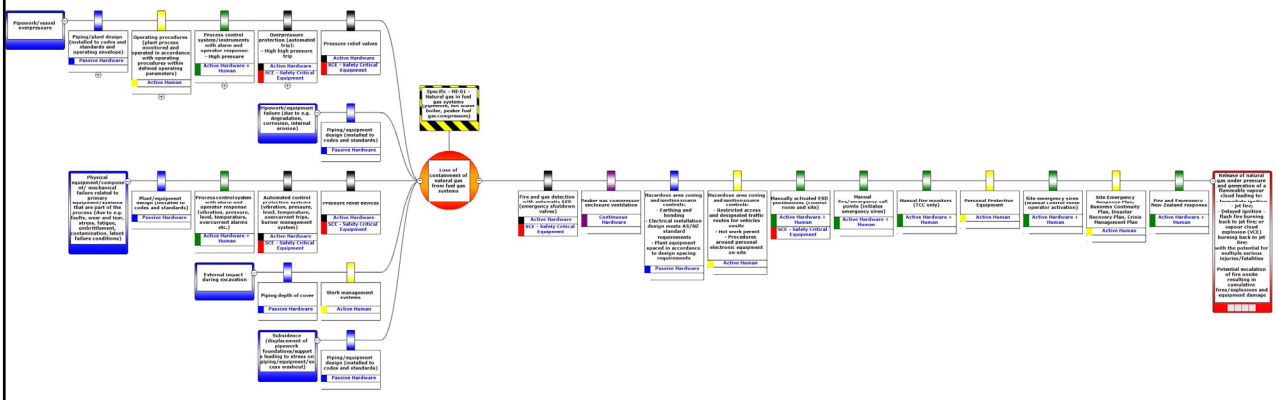
Basic Representation of Turbine Overspeed Threat Line using new standard (example)



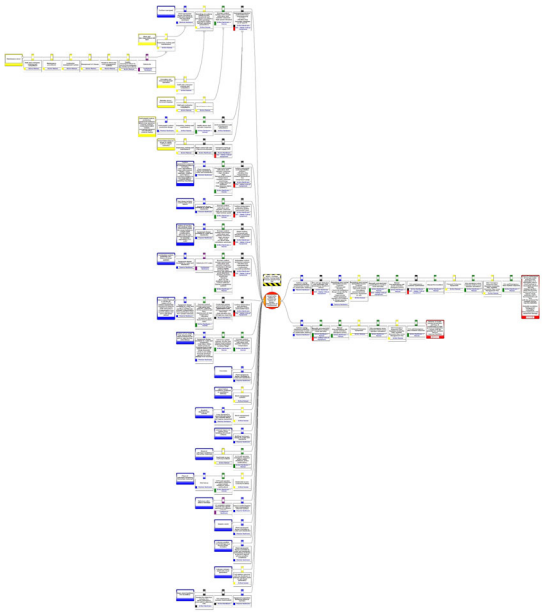
Examples of Bowties- Fuel Gas



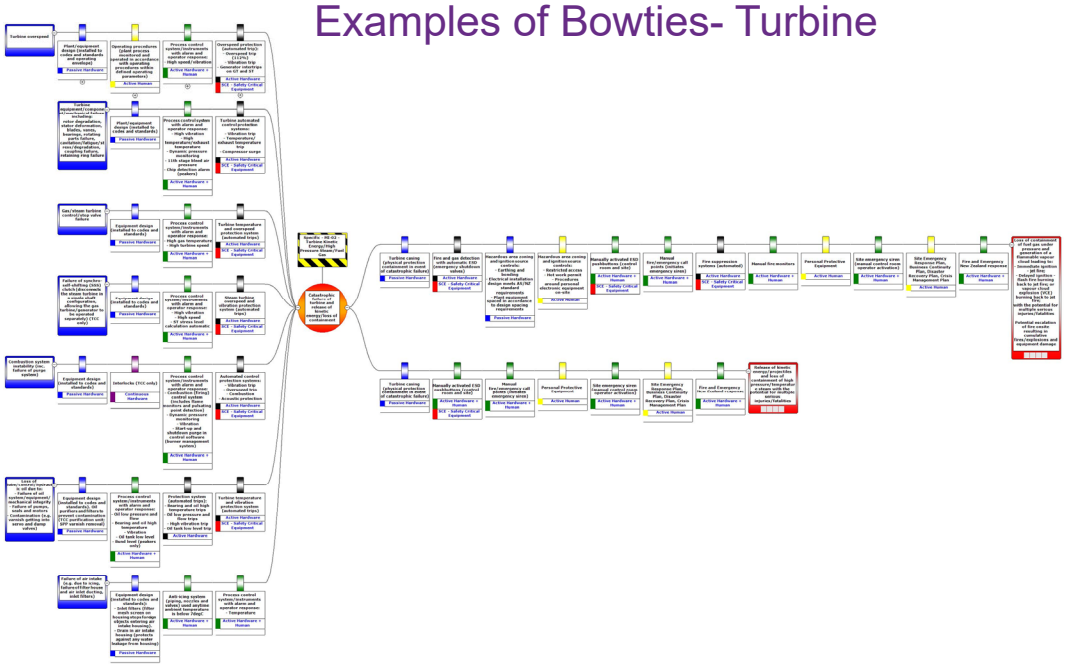
Examples of Bowties- Fuel Gas



Examples of Bowties- Turbine

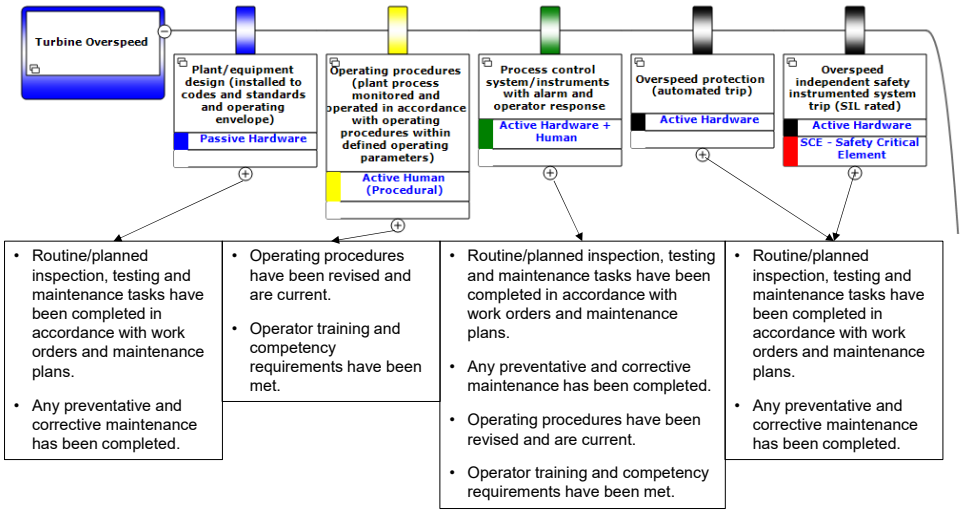


Examples of Bowties- Turbine



Bowtie Reviews

- Review is carried out against a screening check sheet containing a list of prompts for SMEs to determine barrier effectiveness (effective, partially effective, ineffective).
- Review of the Bowties are incorporated into the annual Plant Status Review.
- Condition Assessment Sheet orange and red barriers are discussed and determined if action is required within the next year or not (if not, it is deemed an accepted condition).
- Full Major Incident Hazard Register and Bowtie review to be carried out every 5 years for MHF or 10 years for all other stations.



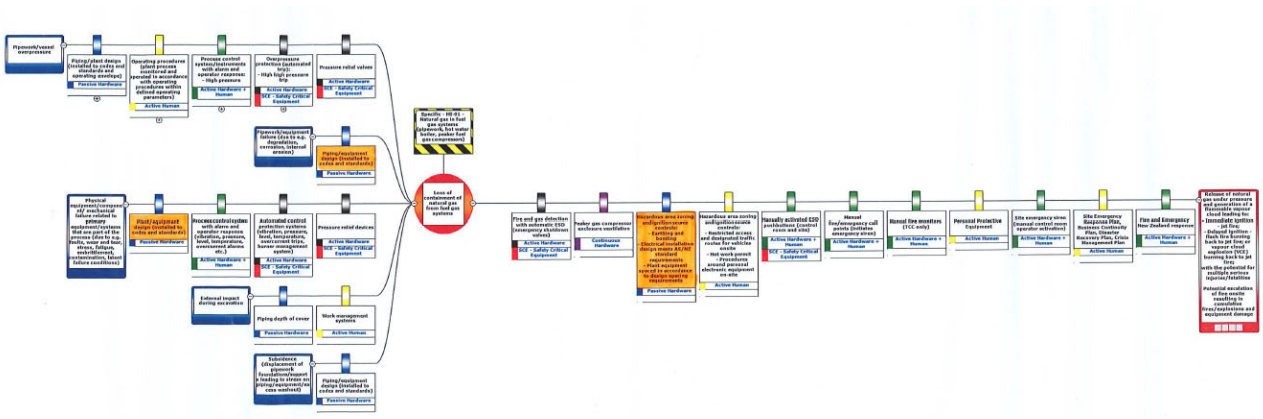
Bowtie and Threat Line Review Check Sheet (example)

MH-01 Catastrophic failure of Turbine and release of kinetic energy/ loss of containment					
Overall Bowtie Review Items					
	Owner	**Review**	**Things to Check**	**Barrier Effectiveness (E, PE, IE)**	**Comments**
	Asset Manager	GT Maintenance Plans in place and being carried out	KPI Dashboard for MP		
	Operations Supervisor	Operator Competencies	GT Specific Competencies Alarm Response		
		Operating Procedures for GT	SAP DMS (no overdue reviews)		
		Permit to Work System	Safety Rules Audit		
Threats					
Threat	**Owner**	**Review**	**Things to Check**	**Barrier Effectiveness (E, PE, IE)**	**Comments**
Overspeed	C&I SME	Overspeed Maintenance Plan	Completed on time Checksheets filled out		
		Overspeed Procedure	Up-to-date SAP DMS (no overdue reviews)		
		Instrumentation (specific)	Calibrations completed No outstanding maintenance		
		UPS operations	Health alarm on DCS		
Turbine Equipment Failure	Mechanical SME	GT Equipment maintained (specific)	Operational hours acceptable Inspections carried out		
		Control system operational	Trip testing carried out		
Corrosion	Mechanical SME	Inspection carried out	Maintenance plans complete Daily walkdowns and visual inspections		
External Impact	Asset Manager	Cranage Contractor	Any non conformances? Spot checks of equipment carried out		
		Lifting Procedures	Any non conformances? SAP DMS (no overdue reviews)		
Physical Sabotage/ terrorism	Asset Manager	Fence	Maintenance Plans complete		
		Cameras	All operational? Any maintenance carried out		
		Site Security	Gallagher system operational Any issues of system failures?		
Seismic Event	Asset Manager	Inspections and maintenance	Any areas where Maintenance plans not being carried out? Civil inspections completed		

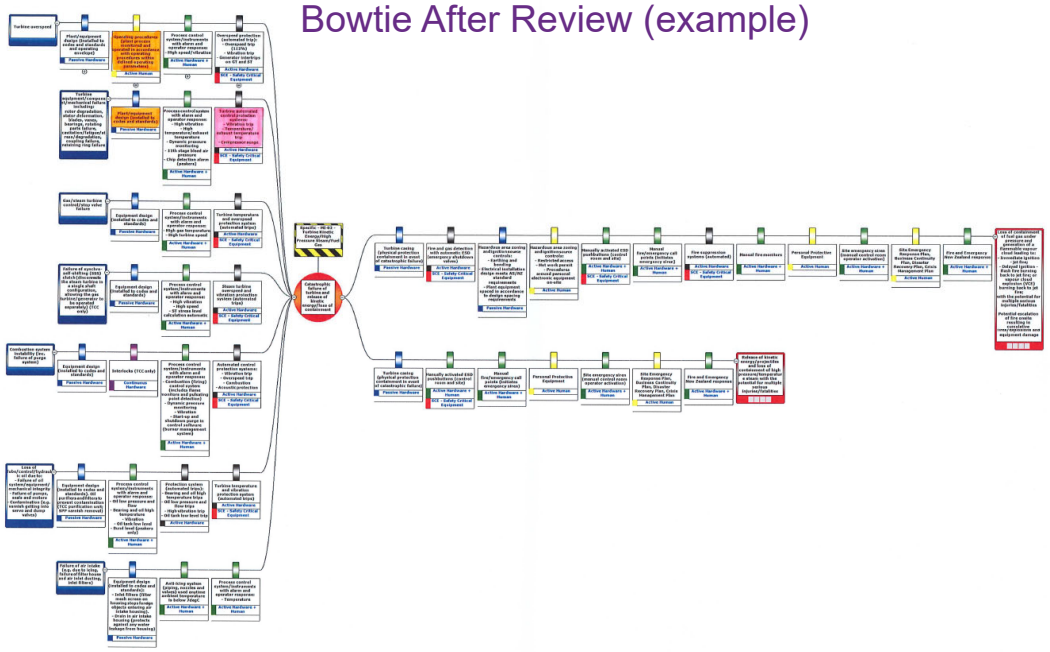
Bowtie and Threat Line Review Check Sheet (example)

MI-02 - Catastrophic failure of turbine (steam and gas) and release of kinetic energy/loss of containment of high pressure steam or fuel gas					
Overall Bowtie Review Items					
	Owner	**Review Item**	**Considerations**	**Barrier Condition Assessment (Red, Amber, Green)***	**Comments**
	Engineering Lead	HGP parts life management Life extension hours (TCC Only)	Review operating hours vs required maintenance Operating house remaining?		
		Equipment/plant design	Any issues with equipment/plant design? Applicable codes and standards are met? Turbine routine/planned inspection, testing and maintenance tasks have been completed in accordance with work orders and maintenance plans (any issues)? Preventative and corrective maintenance has been completed/on-time? Deferred maintenance or assurance activities		
		Spare Parts	Do we have sufficient spares? (any issues)		TCC- Limited spares available for TCC and EOL
		GT maintenance	Boroscopes and surveys carried out		
	C&I SME	Instrumentation and protection systems	Turbine instrumentation testing and calibrations completed (any issues)? Preventative/corrective maintenance tasks completed/on-time? Deferred maintenance or assurance activities Health alarms		Overspeed system issues
	Operations Supervisor	Procedures	Turbine operation procedures have been reviewed and are current and accurate? Any modifications that may impact existing procedures? Any new procedures required?		Peaker overspeed procedure potentially required? Does this require a physical overspeed or not?
		Competency	Turbine operations staff competencies are up-to-date and refresher training completed?		
		Alarm management	Turbine standing/ shelved alarms		
		System operability	Any operator concerns with turbines		
Specific Threat Review Items					
Threat	**Owner**	**Review Item**	**Considerations**	**Barrier Condition Assessment (Red, Amber, Green)***	**Comments**
Overspeed	Mechanical SME	Condition	Any issues with turbine/equipment condition?		
	C&I SME	Instrumentation and protection systems	Overspeed, vibration, generator intertrip instrumentation testing and calibrations completed (any issues)?		
		Overspeed Maintenance Plan	Completed on time Checksheets filled out		Peakers- Overspeed procedure to be reviewed. Physical overspeed test? (Same as above)
		Steam turbine admission valves	Fortnightly testing completed (any issues)? Other valves monthly (any issues)?		
Turbine equipment/component/mechanical failure	Engineering Lead	Engineering advice	Operational hours acceptable Inspections and conditions of EANs met?		
	Mechanical SME	Condition	Any issues with plant/equipment condition/degradation? Casing condition? (mitigation) Corrosion		TCC- Have we assessed the bearing foundations and pedestals etc associated with the turbine vibration
		Inspection and maintenance	Maintenance and inspections carried out (any issues)? Inc. air intake filter replacement, HGP inspection, thermography.		

Bowtie After Review (example)



Bowtie After Review (example)



Key Lessons

- Start small, don't try to solve the world's problems before you have taken the first small step!!
- Industry standard guidance is that bowties should remain qualitative.
- Be clear about your processes.
- Set up the process to be easy and straightforward for the users. May take a bit more effort to begin with but helps to foster engagement in the process longer term.
- Actions- keep any actions/ improvements that come out of these processes achievable and don't overcommit to completing too many actions