• **Control measure:**
  – Means of eliminating, preventing, reducing or mitigating the risk of hazardous events arising at or near a facility

• **Hazard:**
  – A situation with the potential for causing harm

• **Major Accident Event (MAE)**
  – An event connected with the facility, including a natural event, having the potential to cause multiple fatalities of persons at or near the facility

• **Risk:**
  – A function of likelihood and consequence

• **Risk Assessment:**
  – The process of estimating the likelihood of specific consequences of a given severity
• **National Offshore Petroleum Safety and Environmental Management Authority**

• Petroleum and Greenhouse Gas Storage activities:
  – in Commonwealth waters
  – in state waters where powers conferred

• Regulation of:
  – Safety
  – Well integrity
  – Environmental management
Legislation – General duties

• Facility operators must take all reasonably practicable steps to ensure that:
  – The facility is safe and without risk to health
  – All work and other activities are carried out in a safe manner and without risk to health

• Specific duties include:
  – Implementation and maintenance of safe systems of work
  – Procedures and equipment for control of emergencies
• As Low As Reasonably Practicable
• No other practical measures can reasonably be taken to reduce risks further
• Involves assessment of:
  – The risk to be avoided
  – The cost involved
  – The benefit (risk reduction)
  – ‘Gross disproportion’ between cost and benefit
• Formal Safety Assessment
  – Identifies all hazards with the potential to cause a MAE
  – Assesses the risk
  – Identifies control measures to reduce the risk to ALARP

• Safety Management System
  – Identifies hazards to health and safety
  – Assesses the risk associated with each hazard
  – Identifies how risks will be reduced to ALARP
Control measures

• Reduce risk
  – Lower the likelihood
  – Minimise the consequence

• Includes:
  – Physical equipment
  – Process control systems
  – Procedures
  – Emergency plan
Hierarchy of controls – event control

- **Eliminate**
  - Remove the hazard
- **Prevent**
  - Lower the likelihood
- **Reduce**
  - Detect and limit escalation
- **Mitigate**
  - Protect life
Event control

Hazard
Hazard
Hazard
Hazard

Prevention Controls

EVENT

Mitigation Controls

Consequence
Consequence
Consequence
Consequence

Elimination Prevention Reduction Mitigation
Event example
Control types

• Eliminate
• Substitute
  – Use something else
• Engineer
  – Isolate the hazard
• Administrate
  – Do / avoid something
• Personal protective equipment
  – Wear something
• What is the hazard?
  – Vehicle interactions
• What is the potential event?
  – Crash
• What are the potential consequences?
  – Death
  – Injury
  – Damage
## Control measures

<table>
<thead>
<tr>
<th>Eliminate</th>
<th>Prevent</th>
<th>Reduce</th>
<th>Mitigate</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Walk</td>
<td>• Driver training</td>
<td>• Collision avoidance technology</td>
<td>• Seatbelts</td>
</tr>
<tr>
<td>• Public transport</td>
<td>• Road rules</td>
<td>• ABS brakes</td>
<td>• Air bags</td>
</tr>
<tr>
<td>• Bicycle paths</td>
<td>• Headlights</td>
<td>• Traction control</td>
<td>• Crumple zones</td>
</tr>
<tr>
<td>• Vehicle separation</td>
<td>• Collision avoidance technology</td>
<td>• Defensive driver training</td>
<td></td>
</tr>
</tbody>
</table>

A421246  03/07/2015
• What does any of this have to do with organisational psychology?
• Humans interact with control measures
• Human error is a potential failure mechanism
• Errors can contribute to events
• We can consider the role of error:
  – in MAE causation
  – in the efficacy of control measures
  – in demonstrating ALARP
• Where do we start?
Critical human tasks

• Activities people are expected to perform:
  – as barriers against the occurrence of an incident
  – to prevent escalation
  – to support or maintain physical and technological barriers

Case study: BP Texas City refinery

• What is the MAE?

• What is the hazard?

• What is the critical human task?
Event summary

- March 23, 2005, 1:20pm
- Isomerization unit start-up
- Operators overfilled the raffinate splitter tower
- Pressure relief devices activated
- Flammable liquid spurted from a blowdown stack
- No flare installed
- Ignition, explosion and fire
- 15 deaths, 180 injuries
- $1.5 billion
• What is the MAE?
  – Explosion from hydrocarbon ignition

• What is the hazard?
  – Raffinate liquid

• What is the critical human task?
  – Operators were required to maintain the correct level of liquid in the raff tower
• Video - US Chemical Safety Board investigation
  – Human factors extract

• List the controls that failed
  – Where do they fit on the hierarchy?
Hierarchy of control

- **Eliminate**
  - Remove the hazard

- **Prevent**
  - Lower the likelihood

- **Reduce**
  - Detect and limit escalation

- **Mitigate**
  - Protect life
https://youtu.be/XuJtdQOU_Z4?t=35m6s

Note: Human factors content concludes at 44:17, video continues with other findings
<table>
<thead>
<tr>
<th>Control measures at BP</th>
</tr>
</thead>
</table>

### Eliminate
- Not possible

### Prevent
- Control Panel
- Instrumentation
- Alarms
- Supervision
- Communication
- Training
- Procedures
- Personnel

### Reduce
- High level alarms
- Instrumentation
- Pressure relief devices
- Procedures

### Mitigate
- Blowdown drum
- Vent stack
• Control panel
  – Flow data split between screens
  – No material balance indicator
• Instrumentation
  – Malfunctioning
• Alarms
  – Routine violation to fill tower past 9 feet
• Supervision
  – Absent
Prevention (2)

- Communication protocols
  - Poor
- Training
  - Poor quality
  - Poor risk awareness
- Procedures
  - Outdated
- Personnel
  - Not enough
• High level alarms
  – Broken
• Instrumentation
  – Malfunctioning
• Pressure relief devices
  – Switched to manual operation

• Possible but not present
  – High level ‘trip’ on tower
• Blowdown drum
  – Worked as designed
• Vent stack
  – Not upgraded to flare system
Multiple controls

Prevent
- Control Panel
- Instrumentation
- Alarms
- Supervision
- Communication
- Training
- Procedures
- Personnel

Reduce
- High level alarms
- Instrumentation
- Pressure relief devices

Mitigate
- Blowdown drum
- Vent stack
Multiple failures

Prevent
- Control Panel
- Instrumentation
- Alarms
- Supervision
- Communication
- Training
- Procedures
- Personnel

Reduce
- High level alarms
- Instrumentation
- Pressure relief devices

Mitigate
- Blowdown drum
- Vent stack
• How can we reduce error risk to ALARP?

• \( \text{risk} = \text{likelihood} \times \text{consequence} \)
Reducing error risk

- Organisation
- Individual
- Job

**Error Prevention**

- Minimise likelihood

**Error Mitigation**

- Minimise consequence
- Event
- Near Miss

**Human Reliability**

- Desired Performance
- Human Error
Prevent and mitigate error
Knowledge-based mistake

Prevention Controls

Mitigation Controls

Incorrect knowledge

Fatigue

Misleading HMI

Poor handover

Insufficient personnel

Tower overfill
Error prevention

- Incorrect knowledge
  - Training
  - Simulation
- Fatigue
  - Policy
  - Training
  - Drills
  - Competence assurance
- Misleading HMI
  - HF in design
  - Risk indicators
  - Communication conventions
  - Planning rules
  - Quality indicators
- Poor handover
  - Procedure
  - Risk indicators
  - Policy
- Insufficient personnel

Knowledge-based mistake
Error mitigation

Knowledge-based mistake

- HMI
- Maintenance
- Error management training
- Drills
- High-level trip
- Tower overfill
• Evidence-based practice!
• Evidence of uncontrolled error:
  – Events
  – Dangerous occurrences (could have but didn’t)
• Performance-shaping factors
  – Latent conditions
  – Broader implications
How to reduce error risk

- Identify critical human tasks
  - What errors are possible?
  - What are the consequences?
  - What are the performance-shaping factors (hazards)?

- Identify existing controls
  - Do they prevent and mitigate error?
  - Is risk reduced to ALARP?

- Develop appropriate controls
  - Eliminate the opportunity for error
  - Prevent – lower the likelihood of error
  - Reduce – facilitate error identification and recovery
  - Mitigate the consequences of error
• Human error can contribute to events
• Error risk is most significant for critical human tasks
• Apply a hierarchy of controls to reduce error risk
• Effective risk reduction includes:
  – error prevention
  – error management
• nopsema.gov.au
Questions?