Beyond the PHA

Major Hazard Management for Battery Energy Storage Systems Using Bowtie Analysis

Michela Leedow

Hazards, Concurrent Session 5B - Emerging Technologies

Wednesday, 30 September 2026

R4Risk

L14, 222 Kings Way
(PO Box 5023)
SOUTH MELBOURNE VIC 3205

P: (03) 9268 9700
E: solutions@r4risk.com.au
www.r4risk.com.au

Beyond the Preliminary Hazard Analysis: Agenda

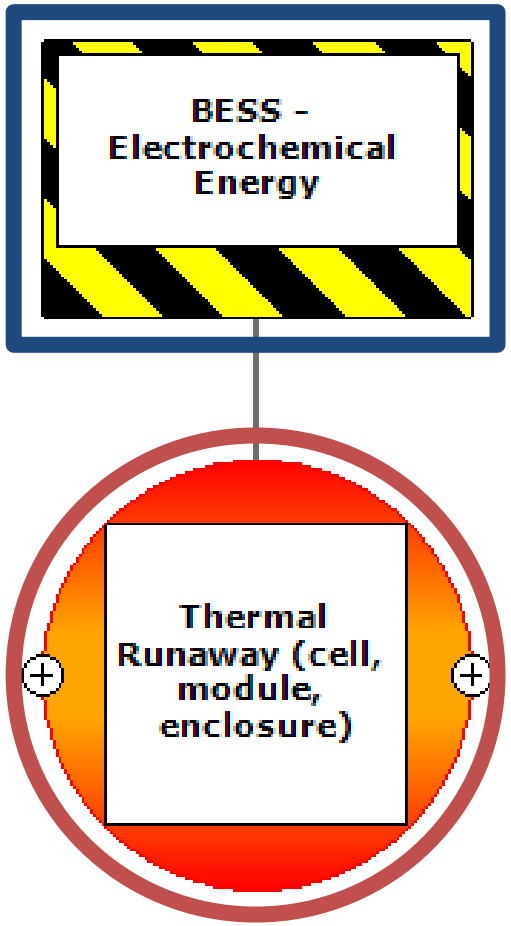
1. Bowtie analysis for a Battery Energy Storage System (BESS)
2. What does the bowtie reveal about the controls?
3. Safety management systems supporting control performance
4. Operational challenges



BOWTIE ANALYSIS FOR A BESS DEVELOPED FROM A PHA



Hazard, Top Event and Scope



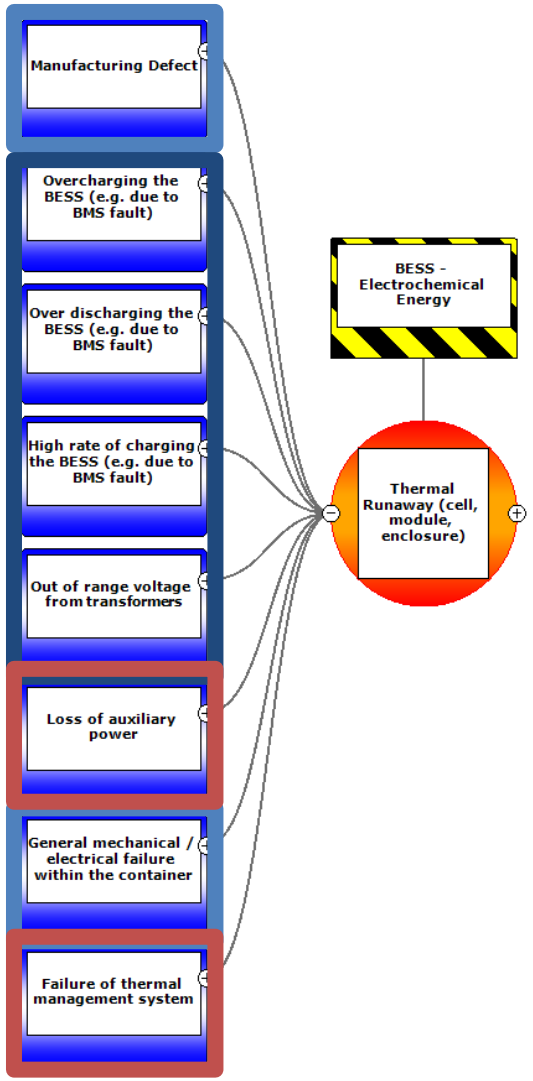
Scope: Large-scale, containerised BESS, lithium-ion technology

Hazard: Stored electrical and chemical energy

Top event: Thermal runaway at any level – cell, module, rack or container

Representative bowtie developed from multiple BESS PHAs

Causes: Asset failures



Battery defects

- Internal or manufacturing defects
- Mechanical damage or electrical failures

Operational issues

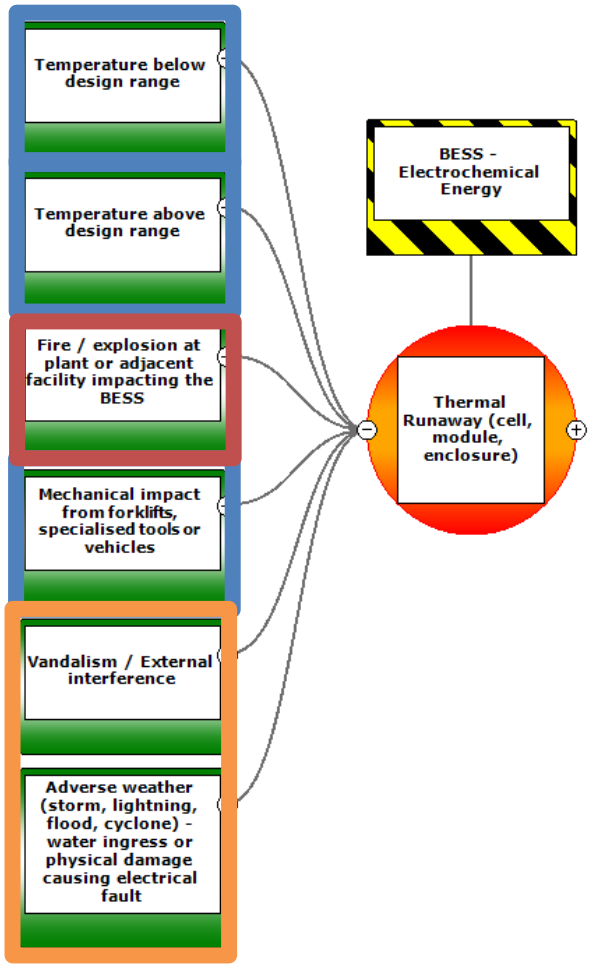
- Overcharging or over-discharging
- High rate of charge
- Out-of-range voltage

Support system failures

- Loss of power
- Loss of thermal management

Each of these degrades battery performance and can initiate thermal runaway

Causes: External Events



Environment and operations

- High or low ambient conditions
- Mechanical impact – forklift, vehicle or aircraft

Deliberate acts and extreme weather

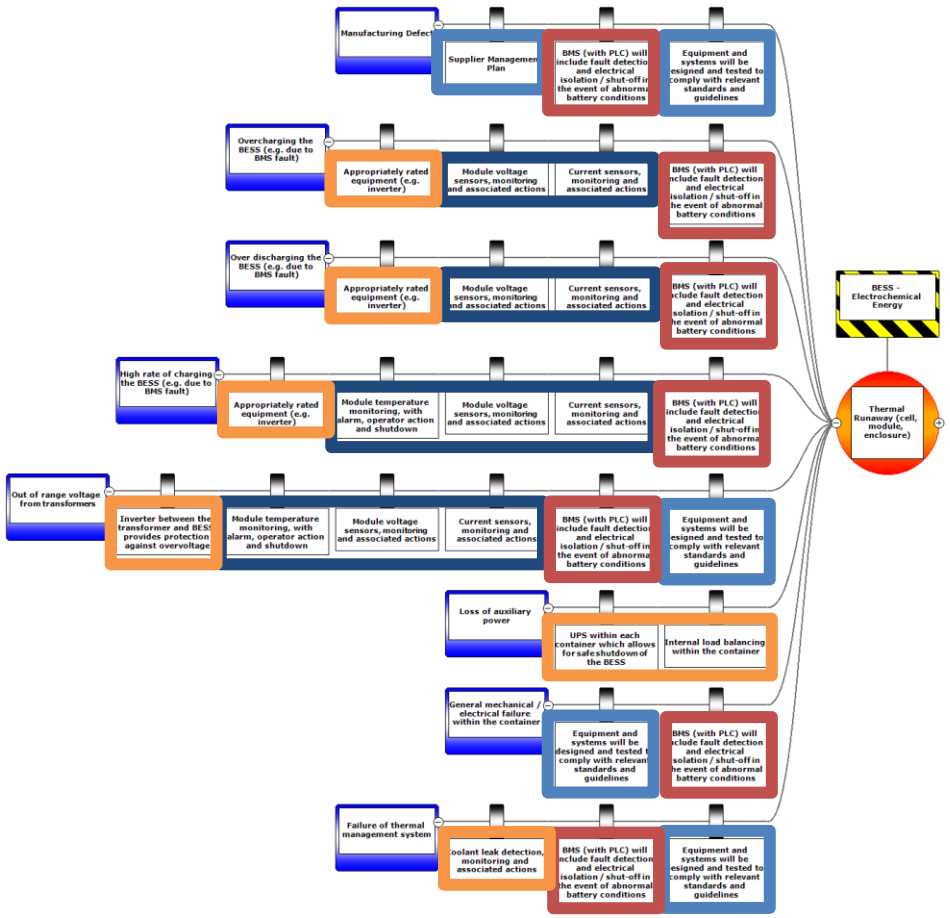
- Vandalism or interference
- Adverse events causing shorting of the system

Adjacent fire or explosion

- Fire in an adjacent container
- Transformer fire or explosion
- Neighbouring facility fire or bushfire

External events act on the BESS from outside the battery system
Siting and separation matter

Preventative Controls: Asset Failures



Proven design and supply

- Known, proven supplier with quality assurance
- Equipment design validated by full-scale fire testing

Monitoring critical parameters

- Current, voltage and temperature
- State of charge

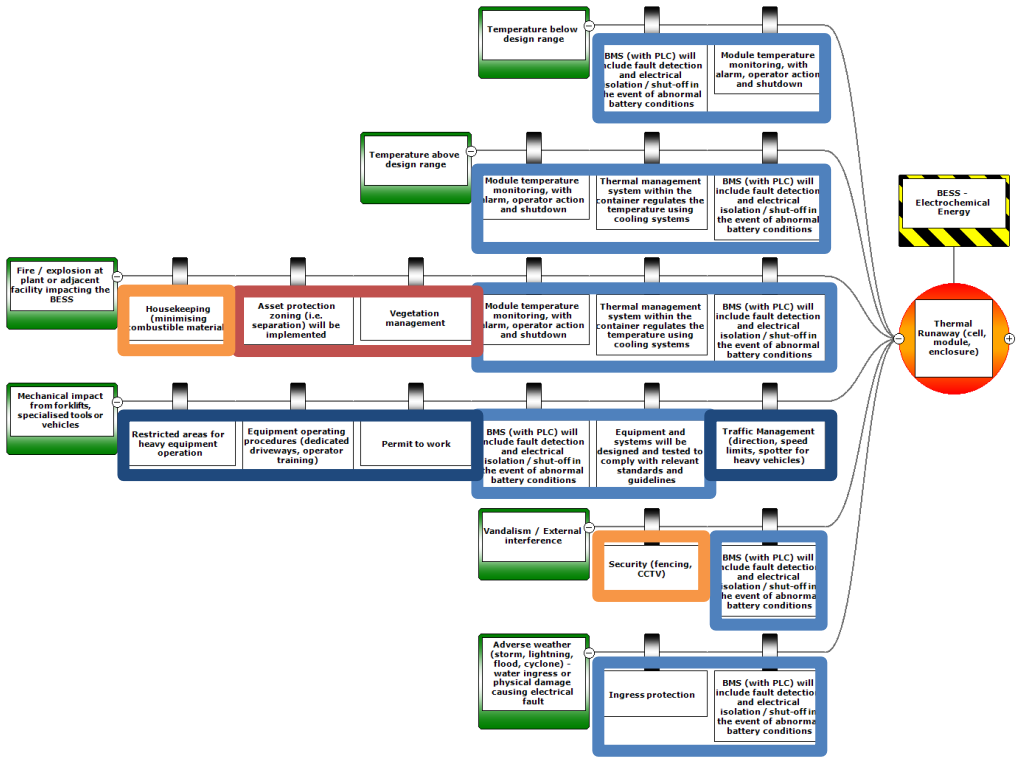
Battery management system

- Detects faults and isolates the system

Supporting engineered controls

- Thermal management (coolant leak detection)
- Uninterruptible power supply
- Inverter design and rating
- Load balancing

Preventative Controls: External Events



Design and monitoring still applies

- BMS and parameter monitoring remain relevant
- Design features

Procedures and permits

- Permit to work – lifting, excavation, isolation, electrical access
- Traffic management

Site and surrounds

- Asset protection zones
- Vegetation management

Continuous activities

- Housekeeping
- Security

Consequences of Thermal Runaway

Fire and explosion

- Accumulated gas finding an ignition source
  - Vent fire, or deflagration within the container

Toxic gas

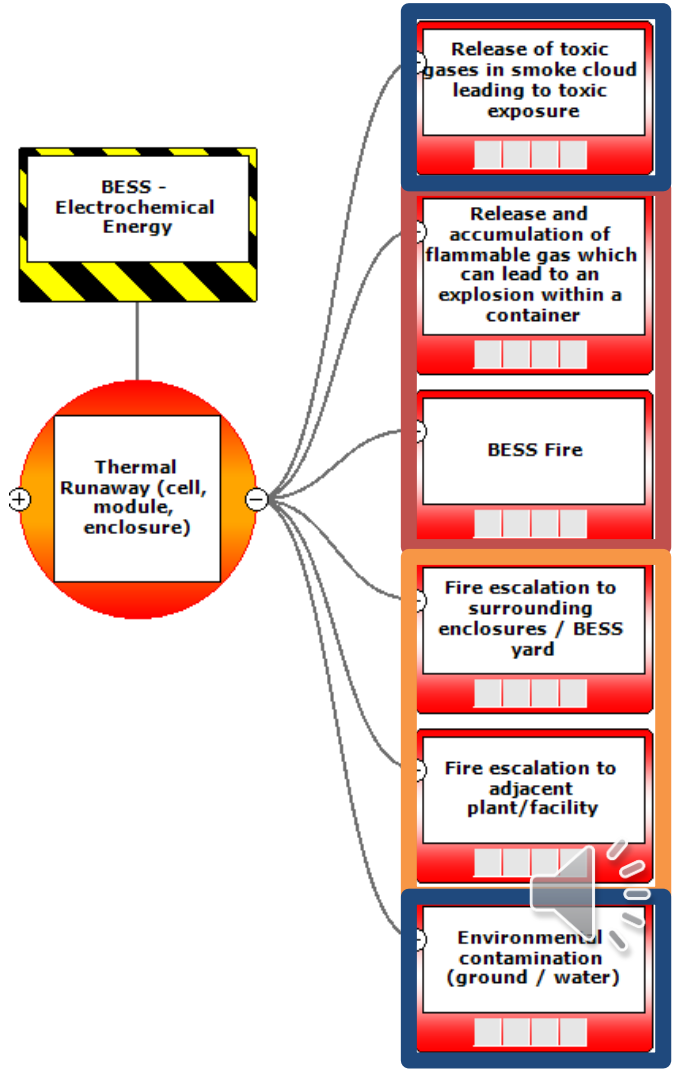
- Toxic gas exposure, irritation and health effects

Escalation

- Adjacent battery enclosure, transformer, adjacent facilities or environment

Environment

- Contaminated firewater affecting soil, stormwater or groundwater



Mitigative Controls

Detect, isolate and shut down

- Gas, smoke and heat detection, with a way to isolate the container or facility

Manage flammable accumulation

- Emergency ventilation and deflagration panels to reduce gas accumulation and limit explosion effects

Limit escalation

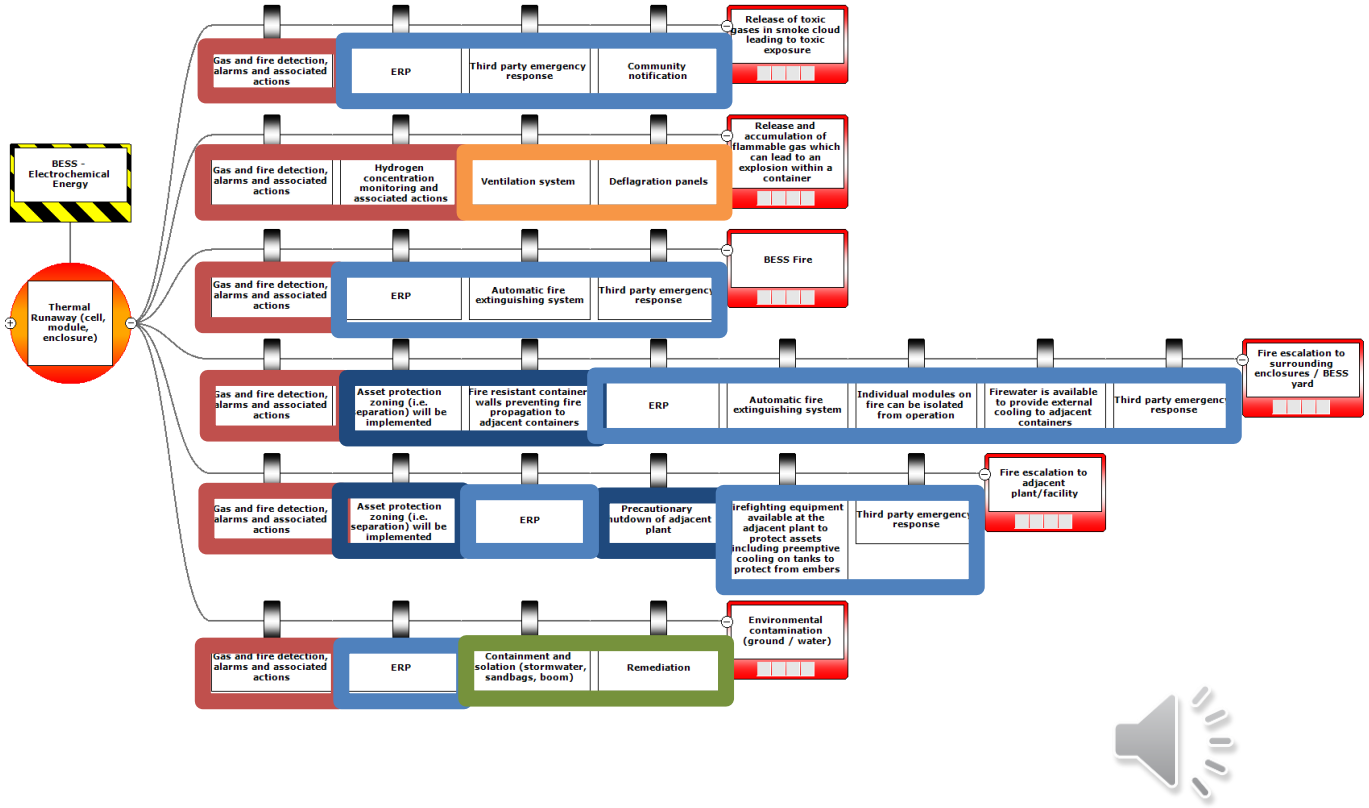
- Separation distances, materials of construction, asset protection zoning, cooling water and firefighting equipment

Emergency response

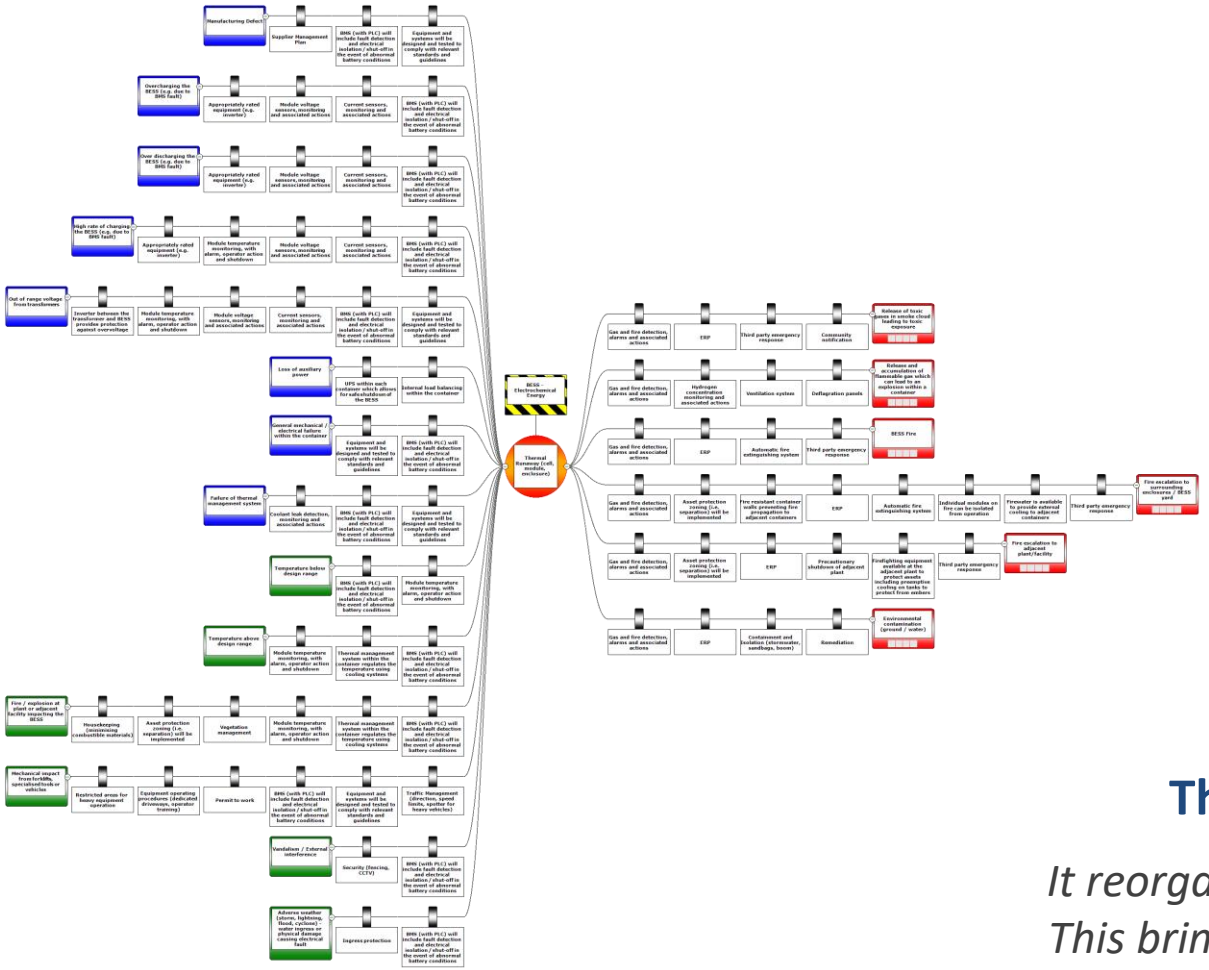
- Facility personnel response, role of emergency responders, evacuation, notification and communication systems

Protect the environment

- Containment on site where possible, followed by remediation as required



Completed Bowtie



Where a well-conducted PHA brings us:

- **Credible initiating events identified**
- **Consequences considered**
- **Safeguards nominated**
- **Standards and design requirements applied**

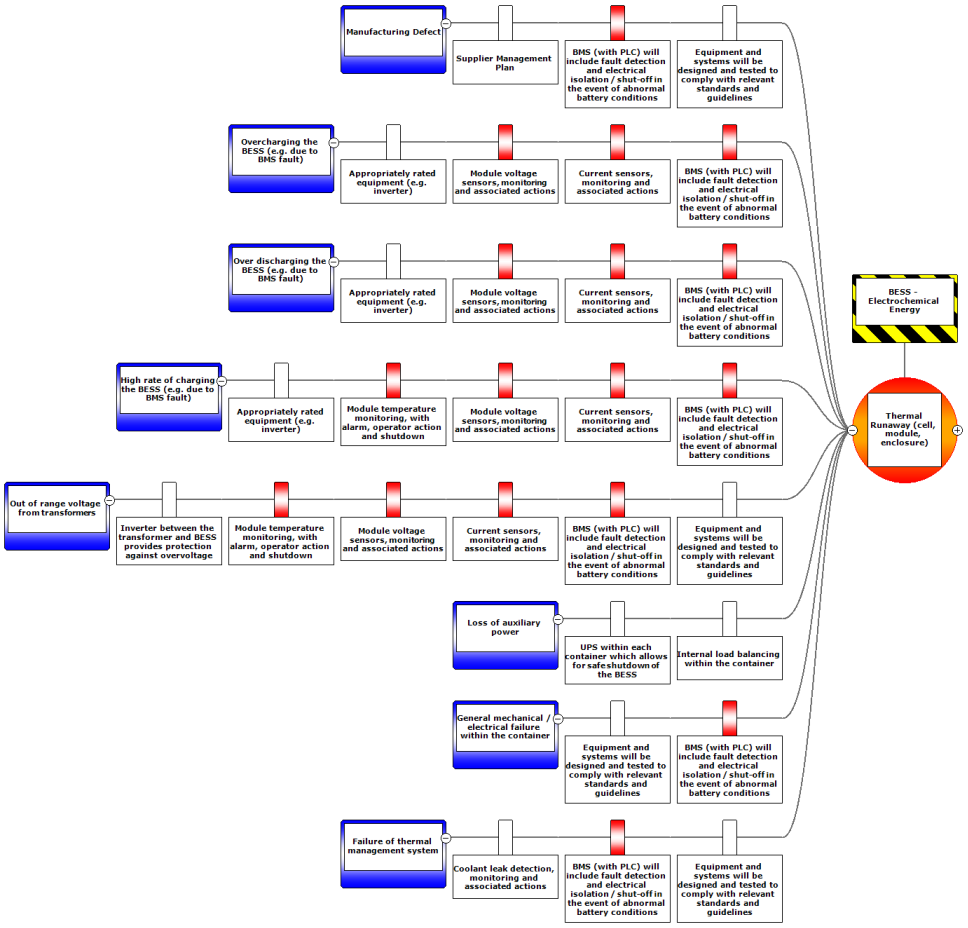
The bowtie analysis does not replace that work

It reorganises the outputs so the entire control set can be examined. This brings the scenarios together and reveals less obvious patterns, one initiating event at a time.

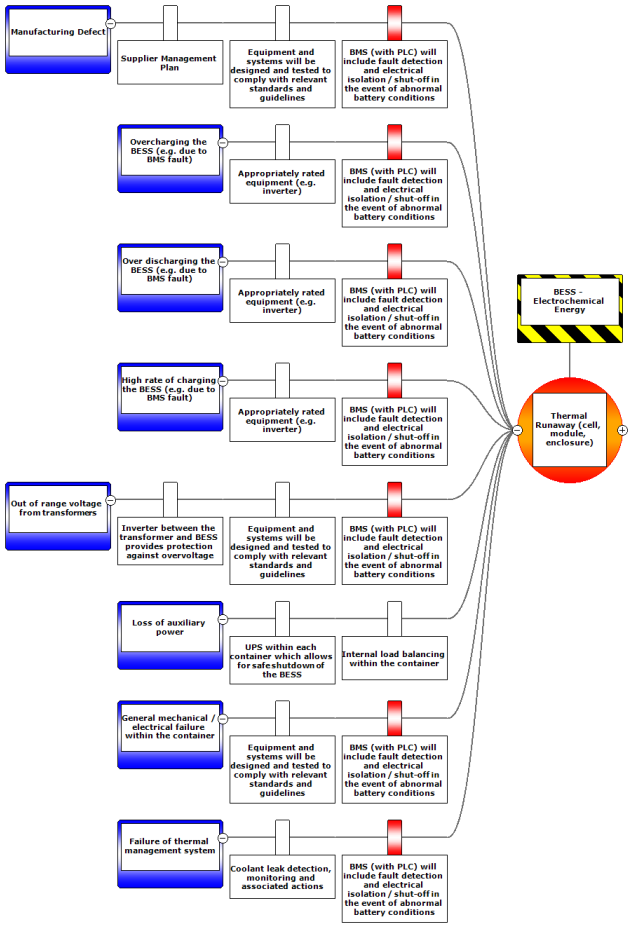
WHAT DOES THE BOWTIE REVEAL ABOUT THE CONTROLS?



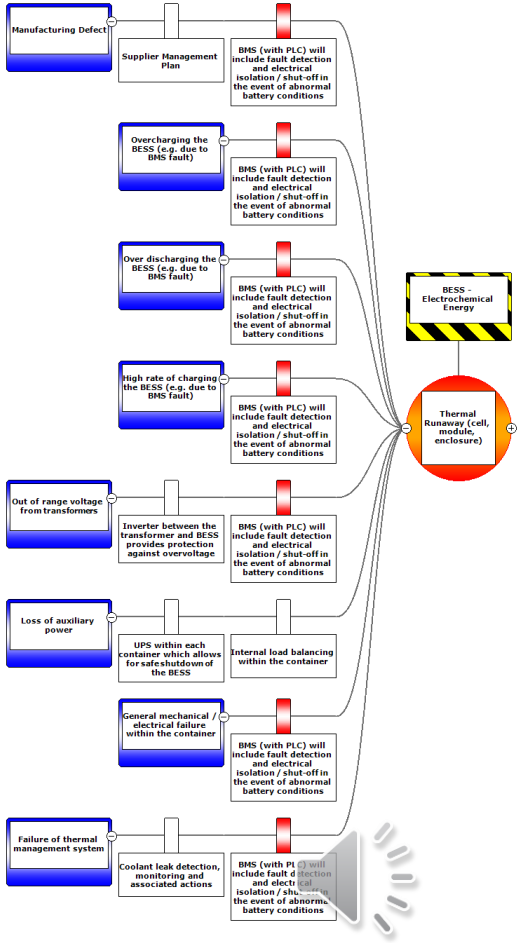
BMS Dependency and Criticality



1. Sensors and BMS shown separately – current, voltage, temperature, rate etc.



2. BMS simplified as one control



3. Focusing on the operational controls

SAFETY MANAGEMENT SYSTEMS SUPPORTING CONTROL PERFORMANCE



Supporting Critical Controls

Energy Institute – Process Safety Management Framework

Process safety leadership	Risk identification and assessment	Risk management	Review and improvement
1. Leadership, commitment and responsibility 2. Identification and compliance with legislation and industry standards 3. Employee selection, placement and competency and health assurance 4. Workforce involvement 5. Communication with stakeholders	6. Hazard identification and risk assessment 7. Documentation, records and knowledge management	8. Operating manuals and procedures 9. Process and operational status monitoring and handover 10. Management of operational interfaces 11. Standards and practices 12. Management of change and project management 13. Operational readiness and process start-up 14. Emergency preparedness 15. Inspection, maintenance and asset integrity 16. Management of safety critical devices 17. Work control, permit-to-work and task risk assessment 18. Contractor and supplier, selection and management	19. Incident reporting and investigation 20. Audit, assurance, management review and intervention

BMS: Defining Control Performance

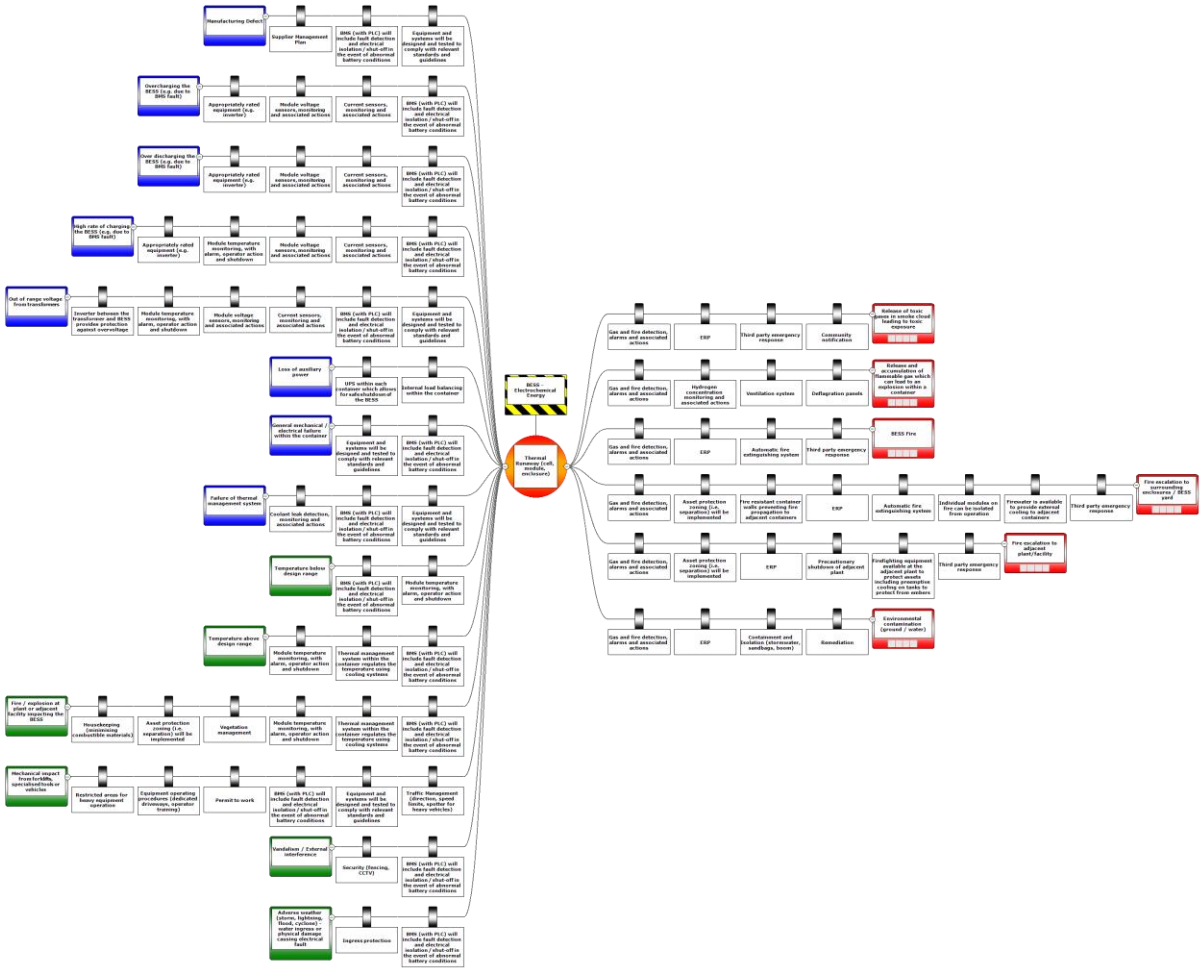
System Expectation / Performance	Performance Measure			
	Task/Activities	Measurable	Performance Target (Range)	Intervention
BMS detects an excursion beyond the safe operating envelope and safely shuts down the battery (cell, module, enclosure)	Function test of sensors against set points: current, voltage, cell and module temperature, rate of charge / discharge, state of charge	Measurement testing completed on time, late or outstanding	100% of tests completed on time Zero tests outstanding > 30 days	Report overdue testing to the management team; assess continued operation until testing is complete
	Proof test of protective trip and isolation function (cell, module, enclosure)	Number of failures on demand Pass / fail against design set points	Zero failures on demand Trip and isolation within design set points	Investigate failure; restrict charge rate or isolate the affected unit until rectified
BMS equipment is available and in good condition	Visual inspection of BMS cabinets, sensors, wiring and connections	Inspections completed to schedule Number of detected issues	100% of inspections completed to schedule Zero critical defects open > 14 days	Raise work order and prioritise critical defects; escalate if resources are not available
	Fault review and close-out of BMS alarms and detected issues	Number of actions open and closed Repeat or recurring faults	Zero overdue critical actions Downward trend in repeat faults	Review trend at monthly operations meeting; investigate recurring faults
Redundancy and support systems keep the BMS effective	Critical spares held (sensors, BMS modules, contactors); backup power and communications tested	Spares availability Backup power test result	≥ 95% of critical spares in stock Backup power test passed each quarter	Expedite procurement; apply temporary operating restrictions until redundancy is restored

Illustrative example only. Set points, test frequencies and performance criteria would need to be determined specifically for the facility.

OPERATIONAL CHALLENGES



Technology Change



Does the change alter the bowtie?

CAUSES

- Does the replacement introduce a new initiating cause?
- Does it change the operating envelope or duty?

CONTROLS

- Can the BMS recognise, balance and protect it?
- Are the alarm and trip settings, electrical and charging assumptions still valid?

CONSEQUENCES

- Does fire testing and consequence modelling still represent the configuration?
- Could the scale or nature of consequences change?

Operating Model

Can the operating model support the credited controls?

PREVENTATIVE SIDE – PEOPLE-DEPENDENT

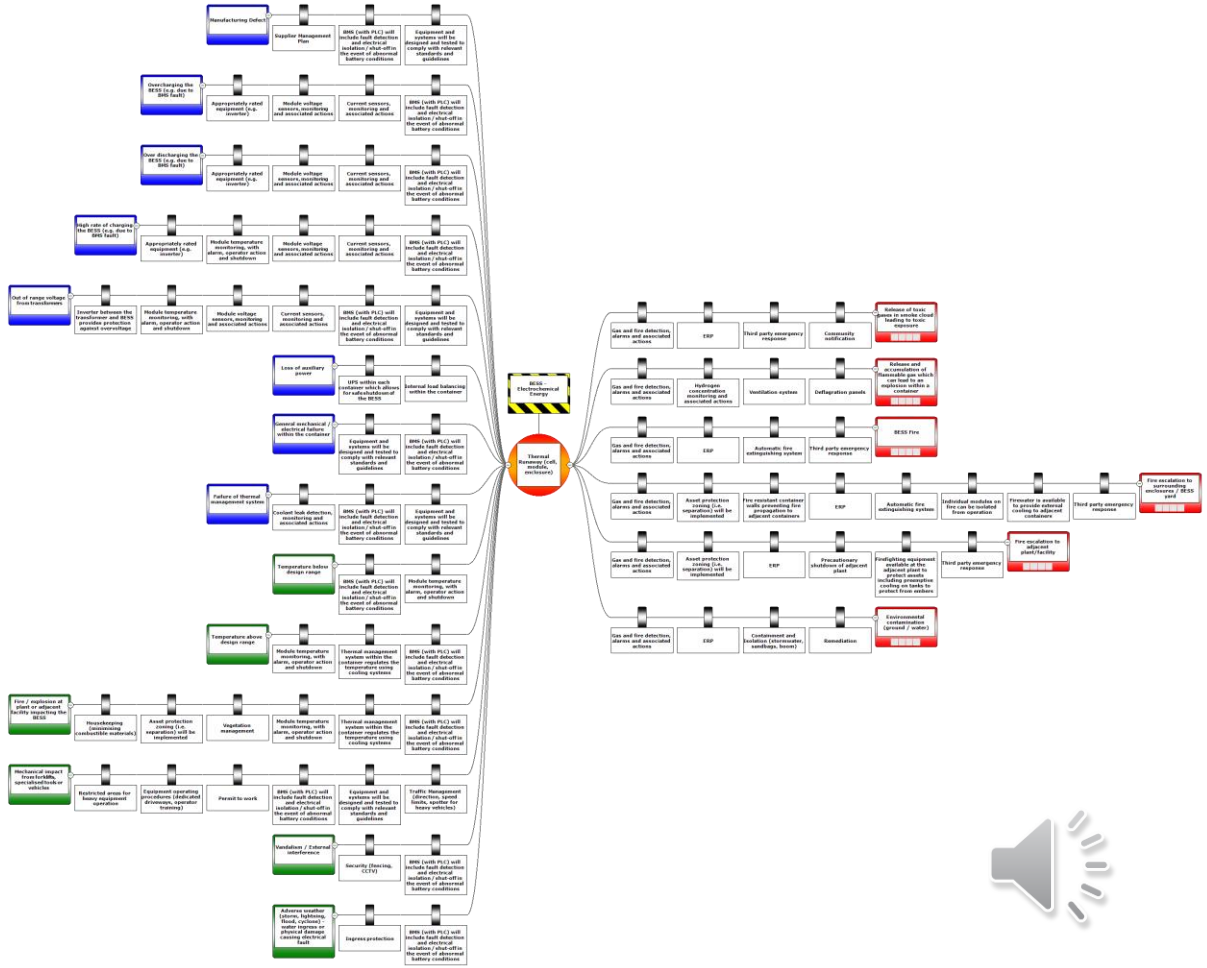
- Inspection, housekeeping, vegetation management, security, permit to work
- Who performs it, how often and with what site knowledge – and what happens if it is unavailable?

MITIGATIVE SIDE – EMERGENCY RESPONSE

- Detection may be automatic; isolation, attendance and notification are not
- Remote response or site attendance? What if telemetry or communications fail?

SUPPORTING ARRANGEMENTS

- Attendance frequency and scope set by the controls needing local presence
- Training, procedures, pre-incident plans, drills, labelling, intuitive displays



Conclusion

1

PHA SETS THE BASIS

A good PHA establishes the hazard, consequence and initial control basis.

2

BOWTIE ANALYSIS REVEALS CRITICAL CONTROLS

Examines the control picture as a whole and shows where focus is required during operation.

3

SMS SUSTAINS PERFORMANCE

Provides a structure to support reliable control performance throughout operation.



Get in Touch



(03) 9268 9700

www.r4risk.com.au

solutions@r4risk.com.au