30 years ago it had never happened

The Cullen Report sought to answer two questions. First, what were the causes and circumstances of the disaster and, second, what should be recommended to avoid such accidents in the future?

The immediate cause of the disaster was a failure in the permit to work system which caused a breakdown in communications between the day shift and the night shift. This led to the use of machinery which was undergoing maintenance and caused the escape of gas from an insecurely fastened temporary flange. Thereafter, there appeared to be a series of failures and errors of judgment which contributed to the overall scale of the disaster. Many of the men on board were unfamiliar with the layout of the platform and had not been trained properly in emergency procedures. Those in the accommodation block were encouraged by the installation manager to stay there to await rescue. Yet as the Cullen Report makes clear to remain there meant certain death.

A number of the emergency systems on the platform failed immediately or within a short time of the original explosion. In particular, the fire-water system was rendered inoperative either due to loss of power or physical damage. In any case, at the time of the disaster the diesel fire pumps were on manual mode so that, even if they had not been disabled, they would have required manual intervention in order to start them.

Personnel on neighbouring platforms were ill-prepared for a disaster on another platform connected to their own. Gas and oil continued to flow from these other platforms to Piper Alpha. This continued flow which the other platforms were unable to shut off contributed to the further explosions and fires on Piper Alpha.

The rescue arrangements were also criticized. The standby vessel, Silver Pit, was unsuitable for the purpose of effecting the rescue of survivors. The searchlight was not working, the boat was not sufficiently manoeuvrable and it was unsuitable for handling the injured. In a damning criticism of the fire-fighting vessel, The Tharos, Lord Cullen argued that it proved to be 'the most expensive white elephant in the North Sea'.

It was clear that the responsibility for many of these failings had to lie with the owners of the platform, Occidental Petroleum. Lord Cullen criticized the management of Occidental for not being as prepared for a major emergency as they should have been and blamed them for “adopting a superficial attitude to the risk of major hazards”. Frequently, the company failed to devise and put in place appropriate safe systems capable of responding to the sorts of foreseeable dangers inherent in oil and gas production. Even where safety arrangements were in place these were frequently broken. In particular, although the company did have a permit to work system which was intended to control certain types of work which were potentially dangerous in a number of significant respects this PTW system was habitually or frequently departed from.

What would you do if your searchlight wasn’t working, you had a fire pump under maintenance, an SSIV compromised and a pump under a PTW?
• Welcome
• History and impact
• Industry examples
• Activity – Case Study
• Operational decision-making
• Outcomes and key themes
• Reg. 2.5(2)(a) and 2.5(c)  
  – Potential loss of containment & risk to people, environment, assets & reputation  
• Reg. 2.16, 2.18 and 2.20  
  – Emergency preparedness and EERA  
• Reg. 2.8  
  – Command structure  
• Reg. 2.11  
  – Workforce involvement
Introductions

• Rob Brown

• Joelle Mitchell
Why a workshop, not a presentation?

- Engagement not imposition
- Listen and seek to understand
- Recognise the issues and their impact on perceptions of our industry
- “The mind works best like a parachute”
- Generate discussion and material for a guidance note
- Recognise that many scenarios, failures, events are foreseeable
• Promote consistent:
  – Expectations
  – Decision-making processes
  – Outcomes for addressing foreseeable failure
  – Outcomes for addressing unforeseen failure

• Generate discussion
  – Guidance Note material
  – Adapted from Oil & Gas UK
  – Industry recognised
  – “Guidance on the Conduct and Management of Operational Risk Assessments for UKCS Offshore Oil and Gas Operations”
• A word from our sponsor...
Topics that may contribute to issues surrounding operational risk:

- Notification and reporting requirements to NOPSEMA
- Titleholder risk – environment, well integrity
- Risk Based Inspections
- Quantitative Risk Analysis
- ALARP & Reverse-ALARP
- Clarity of performance standards
History & impact
• NOPSEMA has observed:
  – Operators continuing to operate with degraded or unfavourable MAE controls or conditions, without additional controls in place
  – Reliance on change management processes to permanently accept degraded SCEs

• Consequences:
  – Risks at the facility ≠ risks allowed for in the accepted safety case
  – The temporary elevated risk may become normalised as the new ALARP without an accepted safety case revision
1.1 Intent and Purpose
   - ‘A facility operator’s procedures for risk management need to be comprehensive such that they accommodate and account for adverse changes in safety-critical equipment (SCE) provision, or other abnormal situations, that may potentially increase levels of major accident event risk.’

2.1 When is ORA Necessary & Appropriate
   - 2.1.1 Contingency Planning for SCE Impairment

2.2 Organisational Factors
2.3 Planning and Implementation
   - 2.3.1 ORA Methodology & Key Considerations
     – Initial Response Action
     – Preparation and Readiness for Conduct of ORA
     – Description of SCE Failure and Hazard Identification
     – Identification of Mitigation Measures
     – Assessment of Residual Risk & Risk Determination
     – ORA, ALARP and Risk Acceptability
     – Combined Risk
     – Review, Endorsement and Approval
     – Validity Period
     – Recording & Communication of ORA

3 Operational Risk in a Broader Change Management Framework

Inclusion of Contingencies within the Safety Case
Consideration should be given to including contingencies and mitigation measures to be implemented on impairment of SCE within the safety case, e.g. loss or degradation of a fire water pump may lead to restrictions in the operational activities that can be safety undertaken at the facility until full functionality and performance of the firewater pump can be restored.

Operational risk assessment should not be utilised for long-term or permanent SCE impairment; as this would typically be considered a modification triggering a safety case revision in accordance with Regulation 2.30 of the OPGGS (Safety) Regulations 2009.

It is particularly important to stress to ORA participants that may be more familiar with conducting Job Hazard Assessments, that they are undertaking an ORA and that a major accident event mindset is required.

It should be emphasised that a determination of ‘Low’ likelihood cannot be used to support continued operations without effective mitigation measures being in place, as the entire major accident event regulatory regime is based around low likelihood, high consequence events.

Depending on the nature of the SCE Impairment e.g. failure on demand, failure triggering a requirement for the emergency response plan to be implemented, etc. there may be a requirement to notify NOPSEMA of a dangerous occurrence in accordance with Clause 82 of Schedule 3 to the OPGGSA 2006.

The particular importance of the role of Technical Authorities and SCE Responsible Engineers (or equivalent titles) in the ORA process should be stressed in the facility operator’s procedures.
Lifeboats
  - Perished seat-belts on Lifeboats
    - Notification (safety case revision)
    - Minimise POB to match “good seats”
    - Impact of loss of availability

Class & Asset Integrity – 2 examples
  - Classification society agree to defer a 5-yearly tank inspection
  - Inspections not conducted
  - Notification to NOPSEMA was not timely (offence)

Actual Surface Temperatures
  - A gas turbine for a generator
  - A gas turbine for a compressor
  - A crane engine
  - Steam distribution piping
  - Temporary equipment

Helicopter transportation
  - Helideck out of certification and condemned from an asset integrity assessment
  - Commenced boat transfers
  - Safety Case revision – controls (medevac, SBV)

EEHA & Ex-equipment
  - Non-compliant paperwork in commissioning & acceptance
  - No detailed inspections over the life of the facility
  - Failed inspection – sampled to full population of tags
    - Many devices & statistical significance vs. certainty
    - Likelihood of hazard:
      - Hazardous area definition versus requirement to operate in a emergent hazardous atmosphere (IP15 to Major Release)
      - Fault condition & atmosphere (compare with hot-surfaces)

SIL - SIS & FSA requirement (IEC 61511)
  - SIS installation and commissioning
  - Failure rates not met

Drift-on & Blow-on: Diving & Supporting Vessels
  - Innovative feature
  - Emergency Compressed Air System (ECAS)
  - Selecting the vessel and what if ECAS not available?

Self Propelled Hyperbaric Life Boats
  - What if not available?
• ESDVs
  – Failure on demand vs. e.g. leak failure
  – Acceptability of failure rate
    • Based on overall failure rate, failure rate of specific valve or any failure?
    • Failure tolerance, attitude and behaviour towards compliance and actual safety

• Inert Gas Fire Suppressant systems
  – Late Life facility:
    • Compliance with test intervals (10% of cylinders)
    • Failure of cylinders – not reported – wall failure and depressurised
  – New facility:
    • Unintended release
    • Design verification and commissioning issues (full system loop testing)

• Minimum & reduced manning
  – Contingency planning included on a minimal manned facility to prevent higher risk work when manning levels are compromised

• Activities / circumstances not described, nor risks identified, in the safety case
  – Extended and excessive venting during abandonment
    • Appropriateness of analysis and controls
  – Third Party equipment

Perception or Problem

• Cranes
  – Crane Control failure
    • Unreliable crane control joystick assemblies (potentiometer)
    • Undesired movement and reliability issues for many years

• Temporary repairs
  – Piping
    • Wrap registers; design codes and standards
  – Scaffolding
    • >12 months; > 36 months; > 60 months
    • Used as primary pipe supports

• Mothballing vis-a-vis decommissioning
  – Preservation and passivation
    • Do they become safety critical tasks?
    • Fully complying with the IMT and integrity requirement for 'Out of Service' equipment
  – Sail-away commitments

• SSSVs and SSIV
  – Good practice but ever had a demand?
  – Likelihood of requiring them is already low – $4 \times 10^{-5}$
  – Testing frequency versus planned shut-down frequencies (and the pressure equalising difficulties)
  – OHS risk of repair and replacement?
  – Long lead repair items
Maximum Specified Risk Level*  

Suspend Operations  

Post-Mitigation ALARP Risk Level  

Mitigating Controls Implemented  

Remedial Controls Implemented  

Duration of exposure above Normal Operating Risk Level should be minimised whenever possible.

Normal Operating ALARP Risk Level (All SCE Available)  

SCE Post-Remediation ALARP Risk Level  

Shut down until contingency measures established  

Contingency measures established in safety case applied

* As provided for in the Performance Standard
Case Studies
Abigail and Gregory are in love. Abigail lives on an island off the coast of the mainland where Gregory lives. The ocean channel separating the island from the mainland is teeming with White Pointers.

Abigail wants to cross the channel to be with Gregory, but the bridge connecting the island to the mainland has collapsed.

Abigail asks Sinbad, the ferryman, to take her across the channel. Sinbad agrees on the condition that she consent to go to bed with him prior to the voyage.

Abigail refuses and seeks assistance from her friend Ivan. Ivan does not want to get involved. Abigail feels that she has no alternative but to accept Sinbad’s terms.

On arrival at the mainland, Abigail tells Gregory about her ordeal. Gregory, disgusted, casts her aside.

Abigail turns to her friend Slug, also on the mainland, with her tale of woe. Slug seeks out Gregory and beats him brutally.
• Rank each character according to their behaviour, from most (5) to least (1) ethical:
  – Abigail
  – Gregory
  – Ivan
  – Sinbad
  – Slug
• Additional information:
  – Sinbad is Gregory’s best friend
  – Abigail and Gregory have an *arrangement* in place for times of separation
  – Gregory has three *friends with benefits* on the mainland
  – Slug knows that his newly pregnant daughter was, until recently, one of Gregory’s *friends*
  – Ivan is responsible for bridge maintenance and owns the ferry company

• Does this change your rankings?
Case Study 1: Hot Surfaces

- Operator A has discovered a hot spot on the exhaust stack of a gas turbine.
- Turbine is adjacent to the accommodation block:
  - Tri-fuel: condensate, diesel and gas; normally on gas.
  - T3 temperature classification 200°C, hotspot is 350°C.
- It’s on a compressor adjacent to a debutaniser?
  - T3 classification (200°C), hotspot is 290°C.
- Actually it’s on both.
- The operator has only one performance standard relating to hot surfaces.

- Multiple sources of actual surface temperatures:
  - A gas turbine for a generator.
  - A gas turbine for a compressor.
  - A crane engine.
  - Steam distribution piping.
  - Temporary equipment.

- Key issues:
  - Application of codes.
  - Hazardous area versus non-hazardous.
  - What ‘down-incident’ remaining controls (‘Swiss cheese’) are available.
  - Nature of fluids (crude, gas, condensate, LPGs, LNGs).

- Additional controls – isolate equipment, shut-down etc.
- What is the impact? (loss of one unit versus, loss of crane, versus shutting-down).
Case Study 2: Emergency Shut Down Valves

SSIVs – Actuator failed - multiple operators reasoning:
- Locked open
- Was designed-in as a RRM – ‘contemporary good practice of the day’
  - but repair is expensive and lengthy
- Risk matrix has changed since design
- ‘Current’ ORA indicates negligible RRM for most fire/release scenarios
- Likelihood of demand is very very low
- In one case the installation is not normally manned; in another the TR is 200m away; or could disconnect & sail-away

Additional measures?
- MoC; TOPs etc?

ESDV – multiple operators
- During a facility shutdown ‘ESDVs’ and ESD supportive systems are initiated
- ESDV failed to fully close on demand coupled with an solenoid incorrectly installed
- Incidents related to ‘failure of an SCE to meet performance standard’ is notifiable under the category ‘damage to SCE’
- The valve data logs present data of ‘valve timing closure as per the SCE’s performance standard’
- During a similar ESD event a number of valves fail to meet their performance standard
- Immediate replacement then OEM inspection
- Other considerations:
  - API 14C section valve
  - Installed bypass on manual control for maintenance (stroke testing)
  - Removing the ESDV for maintenance and requirement in terms of SIL-SRS
  - Pre-maintenance of valves to assure performance test closure test achieved?
The facility is an Oil & Gas FPSO disconnectable turret

- **2 x 100% diesel driven fire pumps installed**
- **30,000 BOPD rich condensate (API-47)**
- **100 MMSCF/D of dry gas export or capable of gas injection into reservoir at 60 mmscf/d**
- The GTG is tri-fuel; gas, diesel and/or condensate; GTGs with waste-heat recovery system used primarily for generating steam for regeneration in the TEG system; which in turn is used for gas dehydration to sales-gas specification
- There is a Deck Boiler used for IG generation during offloading

It is August and the FPSO is at maximum POB (120)

- A diving campaign which had required regular isolation of a fire pump (one pump at a time) was completed 4 weeks ago
- 60 of the POB form the fabrication, rope access and scaffold squads executing a 4-month (critical path), US$12million PFP upgrade project
- The project is fully mobilised and 3 weeks into execution

The PFP project risk assessments considered:

- The risk was acceptable to conduct the work offshore, completing the PFP project before cyclone season substantially reduces the OHS and MAE risk
- A risk reduction measure option to conduct the work at next-year’s Singapore shipyard 5-yearly class inspection (actually 6th year as class agreed to defer in-lieu of additional offshore inspections) was considered and rejected
- Shipyard was less CAPEX and duration (4 weeks vs. 4 months), but production deferment of 2 weeks was grossly disproportionate to the risk reduction

The OIM reports the aft fire pump (Pump A) engine is damaged rendering the pump inoperable.

- The OEM indicates it is a known issue (3% failures) on these engines when they have been in service for 8 years; this unit has been in operation for 9 years
- The engine insurance spare was recently inspected and found to be poorly preserved; a supply chain initiative released it back to the manufacturer
- The OEM indicates the repair will take 4-7 days at the shipyard or 3 weeks offshore; replacement parts are 5 weeks ex-Singapore
• You are the facility management team
  – OIM, Maintenance lead, Production lead, Marine lead, other support members
  – You must decide how to proceed
  – You have 30 minutes
  – 5 minutes to present your argument to the COO
Operational decision-making
The operational context

Productivity

Safety

Workload efficiency

Economic efficiency
The individual context

- Complexity
- Risk
- Uncertainty

Underspecified
Do these things happen?

- Emergency generator out of service
- FRC unavailable / unable to launch
- Standby vessel under restricted service / need to return to port
- Fire / Gas detectors failed or long-term inhibition for project work
- Wells:
  - SSSVs fail
  - Annuli require blowing down
  - Plugs leak / fail
Preference?
• Time
• Reduced goal conflict
• Availability of expertise
• Dispassionate decision-making
• Provides certainty for operations
• Reduces regulatory burden
Duration of exposure above Normal Operating Risk Level should be minimised whenever possible.

Mitigating Controls Implemented

Remedial Controls Implemented

Shut down until contingency measures established

Contingency measures established in safety case applied

* As provided for in the Performance Standard

>30 days

Suspend Operations

Maximum Specified Risk Level*

Post-Mitigation ALARP Risk Level

SCE Post-Remediation ALARP Risk Level

Normal Operating ALARP Risk Level (All SCE Available)
Outcomes
Performance & Lower Compliance risk:
\[ \int(x) = \int(\text{Safety Case detail & description}) + \int(\text{clarity of performance standard criteria}) + \int(\text{Contingency Planning}) + \int(\text{ORA processes}) \]

<table>
<thead>
<tr>
<th>Contingency Planning</th>
<th>Unforeseen Failure, Impairments or Conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assessment &amp; Inspection</td>
<td>MOPO or ORAs</td>
</tr>
<tr>
<td>MOPO &amp; ORAs</td>
<td>Curtail &amp; additional measures</td>
</tr>
<tr>
<td>Shut-in</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Contingency Planning</th>
<th>Unforeseen Failure, Impairments or Conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assessment &amp; Inspection</td>
<td>MOPO or ORAs</td>
</tr>
<tr>
<td>MOPO</td>
<td>Curtail &amp; additional measures</td>
</tr>
<tr>
<td>Shut-in</td>
<td></td>
</tr>
</tbody>
</table>

\( x = \text{Time in Operation} \)
ORA success factors & considerations

• Organisational culture and behaviour
  – You get what you tolerate
  – Motivation: Avoid pain or achieve a gain?
  – Entrepreneurship, innovation

• People
  – Training and competency
  – Defined roles and responsibilities
  – “Perfect team vs. the perfect individual”
  – Knowledgeable about the issues;
    The goldilocks-zone of ownership (too much can obscure, too little to care)
  – Impartial arbiter or decision maker

• Tools
  – Optimum environment: High pressure or low pressure
  – Defined decision-making style: Consensus, Delegate, Democratic, Command, Consensus, Unanimous
  – Quantitative vs. Quasi-Quantitative vs. Qualitative
    • Appropriateness of a RISK MATRIX to impaired circumstances?
    • Right tool & technique: Techniques deployed to determine the intended ‘long term’ residual risk (e.g. HAZOP, LOPA, HAZAN) may need to be adapted for short-term

To ACHIEVE a CONSISTENT and RELIABLE OUTCOME ...
may require a CONSISTENT and RELIABLE APPROACH

• Right Commitment
• Right People
• Right Knowledge
• Right Motivations
• Right Assumptions
• Good Tools
• Process focused not Outcome focused?
ORA success factors & considerations

- Jurisdiction of an ORA and the default position?
  - Continue operation vs. shutdown may be different than restart vs. remain shut-in
  - Is it a function of how it was discovered?

- Initial Response – prior to concluding ORA
  - Defined validity and duration?

- Conducting ORA (see Guidance Note):
  - Data gathering
  - Readiness:
    - Concise description of unfavourable (impaired) change or non-normal condition
    - Risk evaluation ‘as-seen’
  - Assessment, Determination, Approval
    - Risk estimation
    - Identification of further measures / controls
      - Determine if MUST do, SHOULD do, COULD do
    - Assess complementary, antagonising and combined risk
    - Determine residual risk
    - What other risk reduction measures can be considered
      - Full commentary or commentary by exception
      - Account for all measure based on proportional of burden in light of the ‘compromised’ situation / state
  - Approval by Asset and Impartial SME/TA
    - with DEFINED validity duration and target completion for returning to intended situation

To ACHIEVE a CONSISTENT and RELIABLE OUTCOME ...
may require a CONSISTENT and RELIABLE APPROACH
- Right Commitment.
- Right People
- Right Knowledge
- Right Motivations
- Right Assumptions
- Good Tools
- Process focused not Outcome focused?
1.1 Intent and Purpose

- 'A facility operator’s procedures for risk management need to be comprehensive such that they accommodate and account for adverse changes in safety-critical equipment (SCE) provision, or other abnormal situations, that may potentially increase levels of major accident event risk.'

2.1 When is ORA Necessary & Appropriate

2.1.1 Contingency Planning for SCE Impairment

2.2 Organisational Factors

2.3 Planning and Implementation

2.3.1 ORA Methodology & Key Considerations

- Initial Response Action
- Preparation and Readiness for Conduct of ORA
- Description of SCE Failure and Hazard Identification
- Identification of Mitigation Measures
- Assessment of Residual Risk & Risk Determination
- ORA, ALARP and Risk Acceptability
- Combined Risk
- Review, Endorsement and Approval
- Validity Period
- Recording & Communication of ORA

3 Operational Risk in a Broader Change Management Framework
Guidance Note: Indicative Flowchart

- **SCE fails to meet performance standard specification**
  - Contingency identified within the Safety Case?
    - Yes
      - Existing process to manage the abnormal condition
        - Yes
          - Use the existing process
        - No
          - Shutdown / Isolate plant or equipment
    - No
  - Safe to operate with abnormality whilst ORA is conducted?
    - Yes
      - Change to plant or process?
        - Yes
          - Management of Change (MoC) process will be required to implement change.
        - No
          - Raising a procedure to manage the risk?
            - Yes
              - Note. The change may trigger a revision to the safety case under Reg. 2.30
            - No
              - Raising a permanent procedure to fully address SCE failure?
                - Yes
                  - ORA required to assess and manage the abnormal condition
                - No
                  - ORA required to assess and manage the abnormal condition whilst procedure is developed.
            - No
              - ORA required to assess and manage the abnormal condition
  - No
    - ORA must identify that residual risk is As Low As Reasonably Practicable
      - Yes
        - Use the existing process
      - No
        - ORA required to assess and manage the abnormal condition
          - ORA removed once changes implemented and MoC process completed
          - ORA removed once abnormal condition rectified
          - ORA removed once procedure approved and implemented
          - ORA removed once abnormal condition rectified
• Summary of activities and discussions
• Address parked items
• Guidance Note
Thank you