Erfaringer fra kjernekraft

ESRA Seminar
April 10, 2013

Salvatore Massaiu
Industrial Psychology Department
Institute for Energy Technology
Outlook

• Different barrier concepts
  • Defense in Depth and barriers
  • Technical and organizational barriers
  • Safety management and risk analysis

• Main technical point: Integrating human and organizational factors in risk analysis
Defence in Depth

• The idea of multiple levels of protection is the central feature

• Includes the means to provide the barriers themselves with successive layers of protection
Defence in depth

A hierarchical deployment of different levels of equipment and procedures in order to maintain the effectiveness of physical barriers placed between radioactive materials and workers, the public or the environment.
Preventing release of radioactive material
Organizational barriers

Equipment and procedures maintain the effectiveness of physical barriers
Reason’s Anatomy of an Organizational Accident
HSE’s safety indicators

The **indicators** monitor that systems and procedures continue operating as intended.

**Process safety management system:** the parts of an organisation’s management system intended to prevent major incidents.

**Risk control systems (RCS):** the constituent part of a process **safety management** system that focuses on a specific risk or activity.
<table>
<thead>
<tr>
<th>Inspection and maintenance of:</th>
<th>Wear</th>
<th>Corrosion</th>
<th>Damage</th>
<th>Over/under pressurisation</th>
<th>Fire and explosion</th>
<th>Overfilling</th>
<th>Other accidental release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flexi hoses, couplings, pumps, valves, flanges, fixed pipes, bulk tanks</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Instrumentation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Earth bonding</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tank vents</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fire detection and fighting equipment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Staff competence, covering:</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Selection of compatible tank</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Selection of route and tank with adequate capacity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Driver error</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Correct coupling, opening/closing valves, starting pumps etc</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Suitable skills and experience to undertake inspection and maintenance tasks</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Emergency arrangements</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Probabilistic risk analysis

- Incidents and accidents postulated as initiating events
  - selected according to their frequency, estimated from general industrial experience
- Considers equipment failures and human errors
- Well defined risk models
  - How the initiating events can lead to uncontrolled release of radioactive materials outside the plant
Event trees

- Events: safety features and protection systems
- Activated by the operators or by automation
Event trees

Events = Barriers
Risk Assessment vs. Indicators process

1. What can go wrong?
   Initiating events (e.g. small-break loss of coolant)
   Event sequence logic

2. How frequently does it happen?
   Quantification

3. What are the consequences?
   Consequence modeling

1. What can go wrong?
   Hazard scenarios (e.g. leakage) and their causes (e.g. valve wear)
   List of generic causes (wear, corrosion)

2. What control systems control these risks
   (risks = generic causes)

3. What are the outcomes of and critical parts of these systems?
   Identify leading and lagging indicators
Human Reliability Analysis (HRA)

- Probability Risk Analysis estimates the reliability of the barrier functions (engineered safety features)
- Some of these functions are executed by operators
- HRA assess the reliability of the operators
  - Takes into account the task difficulty
  - And the context of performance
- Organizational influences are not accounted for explicitly
  - E.g. Procedures are correct
First Generation: operators as components

- Operator = machine
  - Follows procedures
  - Has known limitations
  - Is unreliable

- Human failures:
  - Individual errors
  - Operator directed by interface and procedures
  - If response is not as expected → Error
Humans role in safety: two views

Human can’t be perfect and can err

Automatize or help operator

Improve interface, procedures, training

Require procedures strict application

Engineering can’t be perfect nor predict everything

Manage safety by

Improve safety culture, skills, experience

Require situation awareness & initiatives

Anticipation

Adaptation
Second generation: The Emergency Operating System

- Emergency operation results from the interaction between operators, procedures and interfaces
- The EOS is a cognitive and distributed system
  - It uses prior knowledge and produces new knowledge in real time
  - Knowledge is deposited in and elaborated by different system components
- Technology and organization are joined
Model of Resilience in Situation

**RESILIENCE**

- **ROBUSTNESS**
  - EXECUTION CONTROL
- **EOS**
- **ADAPTATION**
  - INFORMATION SELECTION AND SHARING
  - VERIFICATION RECONFIGURATION

**ANTICIPATION**
- ROLES ALLOCATION
- DELEGATION
- PROCEDURES
- INTERFACE
- TRAINING
- SAFETY CULTURE

**MANAGEMENT**

**AUTONOMY DEVELOPMENT**
- ORGANIZATIONAL LEARNING
- STORYTELLING
- PEERING
- SIMULATION
The MRS includes organizational and the team influences in risk analysis

• Today:
  • Performance Shaping Factors, e.g., team dynamics
  • Analysts’ knowledge of the plant/organization

• The EOS approach:
  • Produces a model of Organizational and teamwork influences on control room operators capabilities
The dynamics of emergency operation

Central concepts: Rules and In-situation Regulation
MRS model: combines the two views

Human can’t be perfect and can err

Automatize or help operator

Manage safety

Human can’t or predict everything

Engineering can’t be perfect

Improve culture, skills, experience

Anticipation

Improve safety culture, skills, experience

Adaptation

Require procedures strict application

Require situation awareness & initiatives

Rule

Example:

Follow strictly the procedure. No deviations, no violations. AND

Be able to operate without or against the procedure

Two opposite rationalities
The functions of an EOS

1. Effective rules
2. Surveillance rules
3. Realization rules
4. Verification
5. Control
6. Info. selection
7. Process/environment
8. Reconfiguration
Five EOS functions

- Execution (of rules)
- Reconfiguration (if rule not adequate)
- Verification (of rule adequacy)
- Information selection and exchange
- Control (of rules)
The EOS characteristics

- Team
- Formal communications
- Training
- Procedures
- HMI
- Prescriptions
Example
# Team Influences on Verification

<table>
<thead>
<tr>
<th>Openness/Democracy</th>
<th>Supervisory role</th>
<th>Team size</th>
</tr>
</thead>
</table>
| Redundant checks   |                  | To look for extra information  
To assess reliability of cues |
| New info and anomalies | To keep track of reminders | |
| Global overview    | To question current mission  
To evaluate procedure is appropriate  
To reconsider priorities | To keep global overview  
To evaluate procedure is appropriate  
To look ahead in procedure |
Applications: Comparing EOSs

- Evaluate the effects of EOS differences on resilience and failure probabilities
- Relate data collected in one organization/reactor to a different one
- Integrated system validation: Same EOS before/after modification
Status

• The EOS approach has been developed by EDF, with support from PSI and IFE
• Closely related to EDF’s HRA method MERMOS
• EDF is using the Delta-approach in the design and evaluation of a new reactor (EPR)
• Still under development
Conclusion

• It is possible to account for the effect of organizational barriers on safety, provided that

• It is about ultra-safe system:
  • Individual errors are recovered, failure is collective
  • Failures are wrong diagnoses or strategies in unusual situations, not slips and lapses
  • Extensive preparedness (e.g. procedures, training)

• There is substantial time from the initiating event up to the point at which harm occurs

• There exist a risk model (e.g. the PRA)
Thanks for your attention
2nd generation HRA: MERMOS

- Joint-system perspective
- Failure is mismatch not information overload
- Focus on team not individual and attention/memory errors
- Close integration with HF
- Rich inputs for error identification and reduction
- Qualitative insights conveyed in the application
- More than numbers in PRA

ITEM 1) HEP of HFE1A1

<table>
<thead>
<tr>
<th>Probability of mission failure (HEP)</th>
<th>Uncertainty:</th>
</tr>
</thead>
<tbody>
<tr>
<td>4,6 E-2</td>
<td></td>
</tr>
</tbody>
</table>

The probability of the mission is the sum of the probabilities of all the “MERMOS scenarios of failure” (including residual probability) : see Item 2

ITEM 2) SUMMARY OF MOST INFLUENCING FACTORS

List of the MERMOS scenarios leading to the failure of the HF mission (the scenarios found by the analysts are detailed in item 3)

<table>
<thead>
<tr>
<th>Function</th>
<th>Prob.</th>
<th>N*</th>
<th>Scenario</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategy</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>1</td>
<td>Not relevant for Hammlab</td>
</tr>
<tr>
<td>Total: 99,5 %</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2,4 E-2</td>
<td>2</td>
<td>No strategy - The system scrupulously follows the EOPs spending time on points irrelevant to the situation and doesn't complete feed and bleed on time</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>3</td>
<td>Not relevant for Hammlab</td>
</tr>
<tr>
<td></td>
<td>8,1 E-5</td>
<td>4</td>
<td>Erroneous strategy - The system spends time in its attempt to recover the condensate pumps system and puts off too long completion of feed and bleed</td>
</tr>
<tr>
<td></td>
<td>2,2 E-2</td>
<td>5</td>
<td>Erroneous strategy - In its hope to recover the AFS the system delays too long the completion of feed and bleed</td>
</tr>
<tr>
<td>Action</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>6</td>
<td>Not relevant for Hammlab</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>7</td>
<td>Not relevant for Hammlab</td>
</tr>
<tr>
<td>Diagnosis</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>0</td>
<td>8</td>
<td>Not relevant for Hammlab</td>
</tr>
<tr>
<td>Total: 0,5 %</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2,4 E-4</td>
<td>9</td>
<td>Erroneous state diagnosis - The system doesn't perform the state diagnosis on time</td>
</tr>
<tr>
<td>Residual probability</td>
<td>1,0 E-4</td>
<td></td>
<td>(this probability represents all the scenarios that we are not able to imagine: we assign the upper value given the lack of data)</td>
</tr>
</tbody>
</table>
## Levels of protection

<table>
<thead>
<tr>
<th>Levels</th>
<th>Objective</th>
<th>Essential Means</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Level 1</strong></td>
<td>Prevention of abnormal operation and failures</td>
<td>Conservative design and high quality in construction and operation</td>
</tr>
<tr>
<td><strong>Level 2</strong></td>
<td>Control of abnormal operation and detection of failures</td>
<td>Control, testing, limiting &amp; protection systems and other surveillance features</td>
</tr>
<tr>
<td><strong>Level 3</strong></td>
<td>Control of accidents within the design basis</td>
<td>Engineered safety features and accident procedures</td>
</tr>
<tr>
<td><strong>Level 4</strong></td>
<td>Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents</td>
<td>Complementary measures and accident management</td>
</tr>
<tr>
<td><strong>Level 5</strong></td>
<td>Mitigation of radiological consequences of significant release of radioactive materials</td>
<td>Off-site emergency response</td>
</tr>
</tbody>
</table>