Safety Case Assessment Guide

Overview of Technical Assessment

Process Safety Assessment

Randy Cha
Major Hazards Department
20 Oct 2016

MINISTRY OF MANPOWER

A Great Workforce A Great Workplace

Objective

- Key elements of safety case **technical** assessment
- Assessment of process safety in safety cases
- Process safety-related examples

Main Elements in Technical Assessment

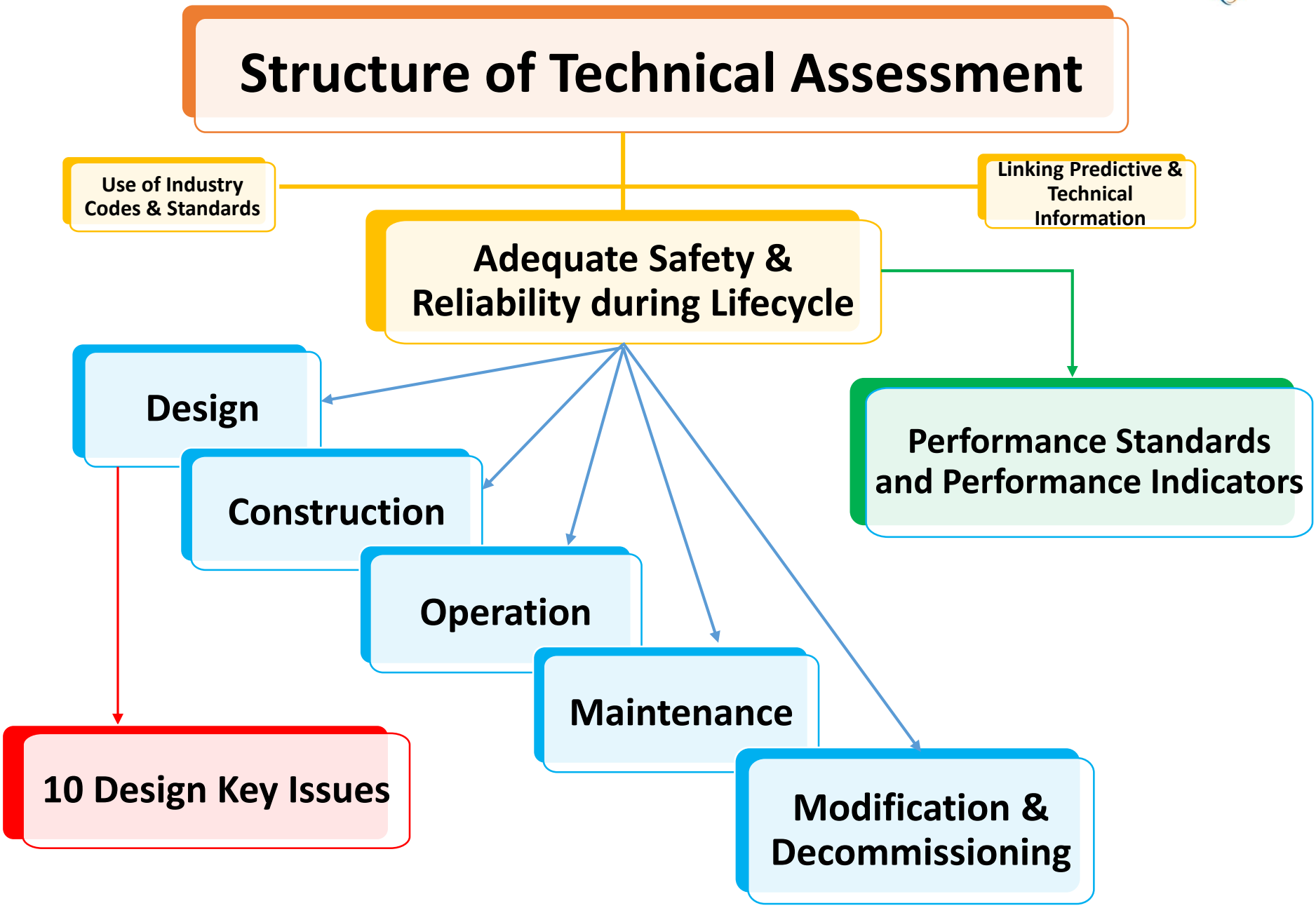
1. Describe and **justify** the choice of risk reduction measures for making risks ALARP based on the SCEs selected

2. Demonstrate that there is adequate **safety and reliability** during the life cycle of the installation and infrastructure relevant to major accidents

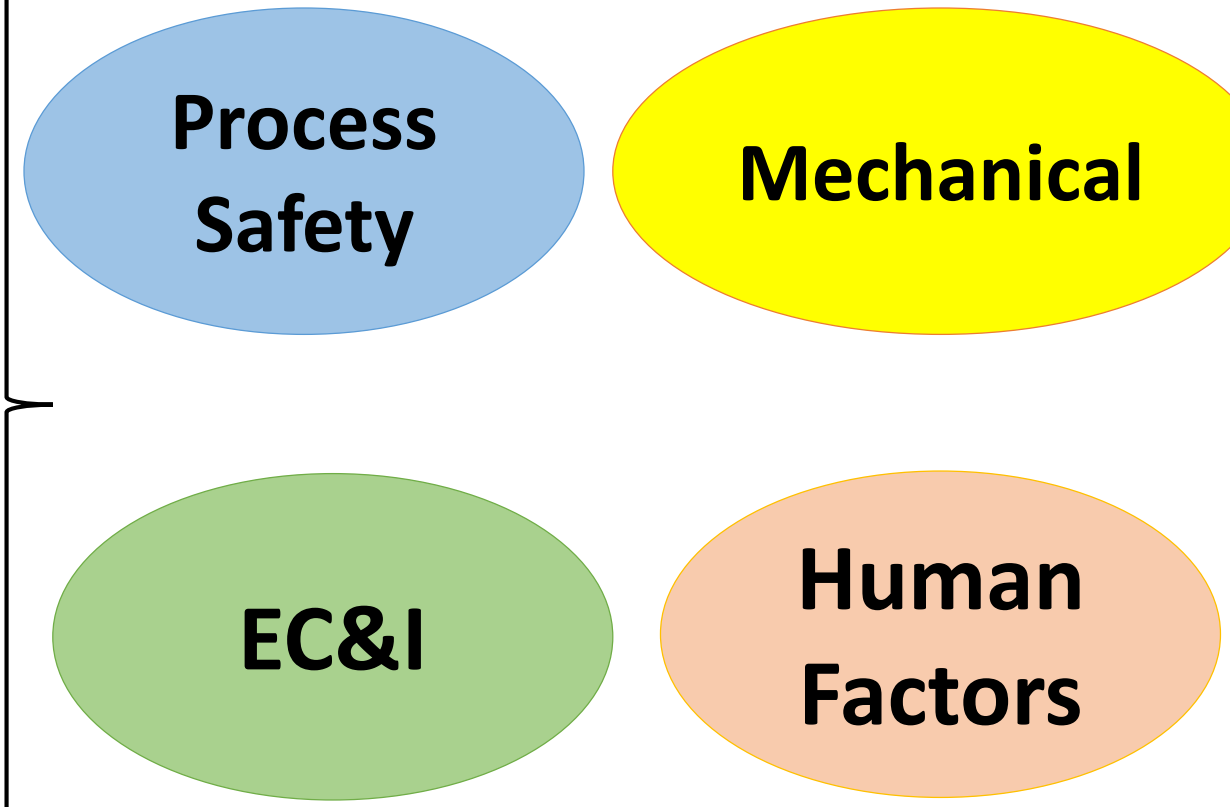
3. Demonstrate that **performance standards** and **performance indicators** are developed to provide ongoing assurance

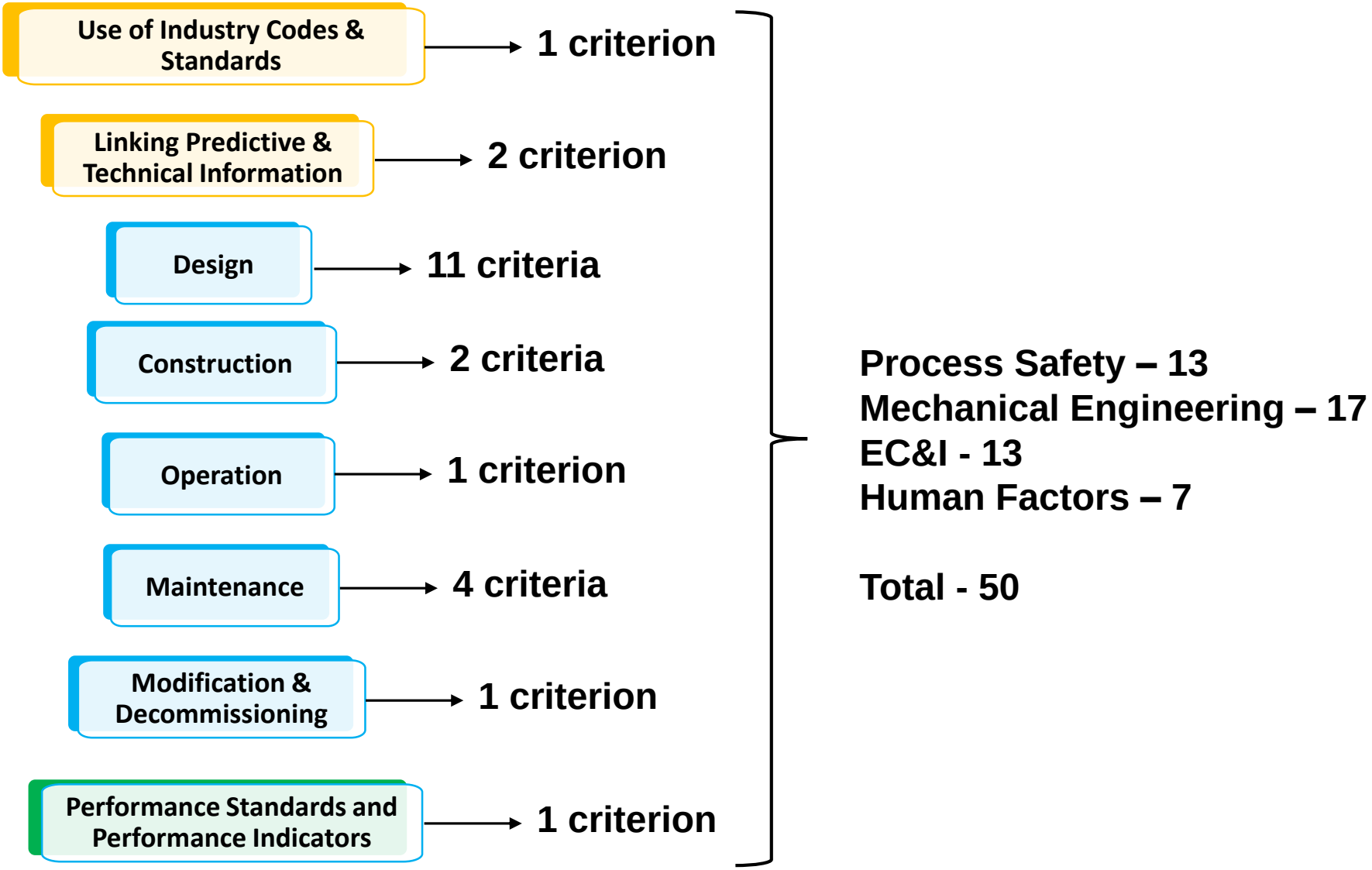
Structure of Technical Assessment

- Use of Industry Codes & Standards
- Linking Predictive & Technical Information
- Adequate Safety & Reliability during Lifecycle



- Use of Industry Codes & Standards
- Linking Predictive & Technical Information
- Design
- Construction
- Operation
- Maintenance
- Modification & Decommissioning
- Performance Standards and Performance Indicators

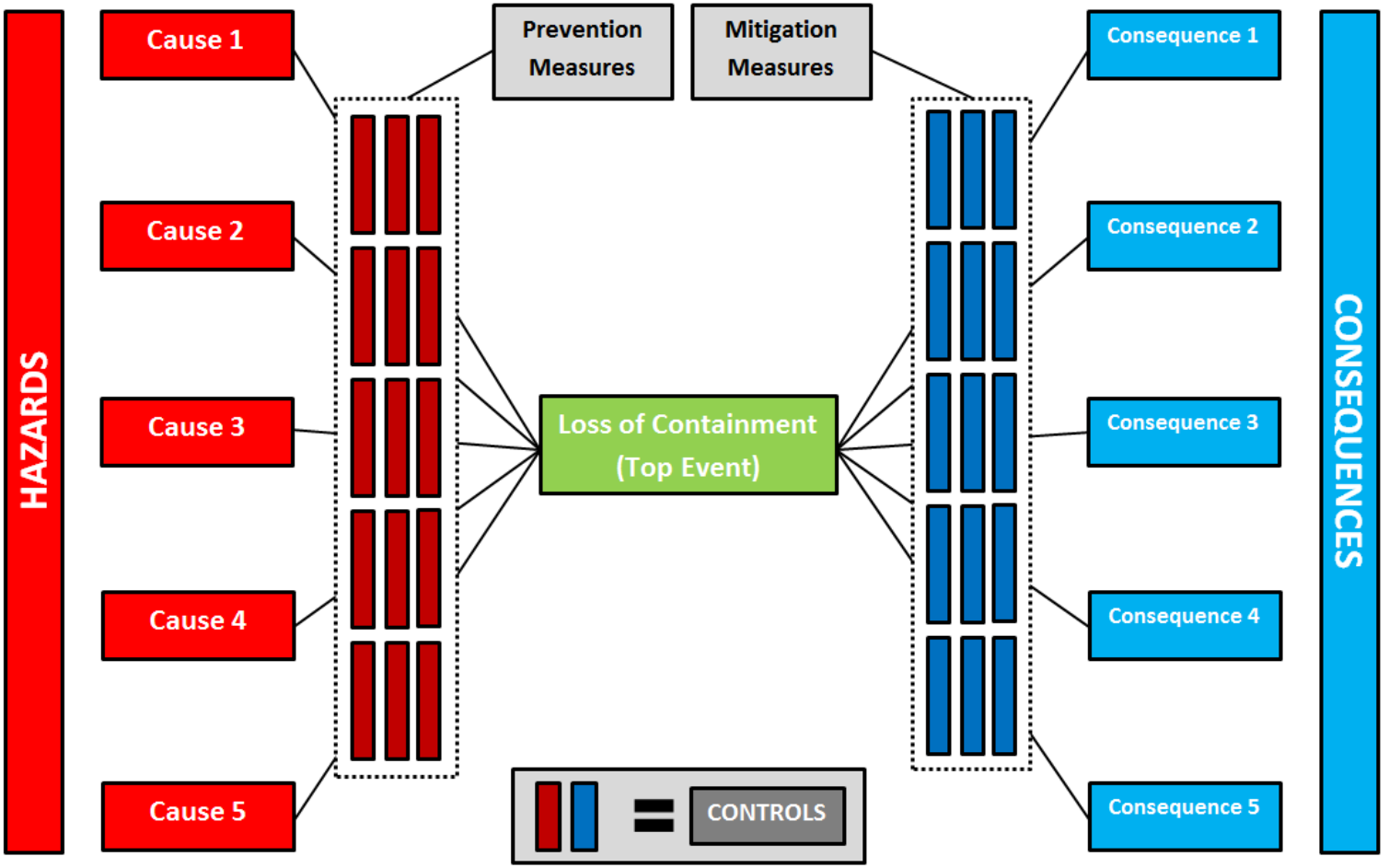




"The safety case shall show a clear link between the measures taken and the SCEs described."

- Identify hazards and safety critical events (SCEs)
- Describe the control measures and demonstrate clear links to the SCEs

Demonstrate Link Between Measures Taken and SCEs



Demonstrate Link Between Measures Taken and SCEs

MAS	HAZARD	Normal control RRM 1	Prevention RRM 2	Prevention RRM 3	Mitigation RRM 4	Mitigation RRM 5	Mitigation RRM 6
1) Overfill of bulk storage tanks from pipeline feed	1.1) LOC of extremely flammable liquid	ATG and alarms	Tank fill procedures – dipping tank, monitoring flow rate	Independent HI HI overfill prevention SIS	Flammable liquid detection in the bund	Secondary containment in the bund	Site fire fighting system
		ATG maintenance	Procedure evaluation	SIS maintenance	System maintenance	Maintenance	Procedure review
		ATG test		SIS proof test	IPS proof test	inspection	Fire drills
		Operator intervention					

"The safety case shall show a clear link between the measures taken and the SCEs described."

- Identify hazards and safety critical events (SCEs)
- Describe the control measures and demonstrate clear links to SCEs
- Explain the decision criteria for selecting the necessary measures to ensure risks are ALARP for SCEs
- Demonstrate adequate diversity and redundancy in the control measures

"The safety case shall show a clear link between the measures taken and the SCEs described."

In addition,

- Describe the link between design stages and associated hazard studies
- Describe how a suitable hierarchical approach has been used
- Describe how inherent safety designs have been introduced where reasonably practicable

"The safety case shall show that the installations have been designed to an appropriate standard."

Gap analysis of facilities/processes against current codes and standards

➔ ALARP demonstration

"The safety case shall show that the installations have been designed to an appropriate standard."

Be aware of changes to codes and standards that have been made in light of new information

Explain how in-house/corporate standards align with appropriate published standards and guidance

"The safety case shall show that utilities that are needed to implement any measure defined in the safety case shall have suitable reliability, availability and survivability."

Identify utilities essential for operation of key safety systems and its back-up system

Effect of the loss of key utilities has been considered as part of a structured HAZID and analysis process

Provide further justification on suitability of the utilities

Utility	Impact on safety	Back up and safety
Electrical power	Loss of electrically operated valves, control systems, SIS	Back up generator, UPS, load shedding, failsafe design
Compressed air	Loss of air actuated systems and instrumentation	Backup compressor, auto switchover, air reservoirs, failsafe design
Natural gas	Fire boilers for steam	Fuel supply, ignition control
Nitrogen	Loss of Inerting of flammable space	Duel supply , bottle and PSA, with auto changeover, low level alarm
Cooling	Loss of process temp control	Duel supply, low water detection and alarm, supply header tank
Fire water	Loss of fire fighting water	Duel supply, low water detection
Fuel Oil	Fire boilers for steam	Fuel supply, ignition control, burner management system

"The safety case shall show that appropriate measures have been taken to prevent and effectively contain releases of dangerous substances"

- **The process** by which dangerous substances could be accidentally released from containment and **the measures** which have been provided to prevent or minimise releases

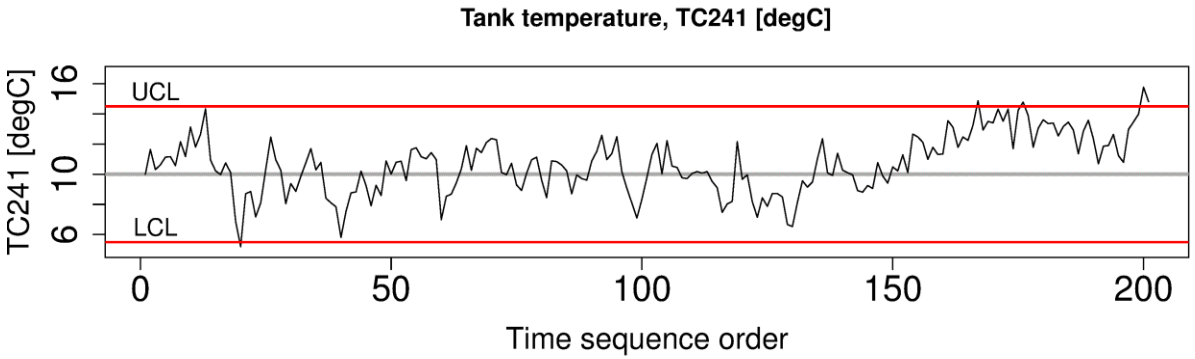
- Key Demonstration Topics
  - ✓ Primary Containment
  - ✓ Secondary & Tertiary Containment
  - ✓ Venting Systems
  - ✓ Isolation Arrangements
  - ✓ Detection of Releases

Example – Isolation Arrangements

Design for Emergency Shutdown (ESD)/Emergency Depressurising (EDP)

- Demonstrate how ESD valves are incorporated to provide for the necessary degree of sectionalisation
- Explain how the ESD system is to be activated and justify the degree of automation or manual intervention required
- Discuss contingency to ensure ESD can still function even in event of major utility failure

"The safety case shall describe how adequate control measures have been provided to protect the plant against excursions beyond design conditions"



- How margin shall be set so that for foreseeable failures, appropriate corrective action can be taken before the safe operating limits are exceeded

- How MHIs monitor and ensure that plant and equipment continues to operate within the design envelope and defined safe operating limits

"The safety case shall describe how adequate control measures have been provided to protect the plant against excursions beyond design conditions"

- How chemical reaction hazards are evaluated and justify the sufficiency of the control measures to prevent runaway reactions, overpressure and LOC

- Describe the emergency prevention and protection measures and show that these are fit for purpose

"The safety case shall describe how adequate control measures have been provided to protect the plant against excursions beyond design conditions"

Key Demonstration Topics

- Design codes and standards
- Safe operating limits
- Control systems
- Explosion relief
- Operating procedures
- Relief systems/vent systems
- Reliability of utilities

Example - Chemical Reaction Hazard

- Chemical process risk assessment
- Evaluating reaction hazards (e.g. thermal decomposition, exothermic runaway)
  - ➔ Predictive data for assessing risk and informing process design/siting considerations
- Select control measures (hierarchical approach)
  - ➔ Basis of safety
  - ➔ Highlight aspects of design and operation which are safety-critical

The safety case should not simply describe the features of the plant and leave it to MHD to decide whether these are sufficient.

Example - Chemical Reaction Hazard & Overpressure

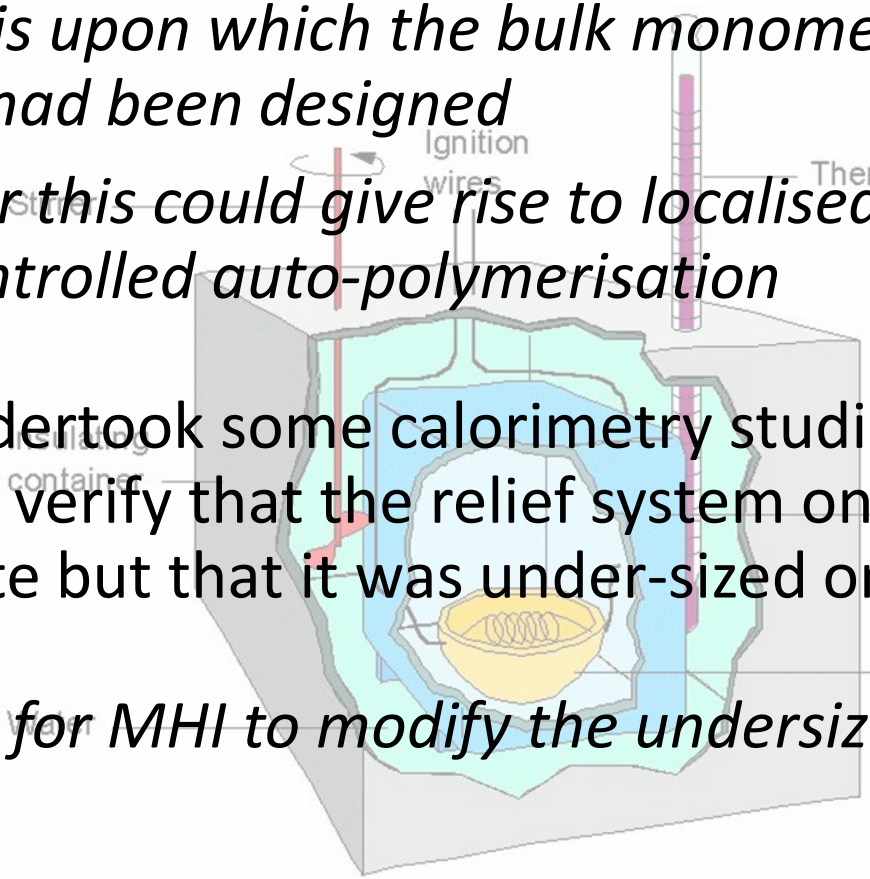
- Safety case describe specifically on two tanks in a tank farm storing bulk quantities of a reactive monomer.

- Nearby piping conveying high pressure hydrocarbon was assessed to be a credible source of jet fire.

Example - Chemical Reaction Hazard & Overpressure

Demonstration asked for:

- *The basis upon which the bulk monomer storage relief system had been designed*
- *Whether this could give rise to localised heating resulting in uncontrolled auto-polymerisation*

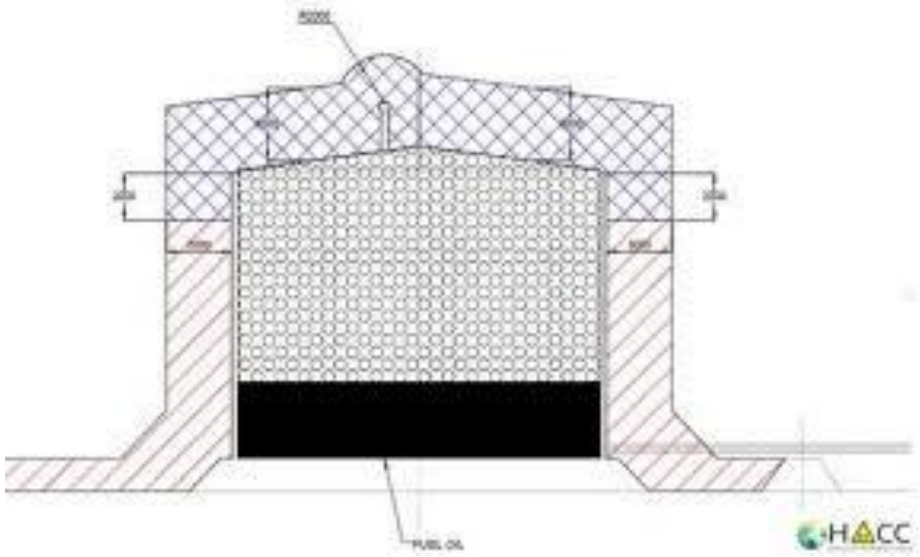


➢ MHI undertook some calorimetry studies which enabled them to verify that the relief system on one storage was adequate but that it was under-sized on another tank.

Action plan for MHI to modify the undersized relief system

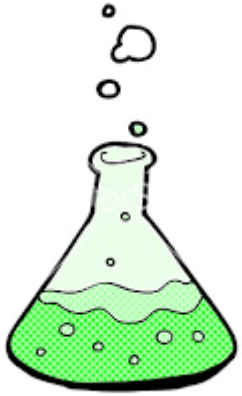
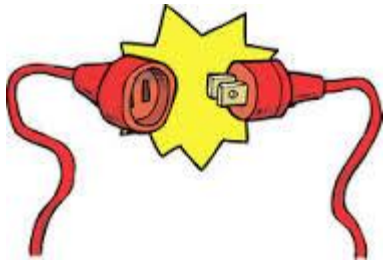
"The safety case shall show that there are systems for identifying locations where flammable substances could be present and how the equipment has been designed to take account of the risk"

Use of Industry Codes & Standards



"The safety case shall show that there are systems for identifying locations where flammable substances could be present and how the equipment has been designed to take account of the risk"

Risk Assessment → **Flammable and Explosive Atmosphere**


"The safety case shall show that there are systems for identifying locations where flammable substances could be present and how the equipment has been designed to take account of the risk"

- Procedures and policies for identifying hazardous areas are based on established codes and standards
- The HAC data is used 1) in the selection and location of equipment and 2) in considering plant and process changes
- The system for periodic review of HAC documentation or for planned review as a result of a significant change

Summary

- Process safety topic is vast i.e. no one-size-fits-all assessment guide
- MHD is looking for demonstration that:
  - ✓ Appropriate codes and standards are used
  - ✓ Adequate safety and reliability have been taken into consideration during life cycle of MHIs
  - ✓ Technical and predictive demonstration are logical, coherent and cohesive
  - ✓ Appropriate performance indicator and performance standards are developed

Q&A