AGENDA

- Setting the Context: “Begin with the end in Mind”
  - What is the goal?: 4 P’s
  - Drivers: The Industry Landscape
  - How is this managed?: A “Management of Risk” Model
- Process Hazard Analysis:
  - When to start and what PHA methods apply?: Life cycle model
  - Success Factors and Potential Pitfalls
  - Methods: HAZID; HAZOP; LOPA/SIL; FMEA: Inputs/Process/Outputs
- Critical Technical Safety Studies: Inputs/Process/Outputs
  - Human Factors; Dispersion and Consequence Modelling; Fire and Explosion Analysis; Facilities Siting Study; Emergency Systems Survivability Analysis; Quantitative Risk Assessment
- Governance and Assurance
  - Sustainability Model
  - Baseline: Risk Matrix
  - Review and Verify: BowTie Analysis
  - Continuous Improvement: Lessons Learned
- Conclusions and Summary
Setting the context: What is the goal?

- Stephen Covey Habit: “Begin with the End in Mind”

- For a Company:
  - Why do we exist?
  - What do we require?
  - How is that achieved?
  - Who is going to do it?

- The 4 P’s Concept
Setting the Context: BASIS FOR COMPLIANCE

- Check the box?
- Meet regulatory minimum compliance? Relevance? Currency?
- What about best practices – RAGAGEP?
- Is it an organizational Core Value?

RELEVANT REGULATIONS AND STANDARDS
- DOT - PHMSA
- NFPA
- ASME B31

RAGAGEP
- OSHA PSM;
- EPA-RMP;
- BSEE – SEMS;
- Safety Case (UKHSE; NOPSEMA);
- API 1173
- IEC 61508/61511: SIL
Setting the Context: What are the drivers?

- What are the drivers to enable the goals?
Setting the Context: How is this managed?

MANAGEMENT OF RISK

- Events/Incidents
  - Incident Management
    - Management of Change
      - Process Hazard Analysis (HAZID, HAZOP, LOPA/SIL, FMEA)
        - Lessons Learnt
  - Risk Management
    - Establish Context
      - Risk Identification
        - Risk Analysis
          - Risk Evaluation
            - Risk Treatment
  - Bowties and Controls
  - Critical Equipment Register

Risk Register

Engineering and Administrative Performance Standards

- MOC
- PHA
- CoW - PTW
- PSSR
- Contractor Mgmt.
- Incident Mgmt.
- M'tce Strategies
- ERP
- Critical Procedures
- SDS/Chem. Mgmt.
- Integrity M’gnt. Etc.

Dashboard Health Checks

Self Assessment Assurance

ACTION TRACKING AND REPORTING

TRAINING AND COMPETENCE

DOCUMENT MANAGEMENT
When to start and which Process Hazard Analysis applies?

When to carry out a PHA: Facility Life Cycle?

Which PHA type is applicable?
Setting the context: What is the goal?

- PHA selection based on the:
  - Size and complexity of the facility
  - Duration and complexity of the activities or life cycle phase being considered
  - Nature of the activities and processes associated with the facility

- The selected PHA should:
  - Be systematic and structured
  - Foster creative and lateral thinking about possible hazards including those not previously experienced
  - Be appropriate for the facility and the stakeholders
  - Consider which approach will extract the maximum quantity of useful information
PHA Success Factors

- Active stakeholder engagement and input in the PHA process
- A comprehensive and accurate description of the facility: drawings, process information, existing conditions, modifications, procedures and work instructions, hazardous materials information, etc.
- Systematic and structured, fostering creative thinking inclusive of extracting the maximum quantity of useful information
- Assumptions and uncertainties are explicitly identified and recorded
- Documented records that provides potential major accident events (MAEs) and hazards along with the underlying causes/consequences, control measures and any assumptions
- “SMART” (specific, measurable, attainable, realistic and timely) actions that can be managed and closed out through an auditable trail
PHA Potential Pitfalls

- Complacency: Just because an incident has not occurred in the past does not mean that it can’t happen in the future.
- Being too generic: in identification of hazards and potential MAEs. Causes and consequences need to provide plausibility and specificity.
- Determination of the underlying cause and not the symptom.
- Lack of understanding and assessing impacts from varying process conditions and activities (start-up; shut-down; emergency shut-down; maintenance etc.)
- Inadequate documentation: insufficient recording of underlying assumptions, uncertainties, knowledge gaps, hazard details, incidents, effectiveness of control measures, etc.
- Equal stakeholder participation: seeking full engagement.
PHA: HAZID

There are different types of Hazard Identification Methods employed: What-If/Checklist or HAZID

- **Inputs:**
  - Activities at the specific location
  - Risk Matrix, Tolerability criteria and existing effective controls
  - List of applicable Guidewords

- **Process:**
  - Brainstorming using SMEs, Guidewords, Risk Assessment
  - Documented in spreadsheet template or software

- **Outputs:**
  - List of main hazards
  - List of effective safety measures/controls
  - Gaps in existing control measures
  - Recommendations and actions to address gaps
PHA: HAZOP

- **Inputs:**
  - Documentation to support scope: P&IDs; Safe Charts; Operating Limits; PFDs; BOD; incident reports
  - Core team of Subject Matter Experts
  - Definition of the respective boundaries to be assessed (nodes)
  - Risk Matrix, Tolerability criteria and existing effective controls
  - List of applicable Guidewords

- **Process:**
  - Using SMEs, Parameters and Guidewords, Risk Assessment
  - Documented in spreadsheet template or software

- **Outputs:**
  - List of deviations from design intent (causes/consequences)
  - List of effective safety measures/controls
  - Gaps in existing control measures
  - Recommendations and actions to address gaps
PHA: LOPA / SIL

**Inputs:**
- From HAZOP/QRA: hazardous events, frequency, consequence, controls
- Documents: P&IDs; Cause and Effect Chart; Operating Limits; PFDs; BOD; incident reports
- Rules/Criteria: frequencies – initiating cause (ICL); maximum acceptable (MAF); probability of failure on demand (PFD); conditional modifiers (CM); Safe Failure Fraction (SFF)

**Process:**
- Identify Independent Protection Layers (IPLs) and type
- Calculate the LOPA Ratio (LR): MAF
- For LR<1: identify additional IPL and/or SIS
- Document in spreadsheet template or software

**Outputs:**
- List of effective layers of protection (safety measures/controls)
- Safety Instrument System and Safety Integrity Level
- Gaps; recommendations and actions to address gaps

---

**Table 1:**

<table>
<thead>
<tr>
<th>Initiating Cause</th>
<th>Likelihood (Frequency)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pressure vessel failure</td>
<td>10^-4</td>
</tr>
<tr>
<td>Piping failure - 100m - full breach</td>
<td>10^-5</td>
</tr>
<tr>
<td>Piping leak (10% section) - 100m</td>
<td>10^-5</td>
</tr>
<tr>
<td>Atmospheric tank failure</td>
<td>10^-6</td>
</tr>
<tr>
<td>Gasket / packing failure</td>
<td>10^-7</td>
</tr>
<tr>
<td>Turbine / diesel engine over speed with closing blade</td>
<td>10^-8</td>
</tr>
<tr>
<td>Third party intervention (external impact by blast, fire, vehicle, etc.)</td>
<td>10^-9</td>
</tr>
<tr>
<td>Crane load drop</td>
<td>10^-9/10</td>
</tr>
<tr>
<td>Lightning strike</td>
<td>10^-9</td>
</tr>
<tr>
<td>Safety valve operates spuriously</td>
<td>10^-9</td>
</tr>
<tr>
<td>Cooling water failure</td>
<td>10^-10</td>
</tr>
<tr>
<td>Pump seal failure</td>
<td>10^-10</td>
</tr>
<tr>
<td>Unloading / loading hose failure</td>
<td>10^-11</td>
</tr>
<tr>
<td>BPCS instrument loop (sensor, controller and element failure)</td>
<td>10^-12</td>
</tr>
<tr>
<td>Regulator failure</td>
<td>10^-12</td>
</tr>
<tr>
<td>Small external fire</td>
<td>10^-13</td>
</tr>
<tr>
<td>Large external fire</td>
<td>10^-13</td>
</tr>
<tr>
<td>Overall failure of multiple element process (e.g. &quot;buck-out&quot; blowout procedure)</td>
<td>10^-14/15</td>
</tr>
<tr>
<td>Operator failure to execute routine procedure (assumed well trained, uninterested, not fatigued)</td>
<td>10^-14/15</td>
</tr>
</tbody>
</table>

**Source:** "Layer of Protection Analysis" CCPS, 2001
PHA: FMEA

- **Inputs:**
  - Equipment or system/sub-system to be evaluated
  - Documentation: system specifications; equipment lists; drawings; incident history
  - Risk Matrix and Tolerability criteria
  - Failure Modes to be evaluated
  - Scenarios

- **Process:**
  - Evaluate response to various failure modes – causes and effects
  - Assess suitability of controls
  - Document in spreadsheet or software

- **Outputs:**
  - List of methods to detect failures
  - Recommendations and actions
  - Further analysis requirements
TECHNICAL STUDIES: Human Factors

• A study of the behavior of man in the organizational environment to better understand their motivations and identify the causes of errors.

• Human Factors Engineering focuses on under normal, abnormal and emergency conditions:
  • Operability: design and layout of equipment is optimised for safe, efficient, and logical access and operation
  • Maintainability: requirements for safe and efficient maintenance tasks have been incorporated into design: workspace and lay down; consideration of maintenance access and reducing work content; equipment criticality analyses
  • Access and Egress: areas of the facility, modules, and equipment can be accessed and evacuated safely and efficiently: handrails; ladders; stairs; ramps
  • Manual Materials Handling: requirements for manual lifting, pulling, pushing, and carrying of equipment, with respect for the capabilities and limitations of the personnel
  • Communication/Labelling: equipment identification and communication of operational and maintenance information: displays; alarms;
  • Environmental: working environment factors in the interests of human health, safety and performance: lighting; HVAC; noise and vibration; chemicals
  • Constructability: Ensure ease and safety of construction and installation operations.
TECHNICAL STUDIES: Dispersion and Consequence Modelling

- **INPUTS**
  - Identified parameters: leak scenarios; type of risk effects; discharge – composition/volume/hole sizes/duration/direction; operating and environment conditions
  - Plot plan
  - Rule sets and parameters applied for the effects of thermal radiation: vulnerability

- **PROCESS (key criteria)**
  - Ignition source (flammable effects including fireballs, jet fires, pool fires and flash fires.)
  - Resource manning and location
  - Equipment spacing
  - Site accommodation

- **OUTPUTS**
  - Contour mapping of the dispersion cloud that includes the Lower Flammable Limit (LFL) for flammable gas or concentration recommended in SDS for toxic gas
  - Contour mapping of thermal radiation and temperature/pressure profiles
TECHNICAL STUDIES: Fire & Explosion Analysis

- **INPUTS**
  - Accident scenario development
  - Explosion, toxic and fire hazard prediction
  - Risk and consequence evaluation
  - Hazard management near portable buildings
  - Occupancy, explosion consequence and risk screening analysis
  - Structural assessments of existing buildings for blast loads and modelling
  - Facility siting guidelines and corporate risk criteria development based on the following criteria: Operating conditions; Fluid composition; Plot plan; Weather/wind conditions

- **PROCESS** (key criteria)
  - Uses Consequence Modelling process

- **OUTPUTS**
  - Graphical display of consequence from explosion, blast, thermal radiation and fire (including smoke)
TECHNICAL STUDIES: Facilities Siting Study

- **INPUTS**
  - Accident scenario development
  - Explosion, toxic and fire hazard prediction
  - Risk and consequence evaluation
  - Hazard management near portable buildings
  - Occupancy, explosion consequence and risk screening analysis
  - Structural assessments of existing buildings for blast loads and modelling
  - Facility siting guidelines and corporate risk criteria development based on: Operating conditions; Fluid composition; Plot plan; Weather/wind conditions
  - Risk tolerability criteria

- **PROCESS** (key criteria)
  - Uses Consequence Modelling process

- **OUTPUTS**
  - Contour mapping of thermal radiation and temperature/pressure profiles
  - Hazardous Area Classification
TECHNICAL STUDIES: Emergency Systems Survivability Analysis

- **INPUTS**
  - Risk Register
  - Plot Plan and Equipment Layout
  - Impacts/Consequences

- **PROCESS** (key criteria)
  - Identify the controls with emergency system applicability
  - Identify critical equipment and functionality of emergency actions
  - Assess vulnerability of critical equipment to major accident events
  - Conduct qualitative risk assessment of impact severity to critical equipment
  - Document outcome Risk Register identifying any gaps and additional analyses required

- **OUTPUTS**
  - Identify the Emergency Systems and their required functions.
  - Identify those Emergency Systems that could be impaired by Major Accident Events
  - For these Emergency Systems, assess their ability to perform their functions during an emergency.
  - Determine whether the Emergency Systems are adequate, or make recommendations for improvement where appropriate
TECHNICAL STUDIES: Quantitative Risk Assessment (QRA)

**INPUTS**
- Risk register
- Risk tolerability criteria (ALARP)
- Dispersion/Consequence Modelling
- Fire and Explosion Analysis
- Emergency Systems Survivability Analysis
- Rule sets: failure frequency and ignition probability; thermal radiation and overpressure vulnerability; process, occupational, transportation and societal risks

**PROCESS (key criteria)**
- Assess facility layout and population exposure
- Apply frequency and consequence analysis

**OUTPUTS**
- Risk contours and/or Frequency/Number fatality (FN) graphs
- Individual risk per annum (IRPA)
- Potential loss of life (PLL)

<table>
<thead>
<tr>
<th>Risk Region</th>
<th>IRPA (Most Exposed Person)</th>
<th>LSR (At Facility Boundary)</th>
<th>Treatment of Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intolerable Risk</td>
<td>$&gt; 1 \times 10^{-3}$</td>
<td>$&gt; 1 \times 10^{-5}$</td>
<td>A level of risk that is so high as to require significant and urgent actions to reduce its magnitude. If these risk levels cannot be reduced to ALARP or tolerable level, the project objectives and operating philosophy must be fundamentally reviewed by the management.</td>
</tr>
<tr>
<td>ALARP Region</td>
<td>$1 \times 10^{-5} &lt; \text{IRPA} &lt; 1 \times 10^{-3}$</td>
<td>$1 \times 10^{-7} &lt; \text{LSR} &lt; 1 \times 10^{-5}$</td>
<td>Efforts must be made to reduce risk further, and as far as can be achieved without the expenditure of a cost that is grossly disproportionate to benefit gained.</td>
</tr>
<tr>
<td>Tolerable</td>
<td>$&lt; 1 \times 10^{-5}$</td>
<td>$&lt; 1 \times 10^{-7}$</td>
<td>A level of risk that no further actions to reduce its magnitude further, but which will be monitored and managed by the site using its management system.</td>
</tr>
</tbody>
</table>

Source: CCPS publications; UKHSE
Governance and Assurance: Sustainability Model

Create/Review/Revise
Risk Management Process

Plan

Data Analysis;
Proactive interventions
Continuous Improvement

Act

Develop systems and Implement KPIs

Check

Embed: sustainability and consistency
Collate and trend data
Governance and Assurance: Baseline

Baseline:

- Using the Company’s Risk Matrix based on:
  - Severity Levels for Inherent Risk (no controls)
  - Likelihood Factors and Severity for Residual Risks (effective controls)
  - For all relevant Impact Categories

- Apply Tolerability Criteria
- Classify and Rank Risks

- Identify and implement improvement actions

- Documented in the Risk Register, inclusive of justifications/details
Governance and Assurance: Review and Verification

Source: CGE publications
Governance and Assurance: Lessons Learnt

![Lessons Learnt Flow Chart](image-url)
Conclusions and Summary:

- Compliance is not driven only by regulatory requirements: it is a Core Value.
- Profitability is a function of how risk is understood and managed.
- The life cycle of “Management of Risk” and the interdependencies need to be understood and applied.
- Selection of risk assessment methodology is driven by objectives/goals. No one PHA is applicable.
- Process Hazard Analyses are applicable from cradle to grave.
- Technical Studies are critical to understanding the risk impacts.
- Sustainability is essential to continuous improvement.
- Establishing risk tolerability criteria provide the bases for assessments.
- Baselines provide the opportunity to determine deviations.

Risk Assessments and Risk Models are an ongoing process.