MIRMAP – Modelling Instantaneous Risk for Major Accident Prevention

Stein Haugen
Department of Marine Technology
NTNU

- **Modelling Instantaneous Risk for Major Accident Prevention**
  - Finansiert av:
    - The Research Council of Norway
    - GASSCO
    - Statoil
  - Budget ca 10 mill kr
  - Research partners
    - NTNU
    - SAFETEC
    - Preventor
  - Xue Yang, Sizarta Sarshar
Objectives

As expressed in the project plan:

• “The objective of this project is to explore and define the concept of *instantaneous major hazard risk* and how this can be analysed in *living risk analysis*, as a basis for providing better decision support in an operational setting.”

• Focus on providing better decision support to operational planning and decision-making
  – Work-order preparation and planning, work permit preparation and planning
  – Not execution («sharp end»)
  – Major accidents, not occupational
Decisions

• Long-term decisions (strategic planning)
  – The plant lifetime should be extended for another ten years – do I have to upgrade my safety systems?
  – My maintenance costs are a heavy burden – can I reduce the cost and still maintain acceptable safety?
  – What explosion overpressure do I need to design for to achieve acceptable safety?

• Day-to-day planning of activities (operational planning)
  – Is it safe to perform all of these activities at the same time?
  – The most experienced operator on the shift is off sick – do I have to postpone some activities?
  – This is a complicated operation with potentially high risk, but it needs to be done – is it safe to do now?
Decisions

**Strategic decisions**
- Long planning horizon (years)
- Risk and benefits of decision alternatives are considered carefully
- Made by blunt-end decision-makers

**Operational decisions**
- Short planning horizon but long enough to carry out risk assessment
- Made by middle level decision makers (Operational managers)

**Instantaneous decisions**
- Spontaneous decisions to follow or violate procedure or decisions triggered by external deviations
- Made by personnel who monitor or control on-going operation

**Emergency decisions**
- Execution decision to avoid or adapt to hazardous situations
- Fundamentally impacted by experience and judgments
- Triggered by indicators out of comfortable zone
- Made by emergency response team
A problem with QRAs?

• QRAs and the methodology was originally developed to support strategic decisions
  – Largely successful in reaching this target

• Like all engineering models, QRAs are simplifications of the real world
  – Take into account (only) the factors that are important for the result
  – Explicitly model (only) factors that we can influence
  – Explicit: Layout and equipment
  – Implicit: Activities and organization

• What happens when we need to support other types of decisions, with other factors that can be influenced?
A long-term (strategic) decision: The weather is awful – maybe I should move?
A short-term (operational) decision: What should I do this weekend?
Decision basis

Climate statistics?

Or weather forecast?

Our hypothesis: «Risk climate» and «risk forecast» is not the same – and we need both for different decisions
Design vs Operation

• Design
  – Develop a solution that in the long term gives the lowest risk on average over the life-time of the system that we are designing
  – Can change technical solutions and average level of operations to achieve the goal

• Operation
  – Avoid accidents today
  – Technical systems are largely fixed, can more or less only change operational and organizational factors
Operational planning in oil & gas

• Key objectives with regard to safety:
  – Each activity must be performed safely
  – The total set of activities must be performed safely together

• Constraints:
  – Technical solutions that are present
  – Possible degradations in barriers – technical, operational and organizational
  – Availability of resources – people, equipment, time,…
  – External conditions

• Put simply the objective is:
  – “We want to get through (also) this day without anyone being killed or injured!”
Important aspects

• Focus modelling on aspects that change during operation
  – From system-based to activity-based modelling
  – Activities influencing barriers

• Averaging of risk over long time periods needs to be removed
  – Update parameters as often as necessary

• Provide support to the types of decisions taken during operations
  – Need to understand these decisions well
QRA vs Operational Risk Analysis

• QRA
  – Based primarily on modeling the technical systems, with activities reflected in a limited way
  – Calculates average long-term risk
  – Advantage: Quantitative, which gives a decision basis which is easier to use for ranking and decision about acceptable risk

• Operational Risk Analysis
  – Typical example is SJA
  – Activity-based analysis with technical systems and design as a «constraint» or context
  – Qualitative, not always good at focusing in major accidents
Types of risk analyses – oil&gas

Quantitative risk analysis (QRA)

Qualitative analysis mainly (FMECA, HAZOP etc)

Qualitative analysis mainly (Risk matrix, SJA)

Strategic analyses
"Climate statistics"

Qualitative design analyses

Operational analyses
"Weather forecast"

WEAK LINKS
What we have tried in MIRMAP

• Develop a method that can exploit the strengths of both QRA and operational risk analysis

• Some important elements of this:
  – Activity-based risk analysis taking into account the configuration and the condition of the technical systems
  – Quantitative, to enable ranking of activities
  – Using relevant models and information from QRA to the extent necessary and useful
Challenges

• To have a good understanding of risk
  – Short-term and long-term effects of decision alternatives
  – Individual activities
  – Totality of activities

• To incorporate the (many) constraints in the decision basis

⇒ To make consistent decisions
  – Safe…
  – …but not overly conservative
# Risk «types»

<table>
<thead>
<tr>
<th>Risk type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average risk</td>
<td>Risk for an industry, a nation or an even wider scope averaging over a large group of plants, activities, areas and personnel</td>
</tr>
<tr>
<td>Site-specific average risk</td>
<td>Risk for a specific plant, averaged over a year and taking into account specific characteristics of the particular plant</td>
</tr>
<tr>
<td>Activity risk</td>
<td>An expression of the effect that completing an activity will have on the risk level after the activity has been completed (risk after the activity)</td>
</tr>
<tr>
<td>Activity consequence risk</td>
<td>An expression of risk level associated with performing a specific activity (risk during the activity)</td>
</tr>
<tr>
<td>Period risk</td>
<td>An expression of risk for a plant or facility over a (normally short) period of time</td>
</tr>
<tr>
<td>Time-dependent action risk</td>
<td>An expression of short-term risk variation while performing one or several activities</td>
</tr>
</tbody>
</table>
Risk Classification

**Strategic decisions**
- Average risk
- Site-specific average risk

**Operational decisions**
- Activity risk
- Activity performance risk
- Activity consequence risk
- Period risk

**Instantaneous decisions**
- Time-dependent action risk

**Emergency decisions**
- Time-dependent action risk
Measuring risk

• The key is avoiding accidents – more focus on probability (or uncertainty) than risk
  – Statistically expected consequences are not relevant in the same way as in strategic decisions

• Relative risk
  – Ranking of activities, absolute values are not focused on
Lack of knowledge

• A key difference between strategic risk analysis and operational risk analysis is the use of probabilistic information vs facts (or at least with reduced uncertainty)
  – Strategic, long-term: Use average probability of failure of barriers, average number of operations, average number of people in area, etc
  – Operational: We can to a much larger degree know if barriers are working or not, what operations are taking place, who will be present, etc

• Uncertainty is expressed in terms of lack of knowledge
What we were aiming to do

![Graph showing daily changing risk level and average inherent risk level over 14 days.]

**Daily changing risk level**

**Average (inherent) risk level**

Day 1 Day 2 Day 3 Day 4 Day 5 Day 6 Day 7 Day 8 Day 9 Day 10 Day 11 Day 12 Day 13 Day 14
Operational planning

Main plan
Operations Plan
Work Order Plan
Work Permit Plan

1 to 6 years
3 months to 1 year
14 days to 3 months
24 hours
Activity-based approach

The lower-level of the risk model are activities

A1: Activities
Risk Increasing Activities (Hazards)
E.g. Hot Work, Work on HC systems

A2: Impairments/Deviations
Risk Increasing Conditions (Barriers)
E.g. Impairment of gas detection/fire detection, removal of PFP

To represent the complete risk picture we also include

B: Technical Degredation
Teknisk tilstand
E.g. Ageing, Fatigue

C: Design Deficiencies
Tekniske begrensninger
E.g. Firewater deficiency, Detector coverage limitations
Activities (A1) and barrier impairment (A2)

Prevent Release
- BF1
  - PSDVs
  - Leak (intervention)
  - Leak (isolation)
  - Leak (normal ops)
  - Leak (reinstatement)
  - PSVs
  - PSD Logic solver
  - PSD Transmitters

Limit Release Size
- BF2
  - Gas Detectors
  - Gas Detection logic solver
  - ESDVs
  - ESD Logic solver
  - BDVs
  - Flare
  - Depressurization Logic solver
  - Manual Call point
  - Control Logic
  - Manual Call point
  - ESD Pushbutton
  - Knockout Drum

Prevent Ignition
- BF3
  - Hot Work B
  - Ventilation
  - Activity generating sparks
  - Hot Work A
  - Ignition Source Isolation

Prevent Escalation
- BF4
  - Fire Wall/Door
  - Scaffolding
  - Open Drain
  - Blast wall
  - PFP
  - Auto Fire Detection Logic
  - Fire Detectors
  - Fire water
  - Auto release mechanisms
Analysis

A. Event trees
B. Fault trees
C. Influence diagrams
A. Event tree

<table>
<thead>
<tr>
<th>Event</th>
<th>Outcome</th>
<th>Outcome Prob.</th>
<th>Outcome Fatality Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prevent Leak</td>
<td>C0</td>
<td>9.9E-01</td>
<td>0</td>
</tr>
<tr>
<td>Detect Leak</td>
<td>C1</td>
<td>5E-03</td>
<td>0</td>
</tr>
<tr>
<td>Isolate</td>
<td>C2</td>
<td>3E-05</td>
<td>0.04</td>
</tr>
<tr>
<td>Depressurise</td>
<td>C3</td>
<td>4E-05</td>
<td>0.1</td>
</tr>
<tr>
<td>Prevent Ignition</td>
<td>C4</td>
<td>1E-03</td>
<td>0</td>
</tr>
<tr>
<td>Prevent Escalation</td>
<td>C5</td>
<td>0.6</td>
<td></td>
</tr>
<tr>
<td></td>
<td>C6</td>
<td>3E-05</td>
<td>0.8</td>
</tr>
<tr>
<td></td>
<td>C7</td>
<td>8E-04</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>C8</td>
<td>3E-06</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>C9</td>
<td>3E-05</td>
<td>1.2</td>
</tr>
<tr>
<td></td>
<td>C10</td>
<td>7E-06</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>C11</td>
<td>3E-08</td>
<td>1.4</td>
</tr>
<tr>
<td></td>
<td>C12</td>
<td>3E-07</td>
<td>1.6</td>
</tr>
</tbody>
</table>

PLL: 7E-05
B. Fault tree

- **Automatic detection fails**
  - Gas detection logic solver loop
    - A: (Gas Detection) logic solver impairment/deviation
      - 20
    - B: (Gas Detection) logic solver technical degradation
      - 94
  - Failure in gas detectors
    - A: (Gas detectors) impairment/deviation
      - 17
    - B: (Gas detectors) technical degradation
      - 16
    - C: (Gas detectors) coverage deficiency
      - 18
- **Manual gas detection fails**
  - MO (Manual gas detection) No operator in area
    - 19
  - Fail to send ESD signal through field pushbutton
    - A: (ESD PB) impairment/deviation
      - 84
    - B: (ESD PB) technical degradation
      - 85
Example – HC leakage

Release from manual intervention on HC systems

Or8
U(10h)=?
Uavg=?

Leak introduced during work on pressurized HC systems

Or9
U(10h)=?
Uavg=?

xA: Leak introduced during isolation
13

xA: Leak introduced during intervention
12

xA: Leak introduced during reinstatement
15

xA: Leak introduced during normal operation on HC systems
14
Evt14
U(10h)=?
Uavg=?
Example 1 – HC leak

Use input from QRA to quantify basic events

Adjust values based on state of influencing factors
Example 2 – Gas detection

Detection probability
(N impairments)

Sensitivities performed in QRA – effect of detectors not working

Used to assign probabilities
Running the model through the four stages of the planning cycle
Purpose: To illustrate how risk develops over time as a result of changes in activities
Probability of Major Accident

- Blue: Baseline
- Red: A
- Green: B
- Purple: C
- Cyan: D
Main reasons for changes in risk

- **Updated knowledge** about the work
  E.g. Surface treatment
- **New** activities
- **Delayed** activities (removed from the plan)
- **Changes** in execution date
Barrier status information

Without barrier status

Baseline risk changes

Change in shape of risk curves

Important to consider barrier status when planning work
Feedback – plus and minus

- Offshore expect risk to be «removed» when they receive the plan
- Can be used in the whole planning cycle (3 months) and in different decision contexts
  - Early risk evaluation of preventive maintenance work
  - Avoid risk peaks when execution date of work changes
  - Quickly see the effect of high priority jobs (that «bypass» the planning cycle)
- Support to reduce uncertainty
  - Information in Work Permits can be made available much earlier
- Needs to be automated
  - Manual feed to the model is too time-consuming
  - Requires plant specific knowledge
Future work

• Have been trying to get a more comprehensive case study from Statoil – so far no success

• What is acceptable risk in the short term?
  – How high «peaks» can be accepted?
  – Does it make sense to accumulate risk?

• More work on the fundamentals
  – Getting a better grip on uncertainty to improve risk management
Potential use

• When preparing Work Orders
  – How much will «my» WO contribute to risk, based on the plant status as it is today?
  – Identify limitations to be taken into account in planning
• When preparing plans up to 3 months ahead and to Work Order Plan
  – Earlier identification of all WOs with high risk
  – More consistent comparison and evaluation
• During preparation of Work Permits
  – Which WPs represent a high risk? Prioritize
• Work Permit Meeting (approval)
  – Better and more consistent basis for comparing, approving and modifying activities
Work required

• Developing a MIRMAP risk analysis will require significant effort
  – Similar order as QRAs that are performed today
  – Replacing existing QRAs will imply similar effort
  – Model can be run on a daily basis with very limited effort

• Risk model “templates” for activities?
  – Many similarities between plants
  – A library of models will save time and effort
Availability of data

• Input from the QRA will be applied
  – Technical systems, consequences – relatively static information, long intervals for update (years?)

• Daily updates
  – Types of activities, number of activities, where they are taking place, how many people are involved, systems/-components that have failed, maintenance status, etc.
  – Data collection must be automatic to make this feasible and cost-effective in practice.

• Information is typically available in the maintenance management/planning system and the work permit system.
Conclusion

• The main «finding» from MIRMAP is that we need to remind ourselves why we do risk analysis!
• After we understood this, we could use standard risk analysis methods to develop suitable input to decisions

• Testing has indicated:
  – Can identify high risk contributors among activities
  – Sensitive to differences
  – Can support understanding of why risk is high
  – Can improve planning