

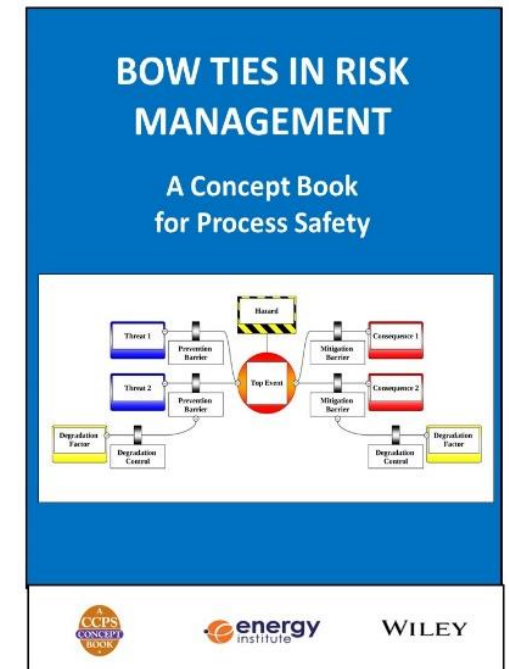
Bow Ties in Risk Management: A Concept Book for Process Safety – Webinar

25th October 2018

Paul McCulloch

Process Safety Consultant

CGE Risk Management Solutions

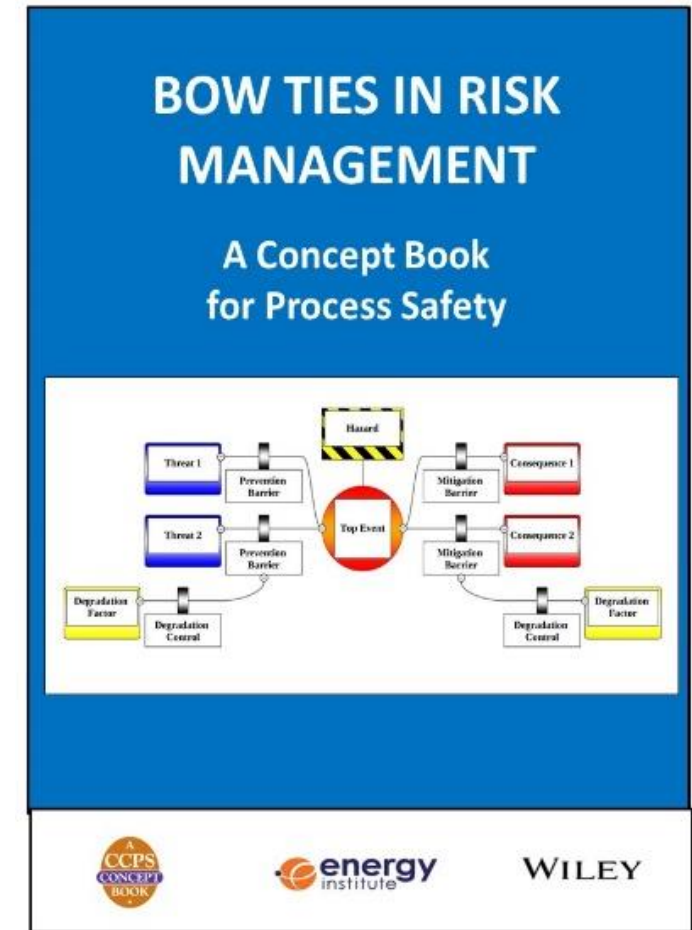


Webinar Agenda

- Introduction webinar
- Introduction CCPS/EI book
- Bowtie methodology in 8 steps (in BowTieXP) – use CCPS terminology
- CCPS specific subjects:
 - Human factors in bowties
 - Multi-level bowties
 - Different bowtie users
- Advanced barrier management subjects
- Live Q&A session with bowtie expert
- Obtain extended BowTieXP Advanced trial and CCPS/EI bowtie template

CCPS / Energy Institute Concept Book

- CCPS decided to develop a Concept Book to capture best practice and define a methodology for bow ties.
- Energy Institute joined the project with a special emphasis on human factors
- “Bow Ties in Risk Management: A Concept Book for Process Safety”
- Proposes standardized bow tie terminology and definitions
- Explains how to:
 - Construct bow ties of high practical value, avoiding common pitfalls
 - Treat human and organizational factors in a sound and practical manner
 - Apply bow tie can be used to create high value organizational learning from incidents and audits
- Practical application and value of bow ties in plant management and active risk management, from the control room to the board room
- Based on current best barrier management knowledge and approaches
- Draws on a wealth of industry experience from well-known experts



Why a book?

- Confusion about who (and what) bow ties are for
- No generally accepted methodology and terminology
- Some typical problems with existing bow ties:
 - Structural errors: e.g. degradation controls shown as barriers
 - Lack of rigour in constructing bow tie elements:
 - Hazard or Top Event description vague, or confused with Consequence
 - Incomplete barriers: barrier elements listed as ‘the barrier’
 - Management System elements included as ‘barriers’
 - ‘Human and Organisational Factors’ confused and ineffective
 - Unfair criticism that bow ties over-simplify incident causation

“Well constructed bow ties, which are clear and enable easy communication, can give the impression that they are easy to create. This is not the case. Too often bow ties are created with structural or other errors which can significantly degrade their value.”



Hazard is an operational activity or materials with the potential to cause harm

“What you are trying to control”

Hazards should

Be specific

For the hazard in its controlled state

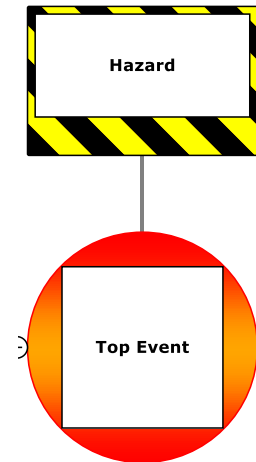
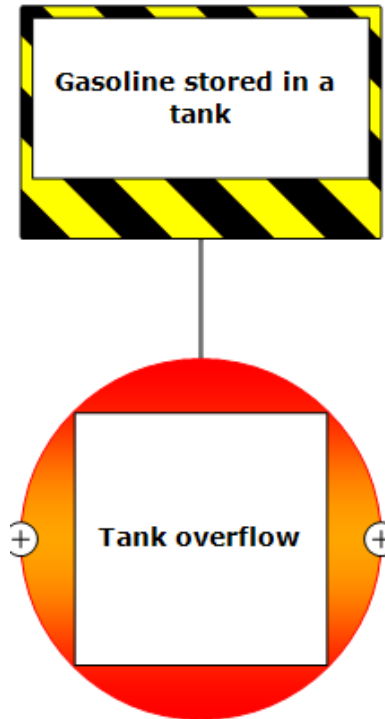
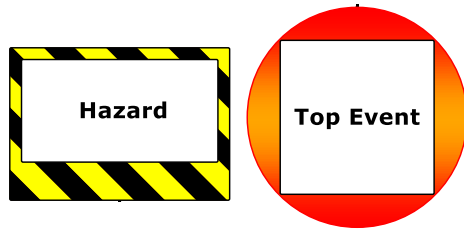
Can also include:

Situational context

Indication of scale

Not always possible to define all in the box – use description field





Top event is the moment when control over the hazard is lost releasing harmful potential

Top event

Describe how / what control is lost

Can give an indication of scale

(e.g. leak vs rupture)

Do not define as:

A threat (corrosion of the tank)

A consequence (e.g. tank overflow and major dike fire)

A barrier failure is not a top event



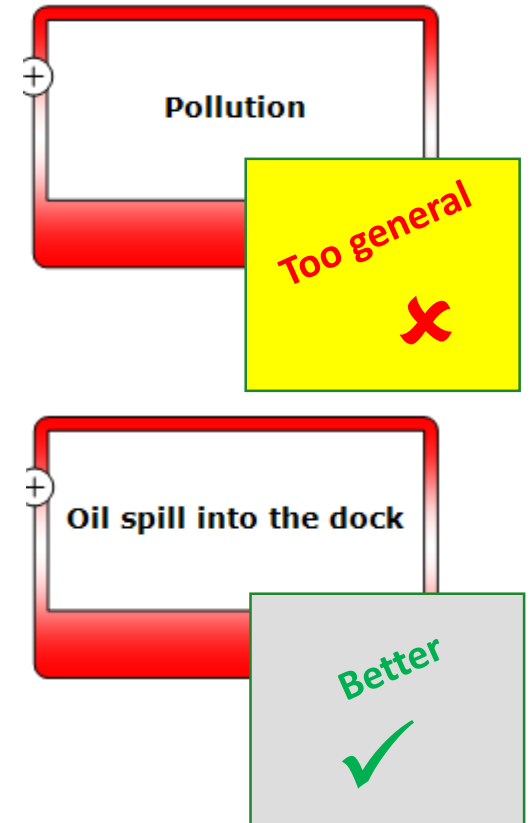
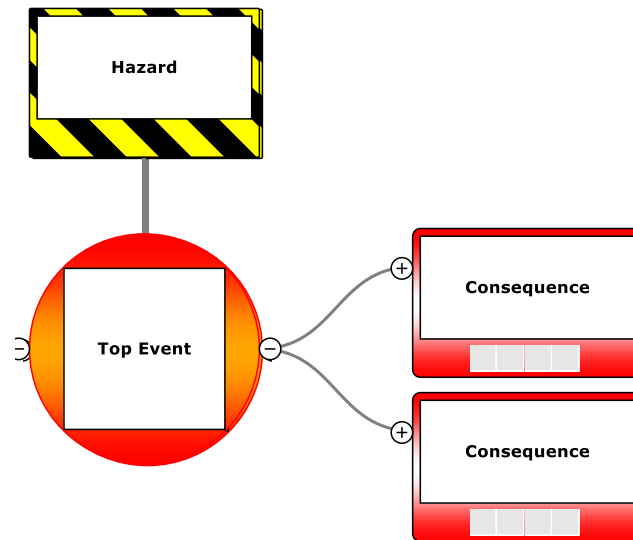
Consequences direct outcome of an accident sequence that results in harm ...

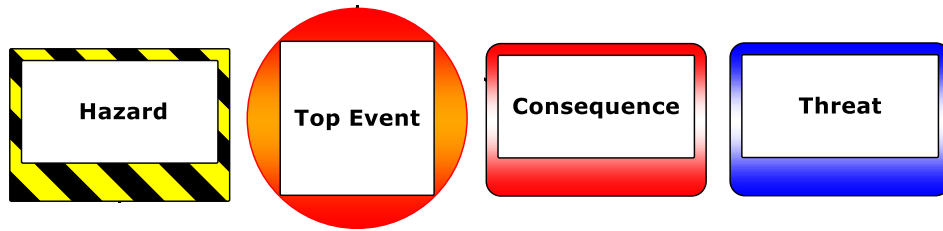
Recommend defining before “threats” – this can help ensure that threats defined are those that lead to the significant consequences

Should be defined as:

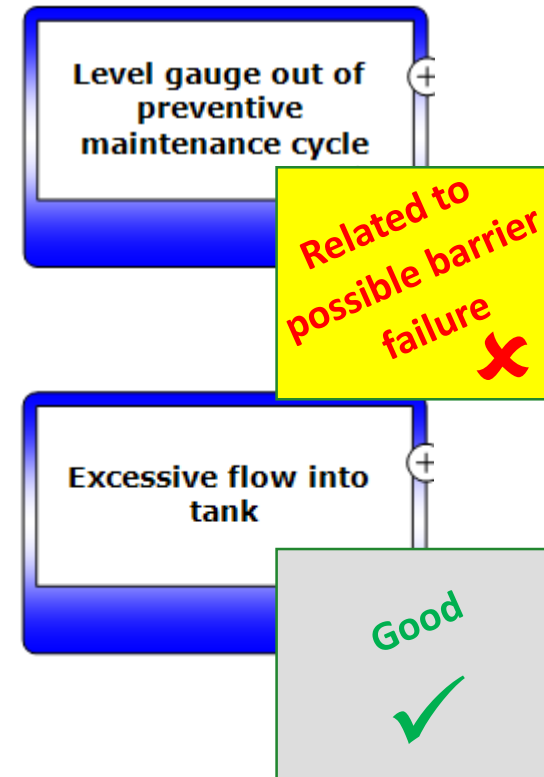
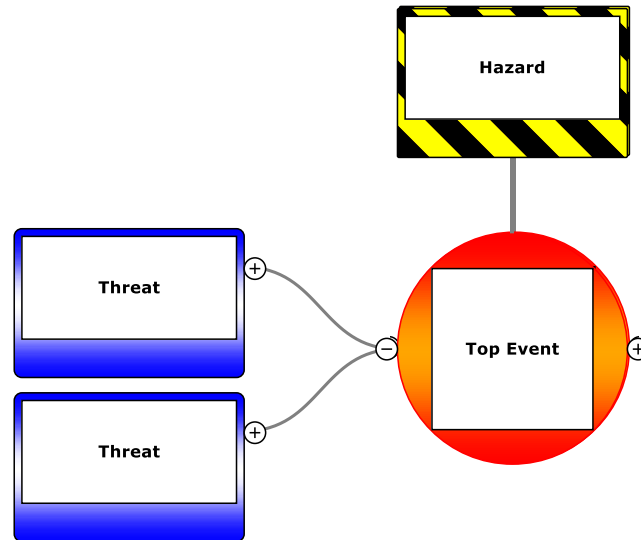
“Damage” due to “Event”, e.g. environmental damage due to liquid spill

Do not be too specific in defining the consequences (e.g. differentiating injury outcomes from fatality outcomes) as the barriers are likely to be the same and the number of branches is increased



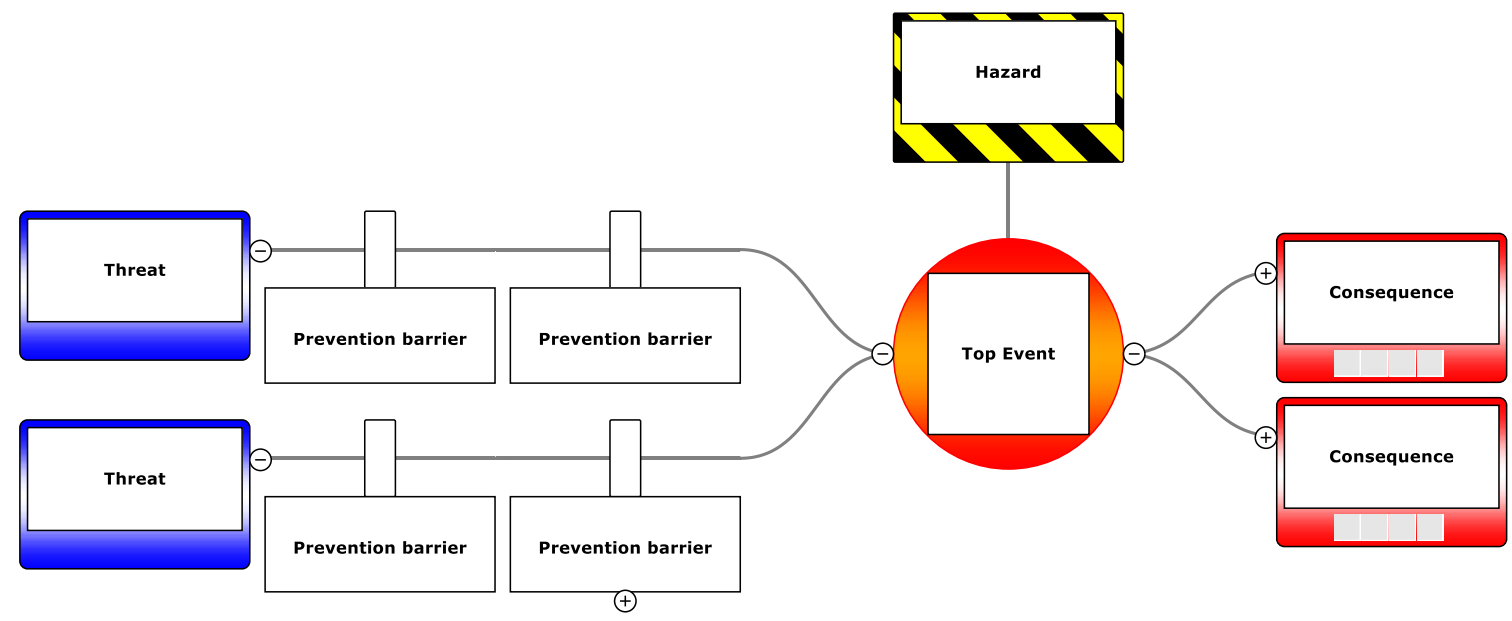


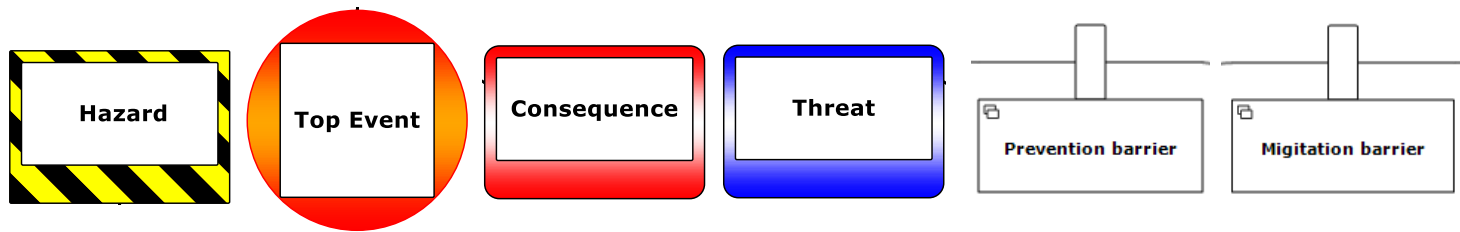
Threats initiating event that can potentially release a hazard and produce the top event
 Should be sufficient to lead to the top event by itself – be a *specific direct cause*
 Should be credible
 Should NOT be a barrier failure



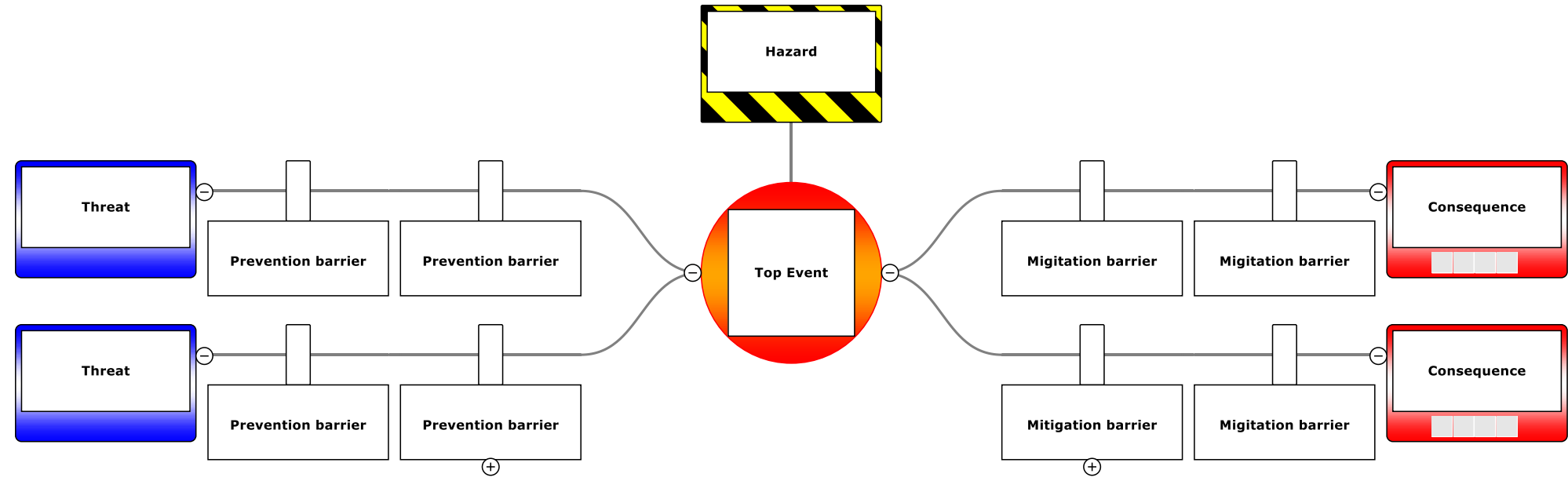


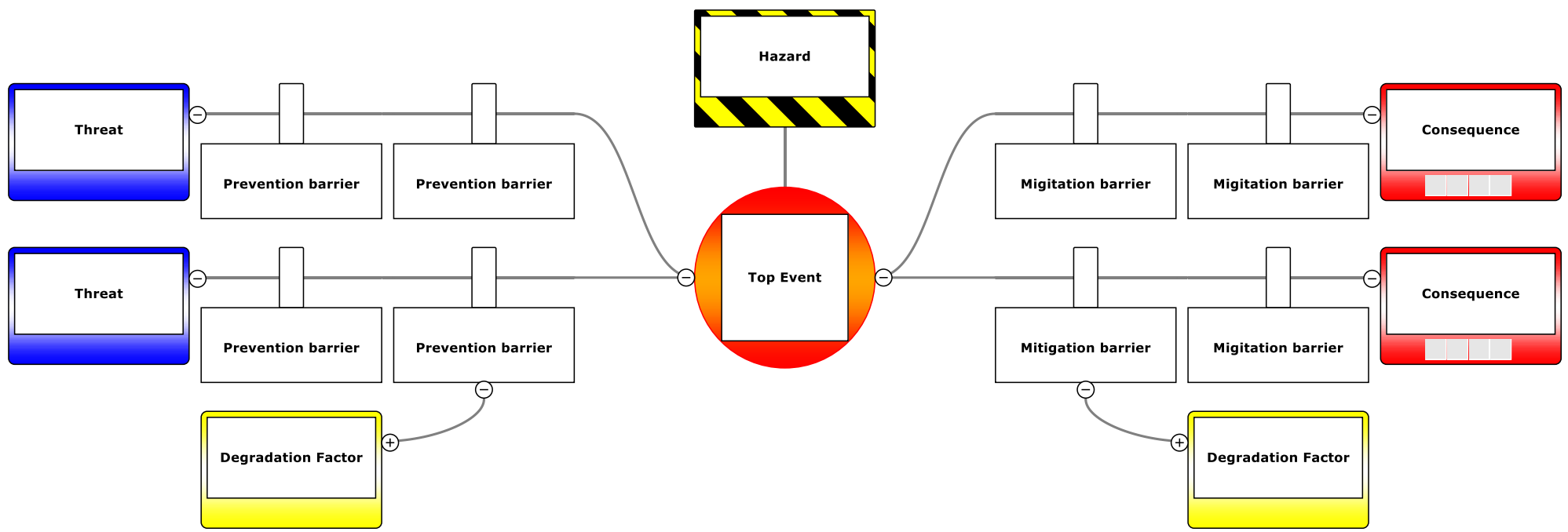
Prevention barrier is effective if it is capable on its own of preventing a threat developing into the top event

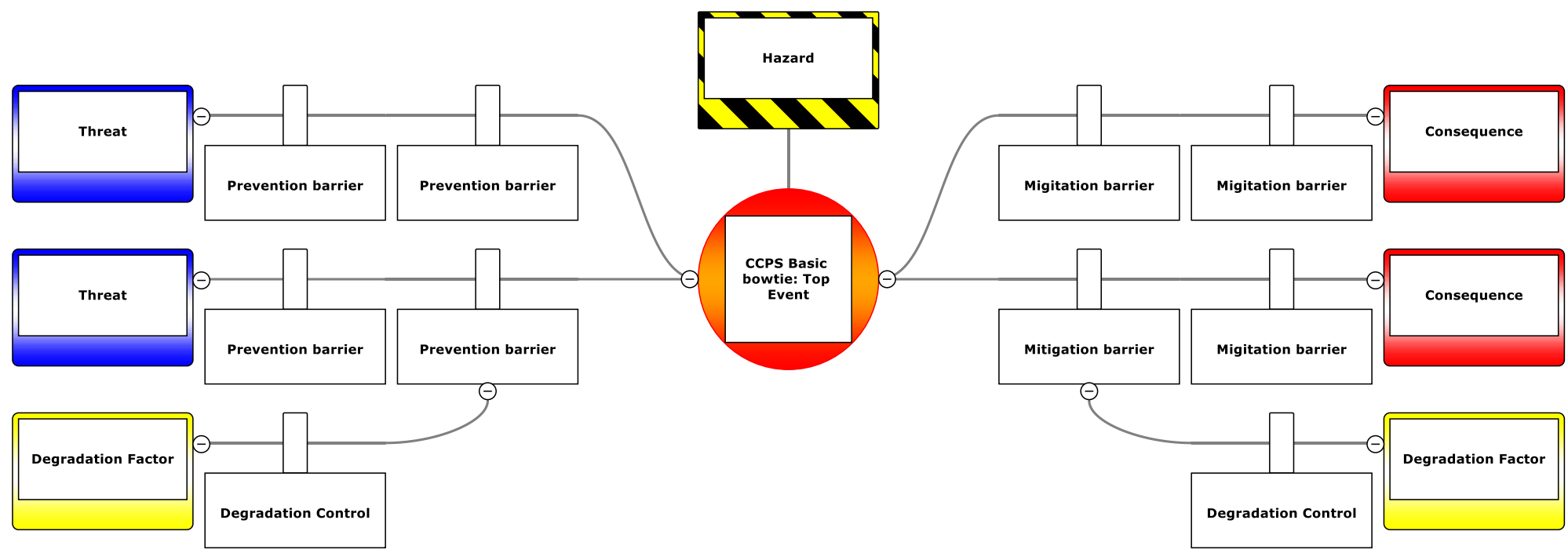
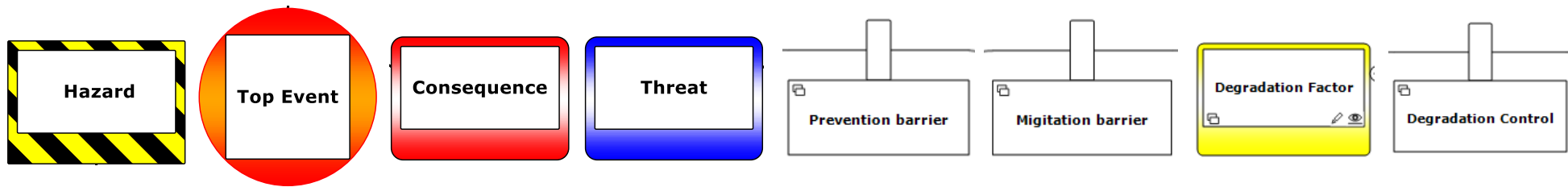


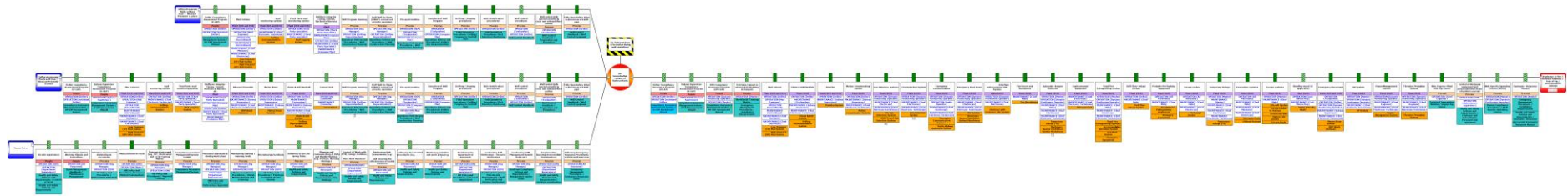


Mitigation barrier is effective if it is capable of completely mitigating the consequences or reducing its severity





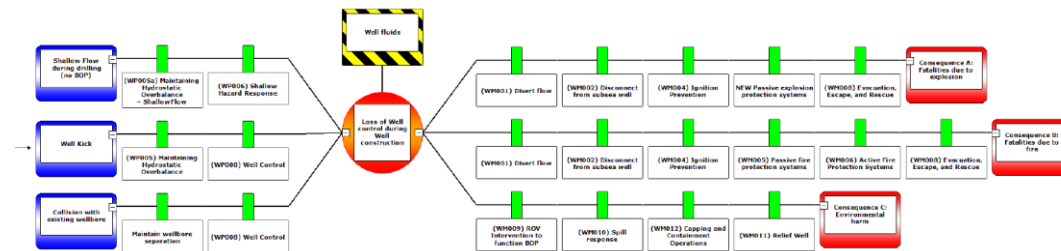




Rule for Barriers

No rules can lead to image of many barriers and perception of great risk control

Rules help present more realistic image



Effective

- *Prevention barrier* is effective if it is capable on its own of preventing a threat developing into the top event
- *Mitigation barrier* is effective if it is capable of completely mitigating the consequences or reducing its severity

Independent

- A barrier is independent if it has no common failure modes with other barriers

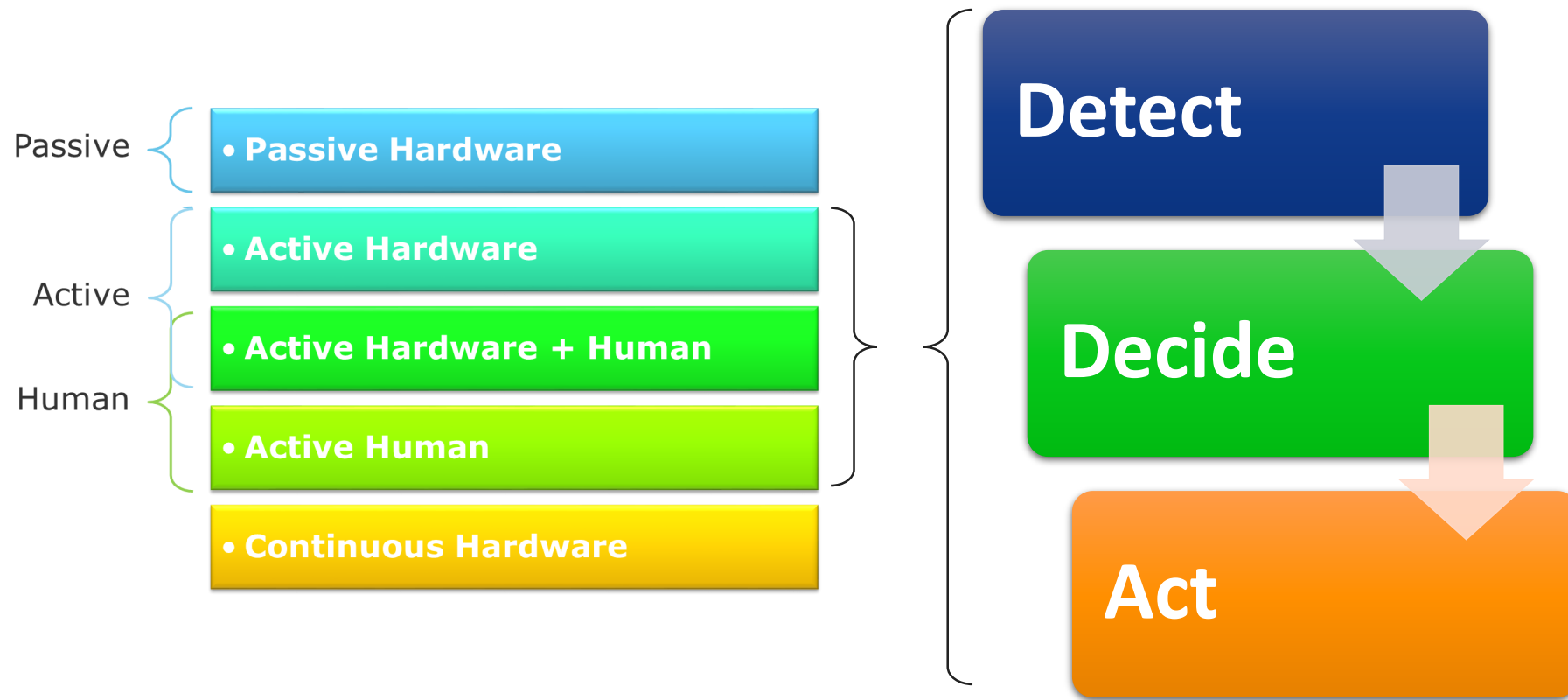
Auditable

- A barrier is auditable if there is a means to check that it works / delivers its functionality on demand
- Barriers can have performance standards for their functionality

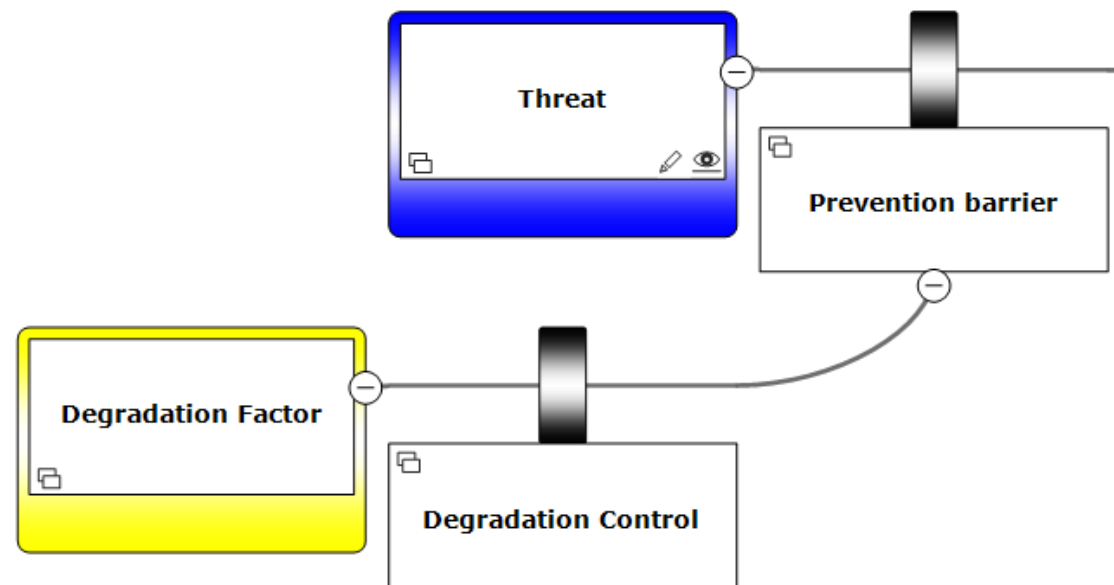
Barrier types



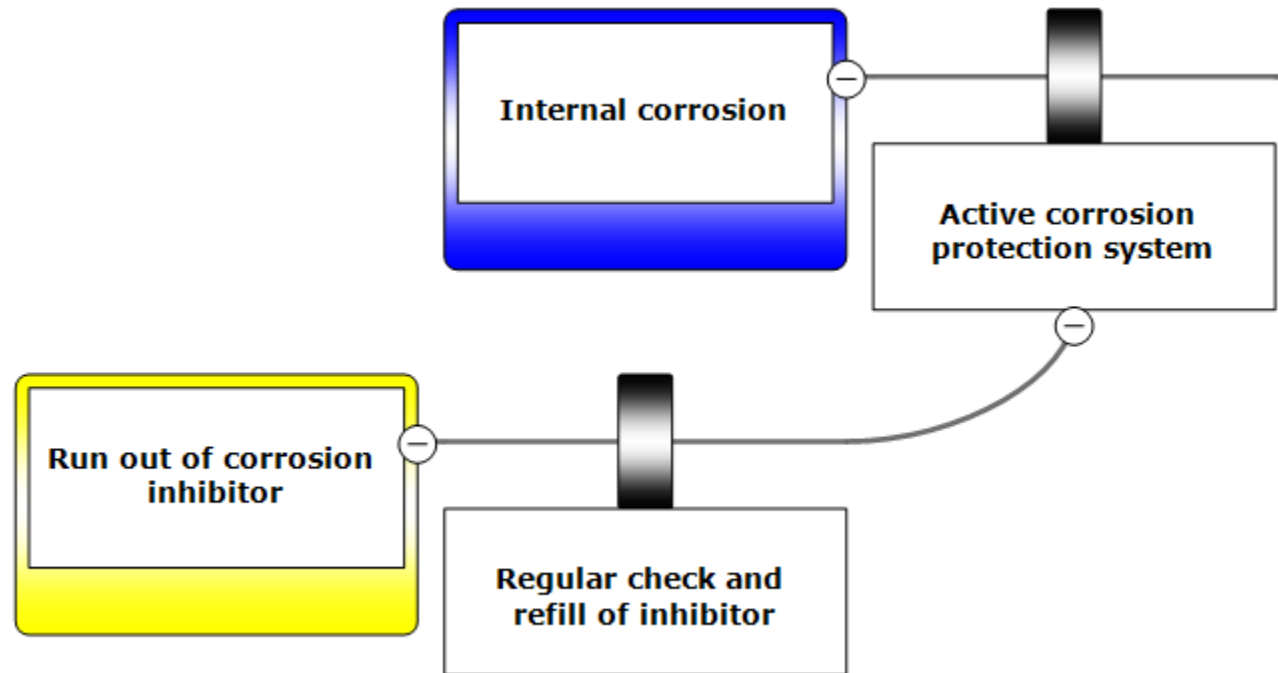




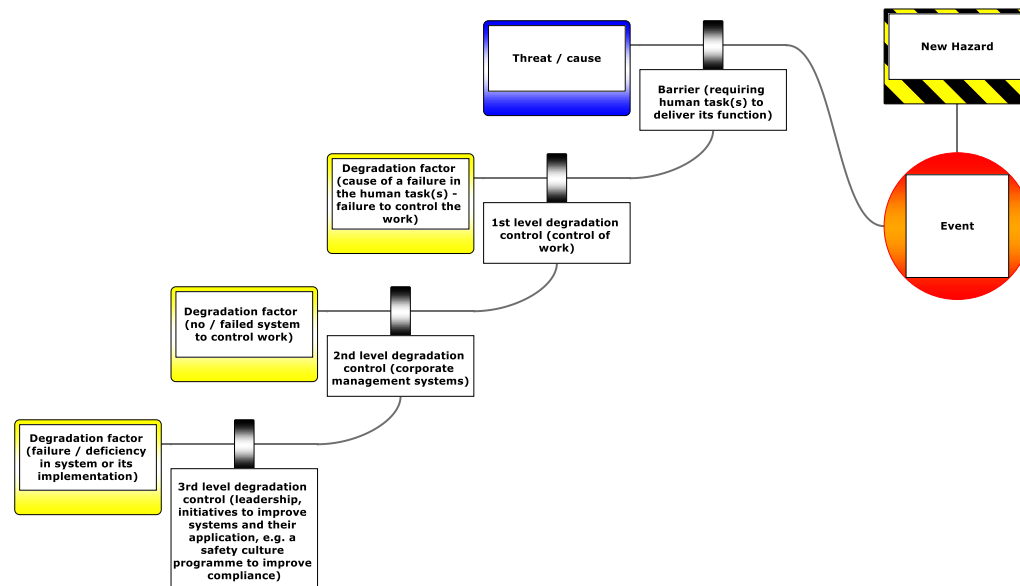
Barriers vs degradation controls



- Degradation Controls are on degradation pathway (NOT on the main pathway)
- Degradation Control types as for barriers
- Degradation Controls may not meet the full requirements of barrier validity

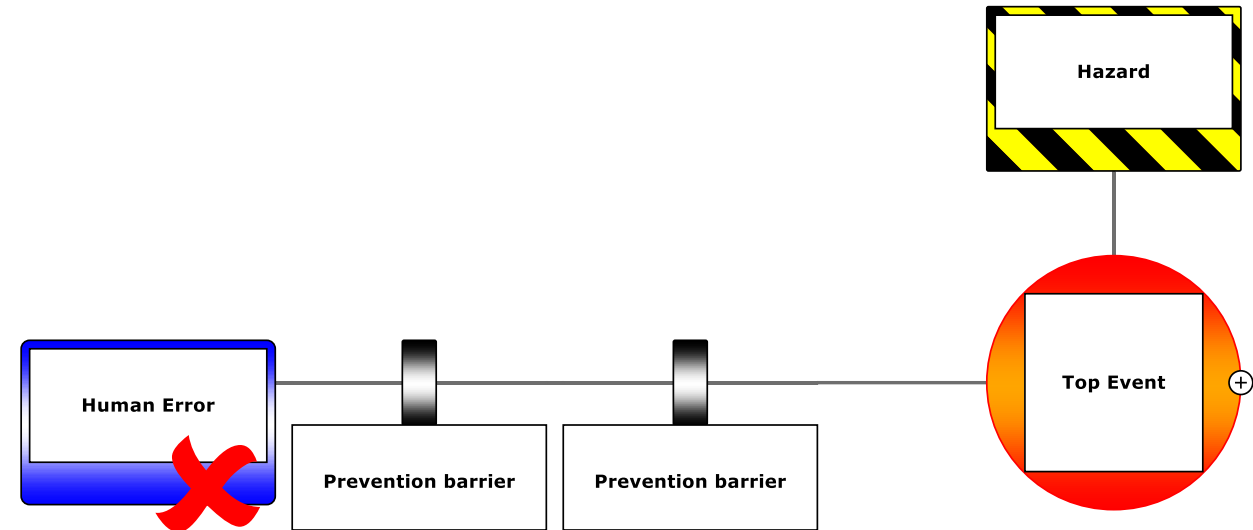


Where human errors fit in a bow tie



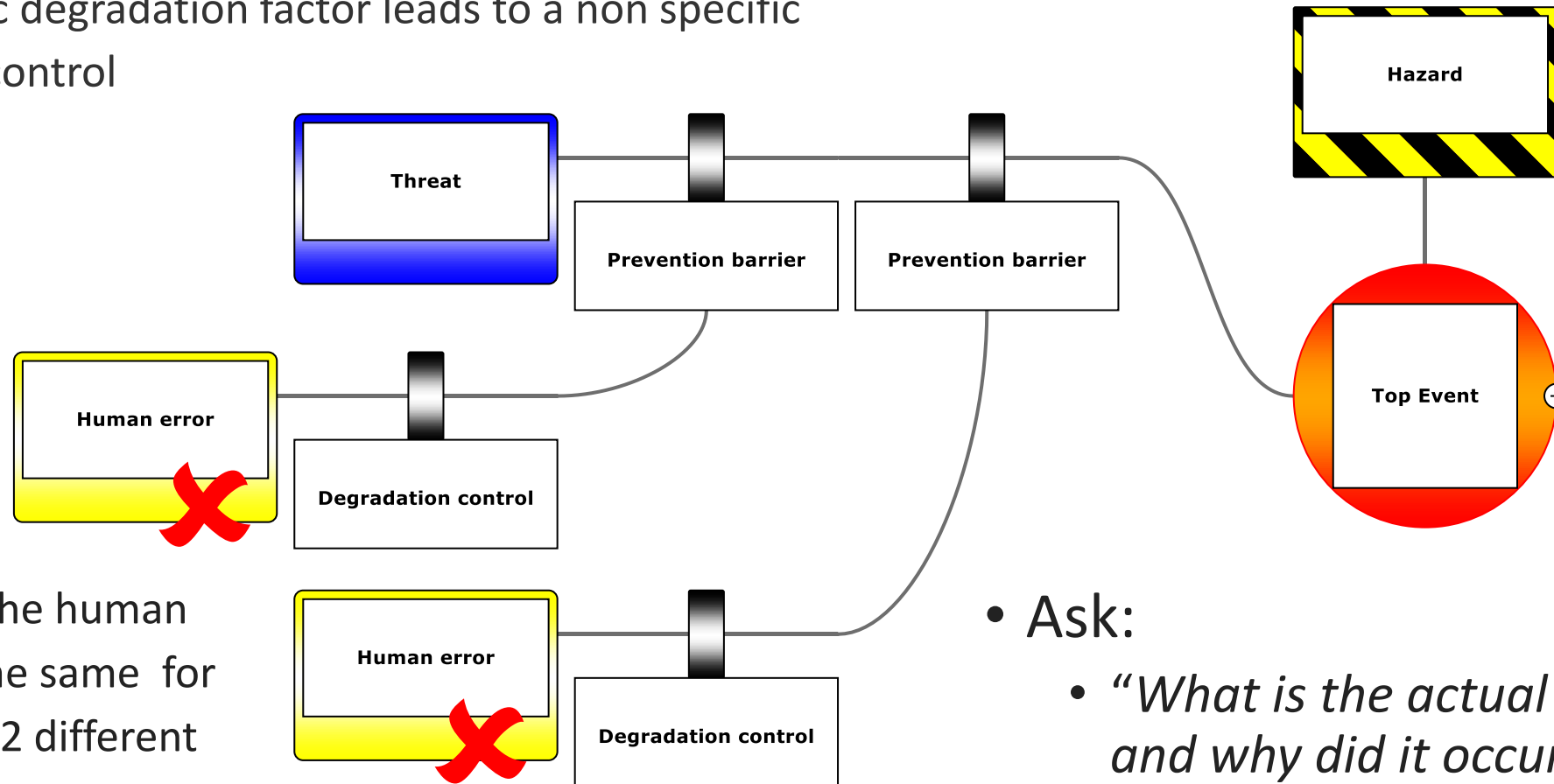
Do not use the words “human error” in your bow ties

- Human error is not a threat leading to a top event, but rather something that could defeat a barrier that is protecting against that top event
- Whenever someone is inclined to put ‘human error’ as a threat, they should challenge themselves by asking:
 - *“What is the barrier (or degradation control) that this error would defeat”?*



Do not use the words “human error” in your bow ties

A non-specific degradation factor leads to a non specific degradation control

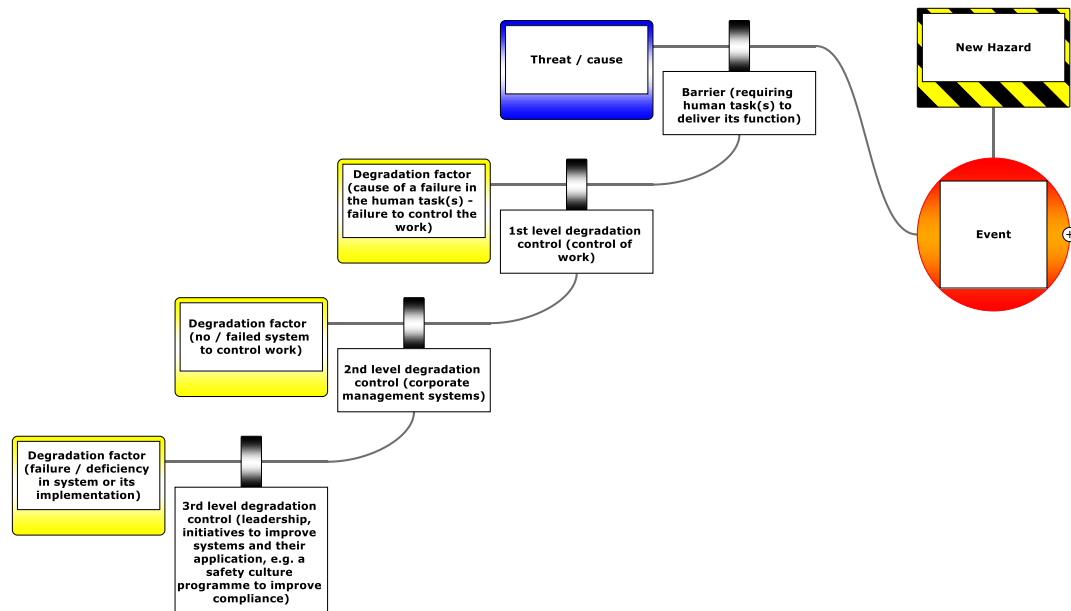


Unlikely the human error is the same for failure of 2 different barriers

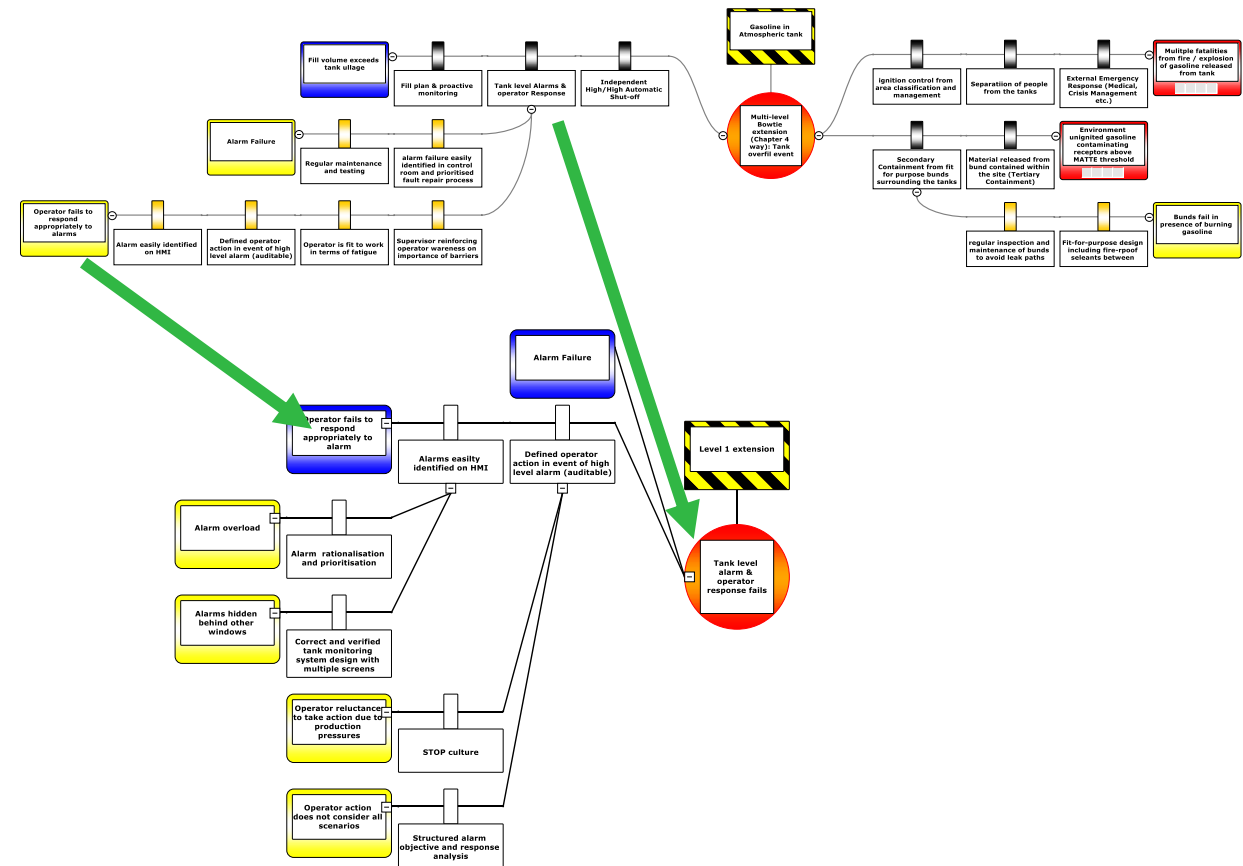
- Ask:
 - “What is the actual error and why did it occur”?

Model for including human error in a bow tie

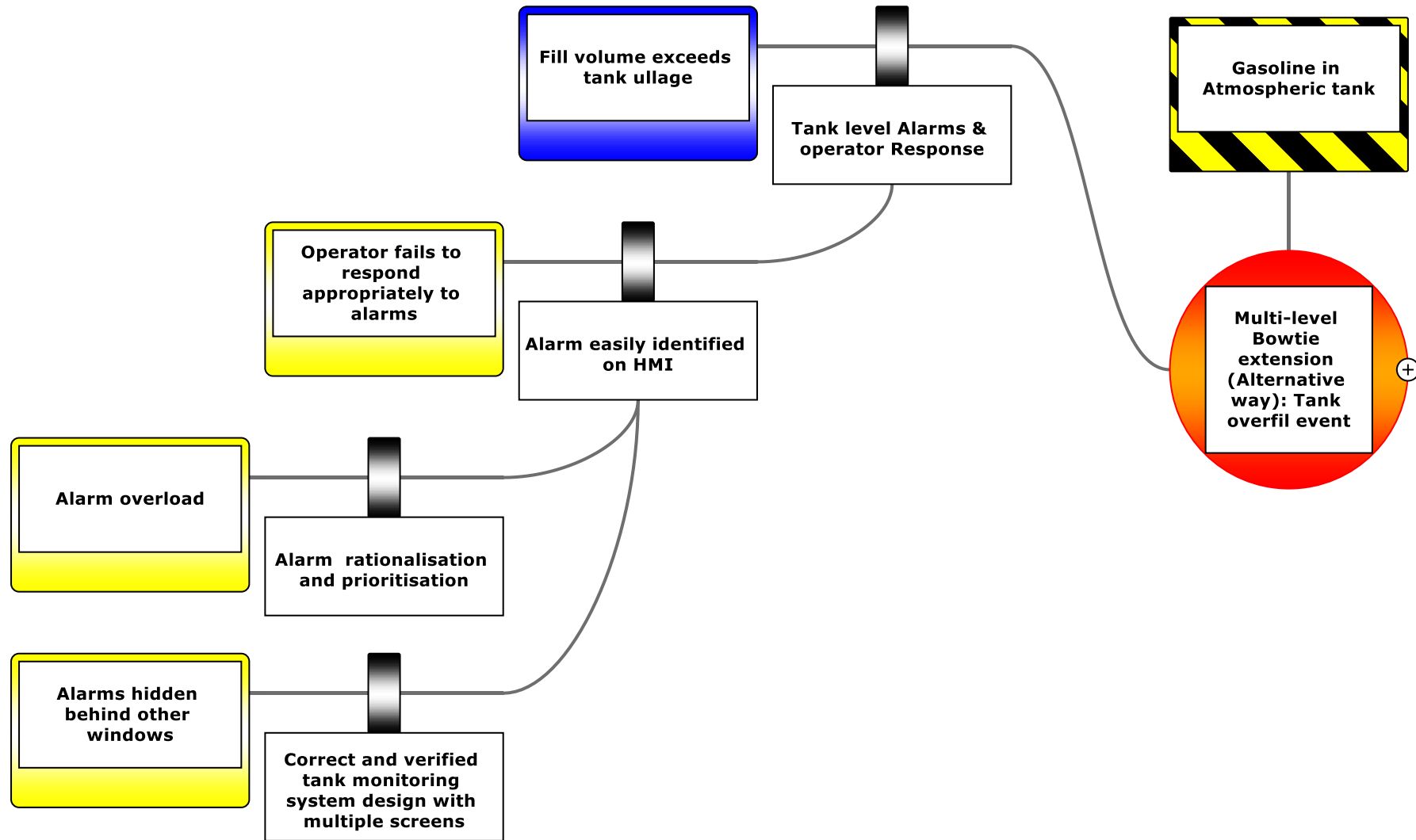
Multi-level bow tie



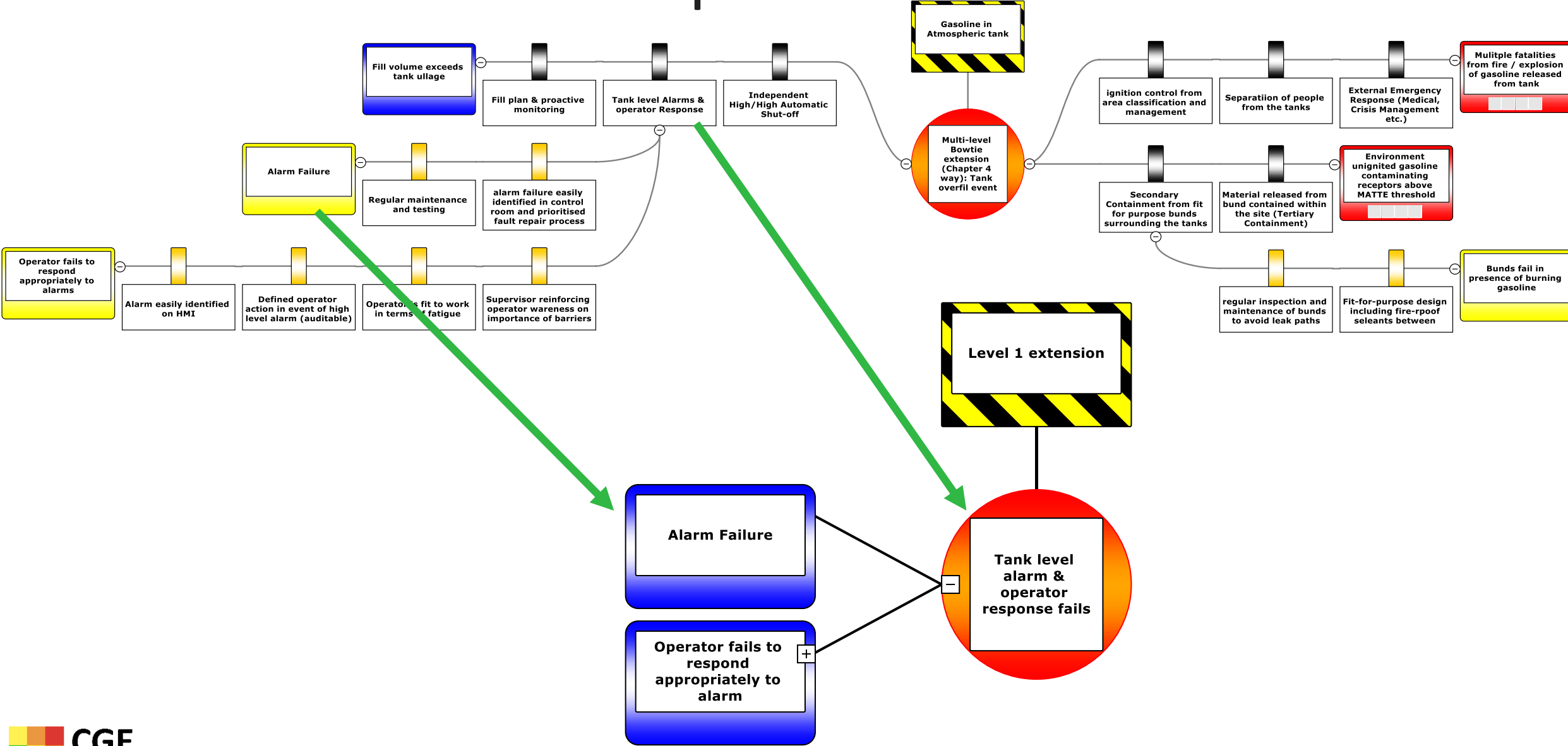
Multi - bow ties



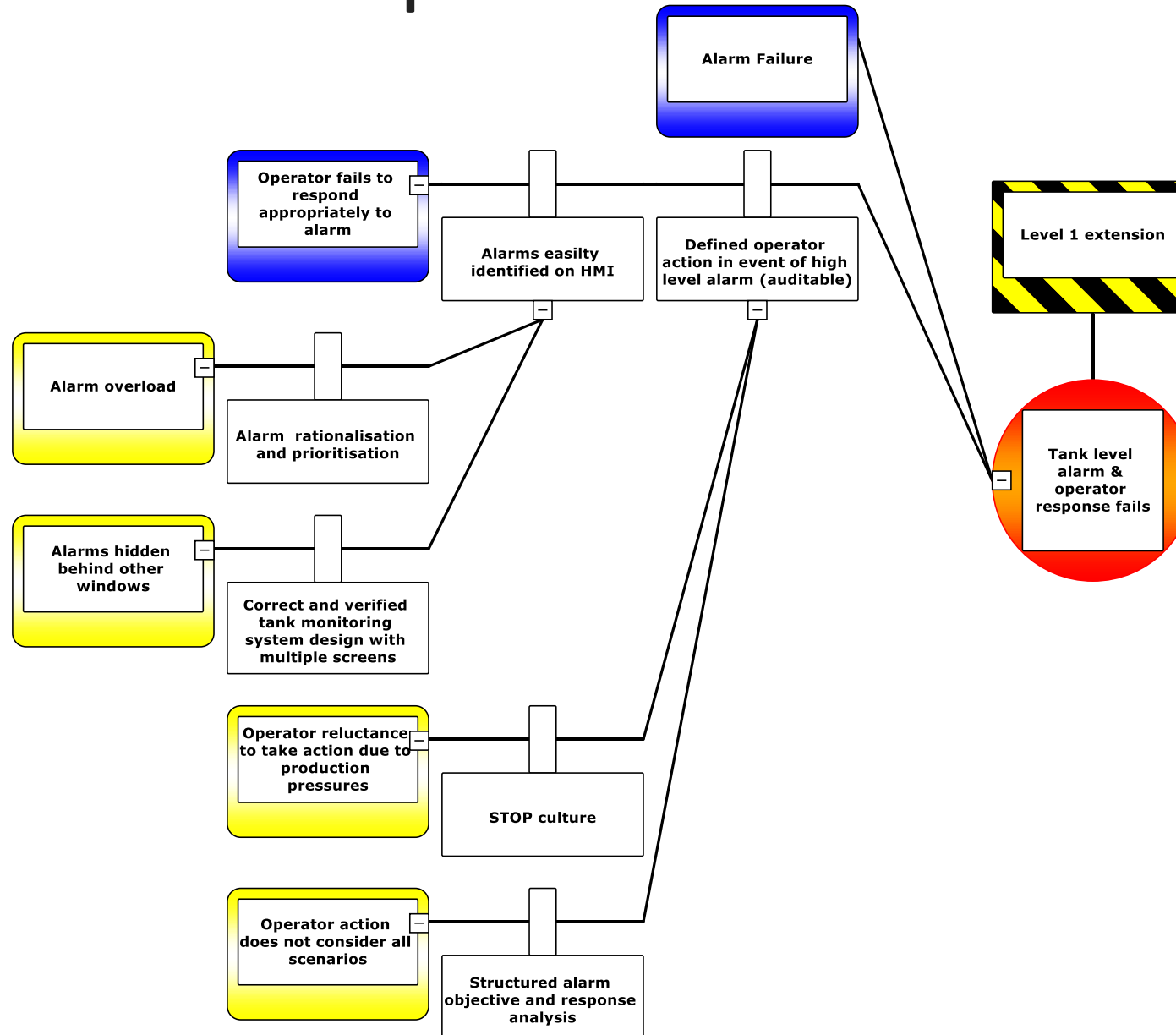
Multi-level example



Multi-Bow tie example

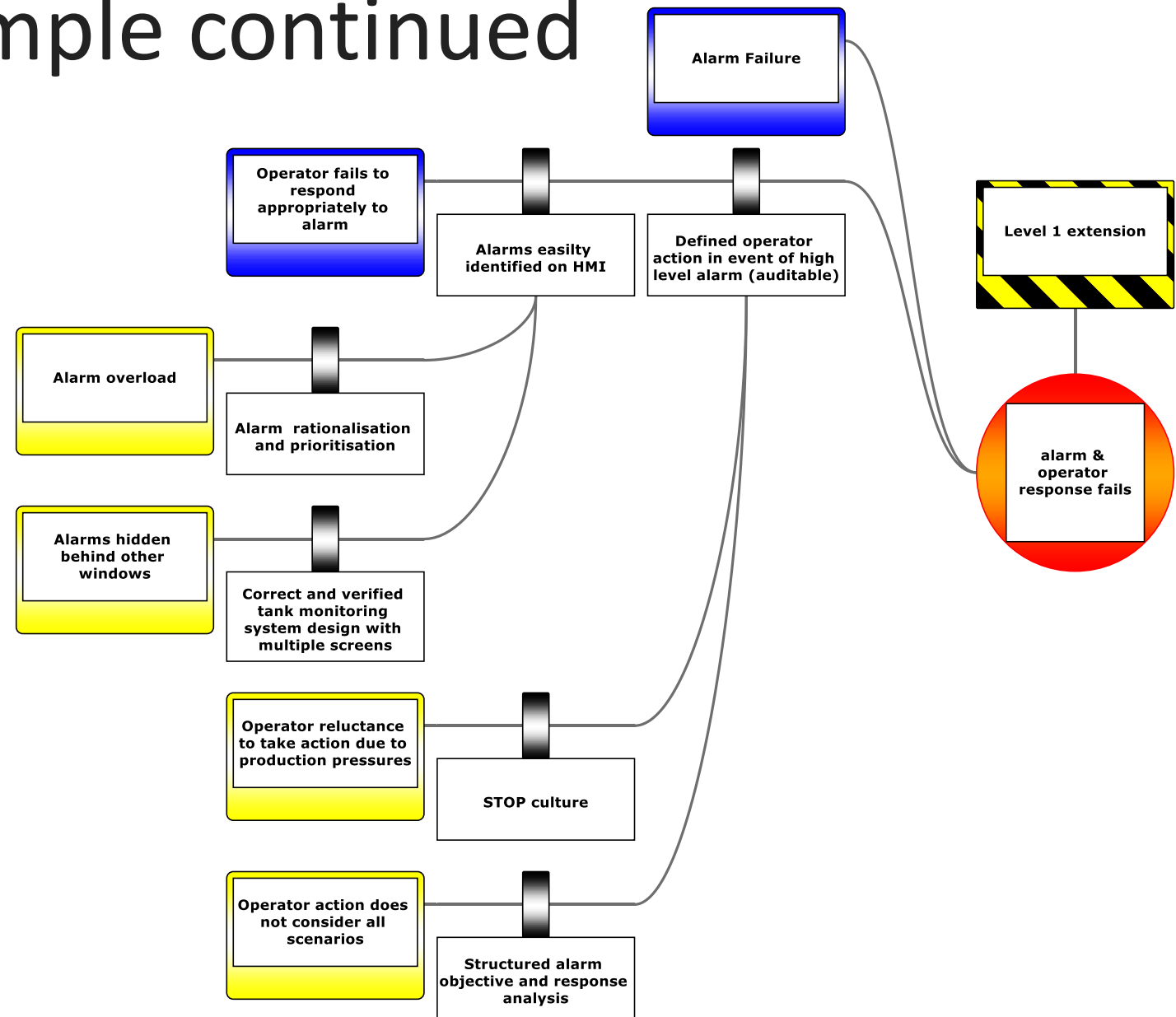


Multi-Bow tie example continued



Multi-Bow tie example continued

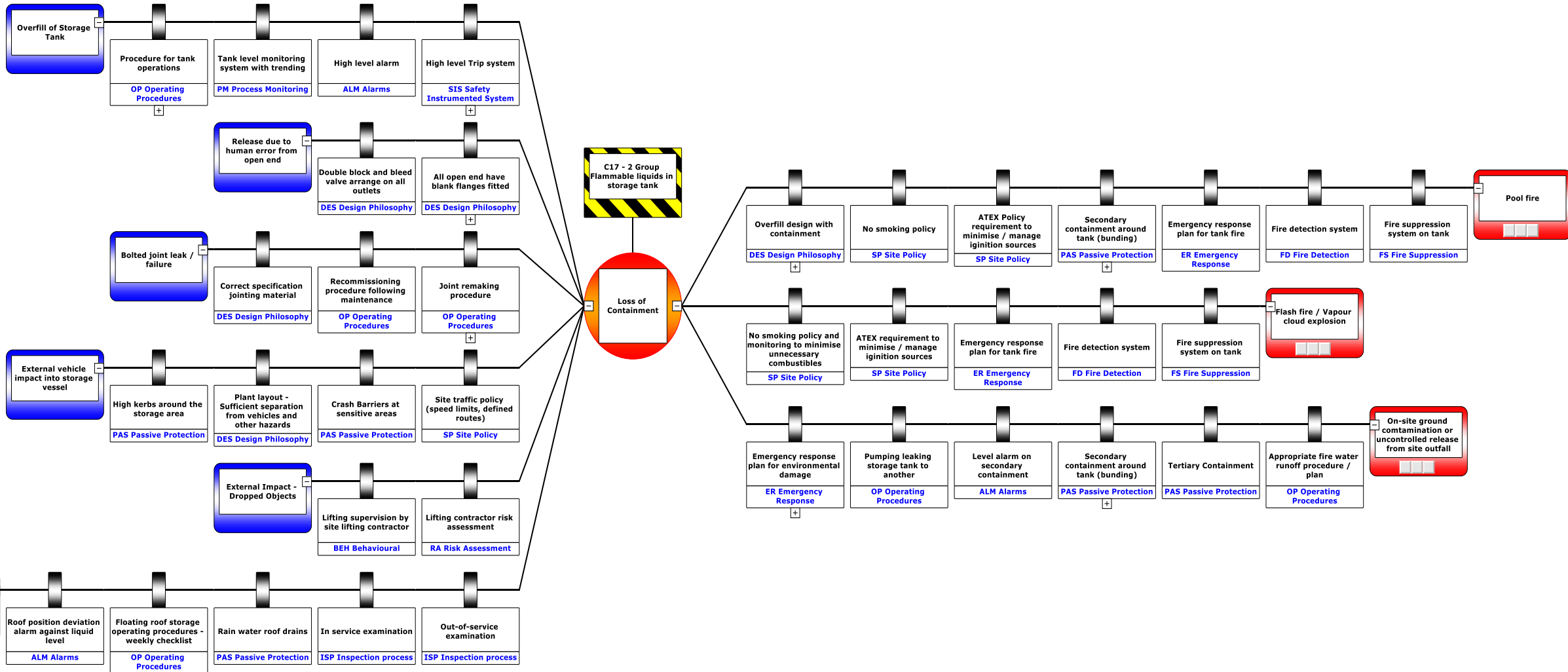
- Go more generic with Top Event
- Now all Alarms with operator response can be connected to it Extension Level 1 bow tie



Different uses of bow tie

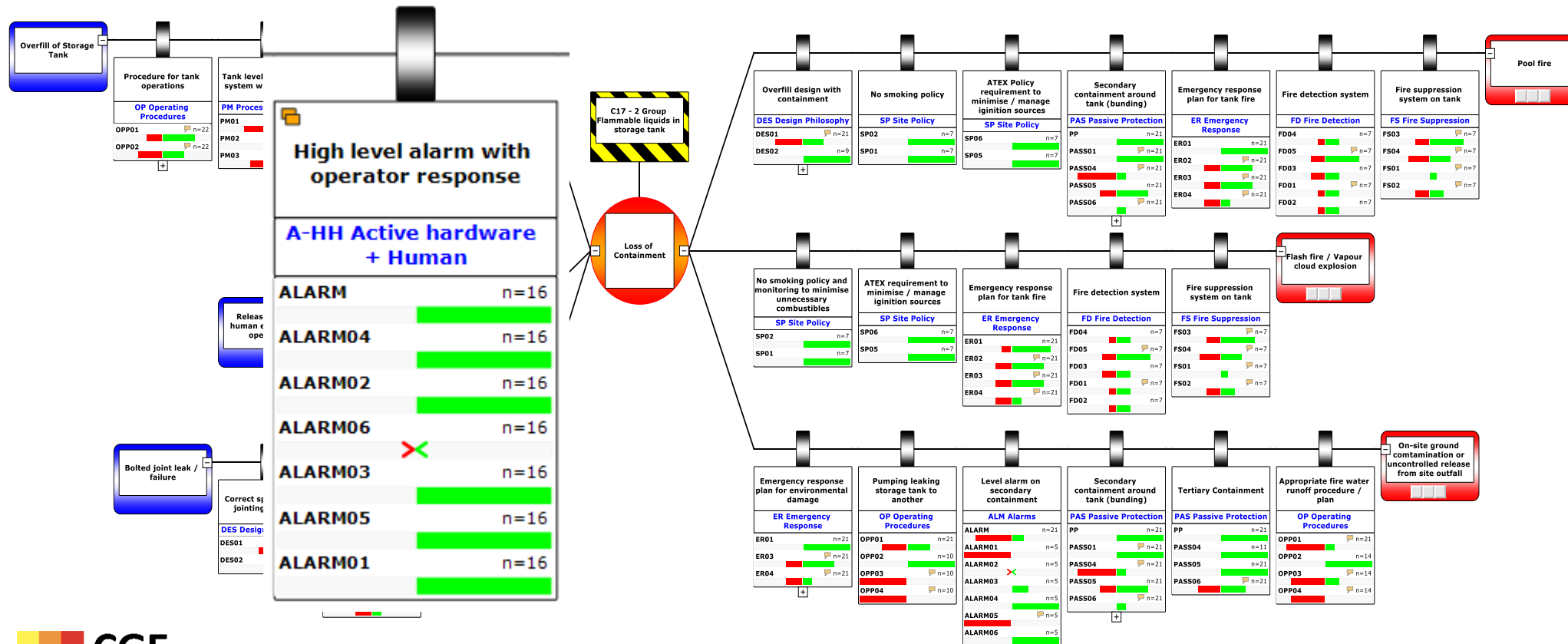
- Allow the communication of accident scenarios and the understanding of the importance of barriers and degradation controls
- Uses of bow ties discussed includes:
 - Linking bow ties to the risk management system (e.g. development and verification of design and as part of risk management in operations)
 - Communicating accident scenarios and all important barriers and degradation controls (including for different audiences)
 - Sharing barrier metadata
 - Accountability and engagement
 - Assessment of risk treatment
 - Identification of safety and environmental critical information
 - Supporting ALARP demonstration
 - Supporting organisational learning through corporate bow ties for major accidents
 - Supporting investigations
 - Real time dashboards
 - ...

Advanced Barrier Management



Visualising Audit Data

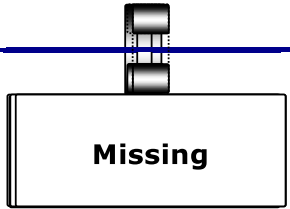
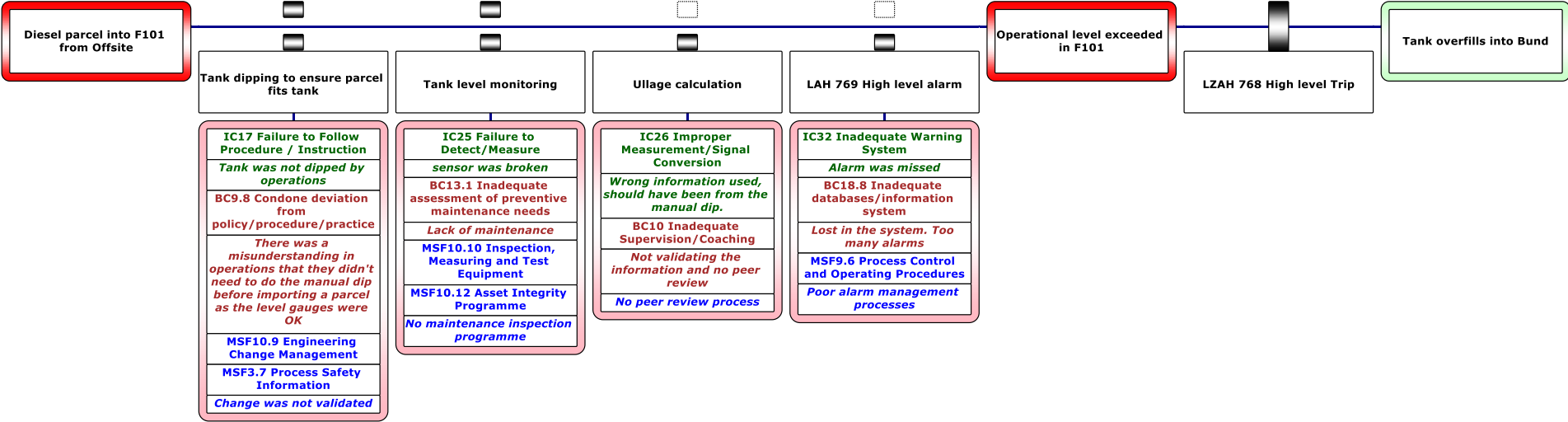
- Easy to spot weak spots
- Intuitive display
- Results focus on risks, not categories



Incidents

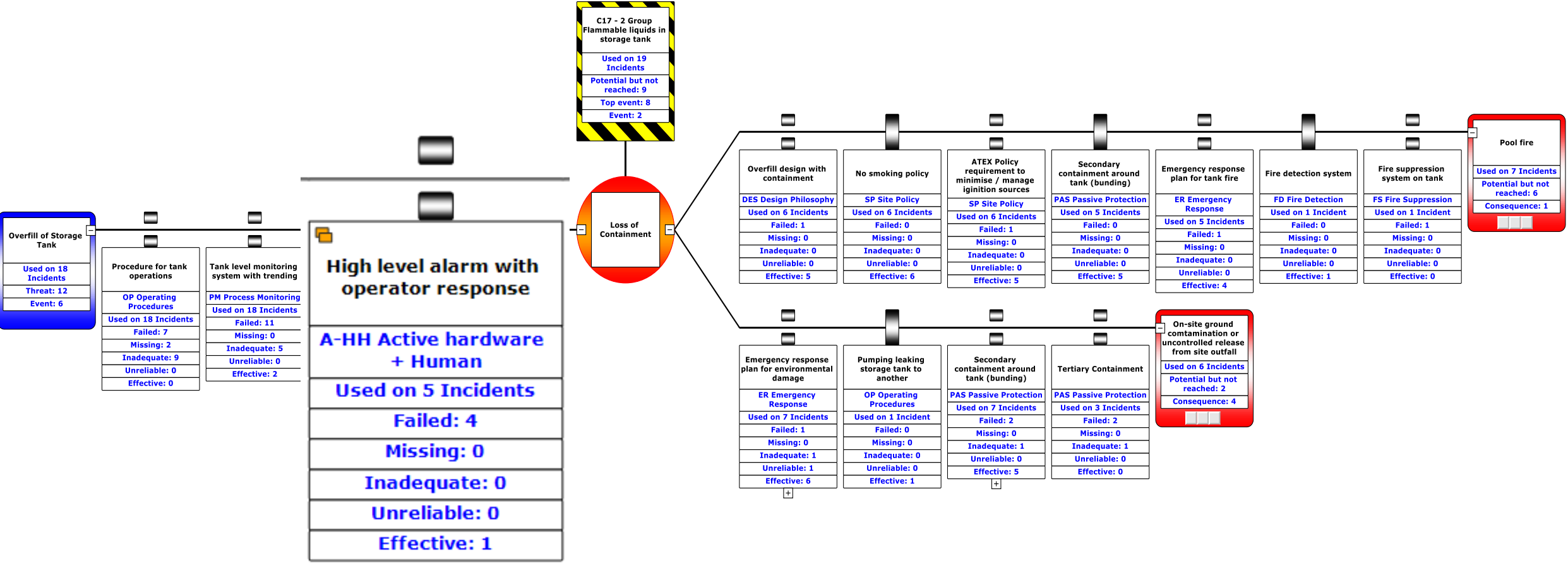
- Incident feedback about a barrier gives that real world sense on how the barrier has actually performed and what (if anything) failed to do as expected
- Incidents tend treated in silos
- No theme trending or collating what multiple incidents mean to an organisation
- Lack of a big picture

Incident Data



The barrier functioned as intended by its design but
 The barrier was described in the organization's SMS or
 was considered an industry standard, but it was not
 successfully implemented.
e.g. High level trip is required, but was not installed.

Visualising Incident Data



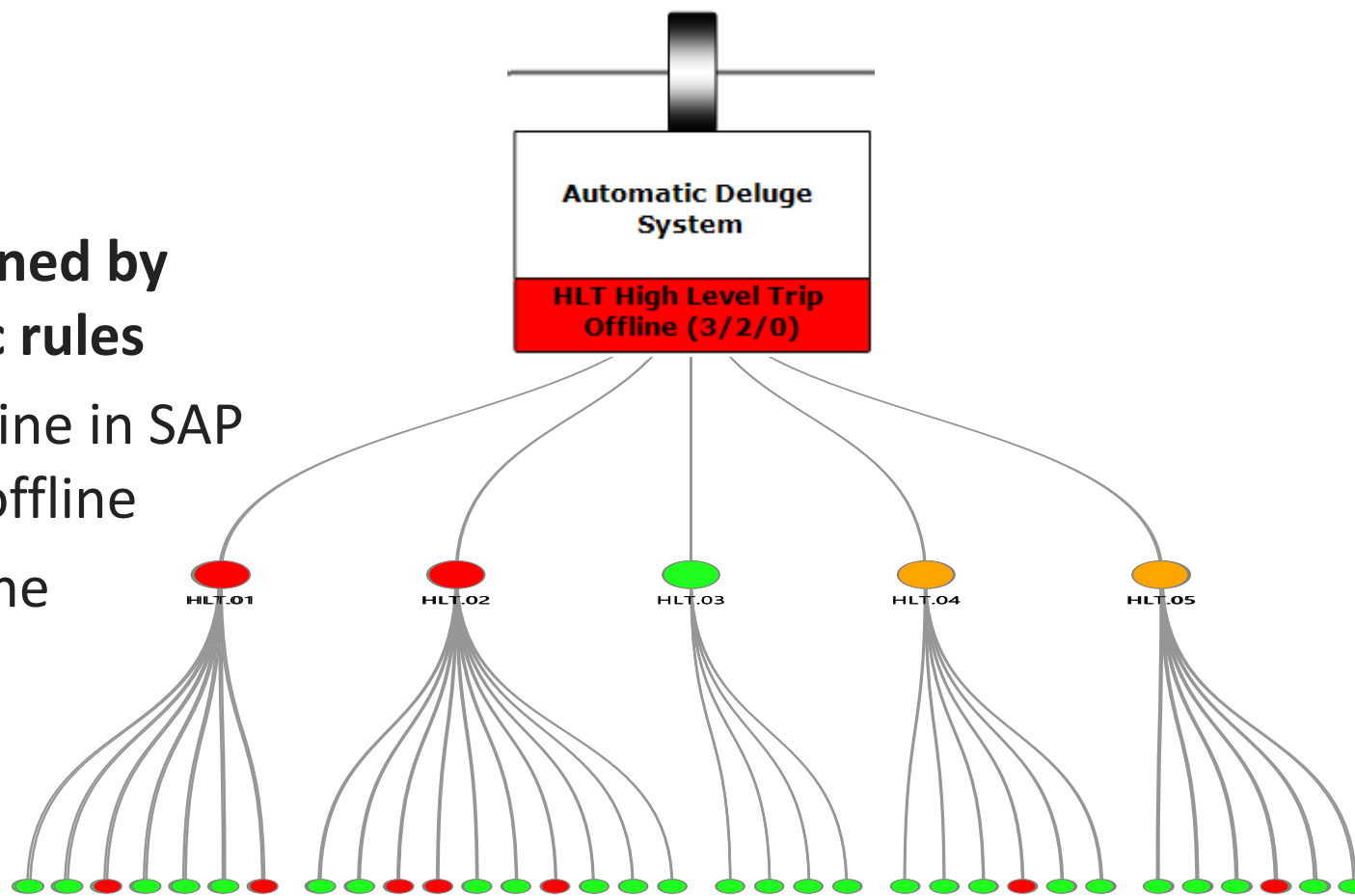
Which systems and barriers are offline today?

On/Off determined by system-specific rules

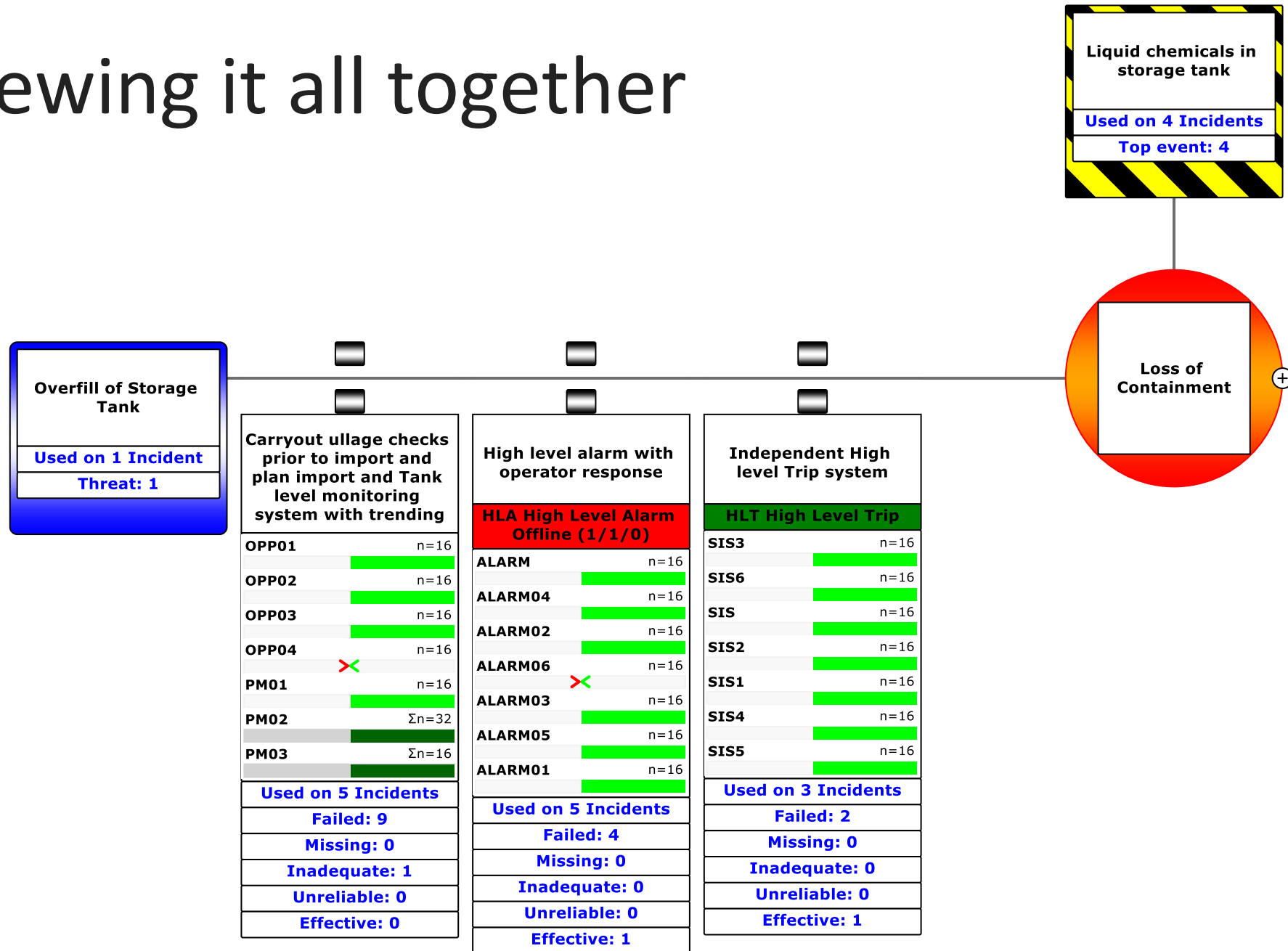
e.g. 3 tag items offline in SAP

=> subsystem offline

=> barrier offline



Viewing it all together





In collaboration with the Energy Institute



Also in collaboration

European Commission Joint Research

Centre

- Major Accident Hazards Bureau



Project Team Chair: Kiran Krishna, Shell
Co-Chair: Mark Scanlon, Energy Institute
Vice-Chair: Tim McGrath, Genentech (ex Chevron)
CCPS Staff Consultant: Charles Cowley
Principal author: Robin Pitblado, DNV GL
Sub-contractor to DNV GL: CGE Risk (Ben Keetlaer, Paul Haydock)



Peer Review group

Some of the peer review participants, in addition to companies of the working group.

UKPIA Major Hazards Working Group
 UK Health & Safety Executive (HSL)
 API RP 75 revision
 COMAH, Environment Agency England
 Process Safety & Reliability Group
 ExxonMobil
 Patrick Hudson Independent Consultant ex
 Professor, Delft University
 John Sherban, Systemic Risk Management.

Project Team members: CCPS

Martin Johnson BP
 Mark Manton ABS
 Ron McLeod Independent Consultant
 Darrin Miletello Lyondellbasell
 Americo Neto Braskem
 Sid Phakey Linde
 Keith Serre Nexen
 Ryan Supple ConocoPhillips
 TV Venkateswaran Reliance Industries India
 Stephanie Wardle Husky Energy
 Danny White BHP Billiton

Project Team members: Energy Institute

Dennis Evers Centrica
 Peter Jeffries Phillips66
 Rob Miles Hu-Tech
 Rob Saunders Shell
 Donald Smith ENI

Project Team members: EC JRC MAHB

Zsuzsanna Gyenes EC JRC MAHB
 Maureen Wood EC JRC MAHB



Live Q&A session