PSA Applications and Risk Monitors

Paul Boneham
Summary of PSA Applications
## Typical/Popular PSA Applications

<table>
<thead>
<tr>
<th>Application</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintenance</td>
<td>USNRC regulation established requirement in 2000 to assess and manage configuration risk. Scope of SSCs may be limited based on risk-informed evaluation process.</td>
<td>US NRC regulation a strong driver for US NPPs to control risk impact of maintenance. Risk Monitor is the tool of choice for compliance.</td>
</tr>
<tr>
<td>Regulatory Inspections</td>
<td>Use of PSA and risk Insights to improve the focus and effectiveness of inspections.</td>
<td>Risk ranking of components, structures, systems. Response of regulator to findings – importance?</td>
</tr>
<tr>
<td>Regulatory Reporting Requirements</td>
<td>NRC revised requirements for licensee reporting of events and conditions with several objectives, including elimination of reports of no risk significance.</td>
<td>PSA based event analysis – NPPs incentivised to analyse events and reduce reporting where risk significance shown to be low.</td>
</tr>
<tr>
<td>Plant Vulnerabilities</td>
<td>Use of PSA to reduce risk by implementing design, operational, and maintenance changes.</td>
<td>The first application of PSA!</td>
</tr>
<tr>
<td>Fire Protection</td>
<td>Use PSA to support improvements in fire protection and cost-effective resolution of fire protection issues.</td>
<td>Some problems with uncertainties in models and plant equipment capability. Currently strong uptake in US due to regulation</td>
</tr>
<tr>
<td>NRC Accident Sequence Precursor Program</td>
<td>This ongoing program to assess the significance of events will continue.</td>
<td>PSA based event analysis by regulator</td>
</tr>
<tr>
<td>Risk Monitors</td>
<td>Real time risk tracking. Real time risk impact of maintenance. Outage planning/maintenance scheduling.</td>
<td>Risk monitors often used to support other applications</td>
</tr>
</tbody>
</table>
Some more PSA Applications

<table>
<thead>
<tr>
<th>Application</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Control Room Habitability</strong></td>
<td>Apply PSA and Risk-informed approaches to support resolution of radiological and toxic gas issues related to control room monitoring and in-leakage.</td>
<td>Assessments aim to establish the frequency of loss of control room habitability to be below 1E-6 per year. Some plants have also included an assessment of the conditional probability of core damage to demonstrate an acceptably low frequency.</td>
</tr>
<tr>
<td><strong>Emergency Planning</strong></td>
<td>Using alternate source term and PSA to improve efficiency and cost, including development of emergency plan exercises and changes to emergency plan requirements.</td>
<td>Use to reduce emergency planning zones and requirements was not successful. Evolving area for use in establishing Emergency Action (Response) Levels.</td>
</tr>
<tr>
<td><strong>In-Service Inspection</strong></td>
<td>NRC has approved two methods (WOG and EPRI) for weld exams. Both methods provide significant reduction in scope of RCS ISI.</td>
<td></td>
</tr>
<tr>
<td><strong>Risk Significance of Systems, Structures and Components for testing, corrective actions</strong></td>
<td>Use of PSA to rank SSCs for application in programs such as IST, MOV Testing, Corrective Actions.</td>
<td>Routine in the US and remains key element of both Industry’s and NRC ranking of Safety Issues</td>
</tr>
<tr>
<td><strong>Technical Specifications</strong></td>
<td>PSA application to support allowed outage time (AOT) extensions.</td>
<td>This type of application becoming more frequent - Risk Monitors</td>
</tr>
</tbody>
</table>
# Less common PSA Applications

<table>
<thead>
<tr>
<th>Application</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alternate Source Term</td>
<td>Replace design basis choice of source term with risk-informed choice</td>
<td>Link to emergency planning / emergency planning zones</td>
</tr>
<tr>
<td>Corrective Action Program</td>
<td>Use of PSA to support significance assessment and disposition of events.</td>
<td>Link to PSA based event analysis</td>
</tr>
<tr>
<td>Graded QA</td>
<td>Graded Quality Assurance Program implementation on the basis of risk significance.</td>
<td>Possibly not as beneficial as expected.</td>
</tr>
<tr>
<td>In-Service Testing</td>
<td>NRC has approved risk-informed IST approach for pump and valve test interval optimization.</td>
<td>Benefit versus cost can vary.</td>
</tr>
<tr>
<td>Insurance</td>
<td>Use of PSA to reduce Insurance costs</td>
<td>Conservative Risk Modelling. Applications have been more for decommissioning/dismantling plants.</td>
</tr>
</tbody>
</table>
PSA Quality for Applications

- Proliferation of PSA applications has been accompanied by quality standards
- ASME Standards for Level 1 PSA and LERF
- ANS Level 2 Standard
- USNRC expects compliance with Reg Guide 1.200 (mostly ASME with some comments/clarifications)
- IAEA has published TECDOC on PSA Quality
PSA based event analysis (1)

• PSA based event analysis is the application of PSA to rank events by risk significance

• Risk significance measured by
  – CCDP: conditional core damage probability or
  – CLRP: conditional large release probability

• Sometimes called precursor analysis

• Regulatory and NPP use
  – Reporting
  – Significance determination of inspection findings
PSA based event analysis (2)

• Applicability:
  
  – Any event that can be mapped to PSA model
    • Depends on scope of PSA (e.g. shutdown events)
  
  – Usual to distinguish between condition events and precursor to initiating events
    • Condition: a degradation or unavailability persists for a time
    • Precursor: an event occurs which may lead to IE in PSA or maps directly to IE in PSA
PSA based event analysis (3)

• Key Points of Methodology
  – Quantification of appropriate parts of PSA with appropriate assumptions
  – Failure memory (usually the original event didn’t lead to CD!)

• PSA status / quality
  – Simplifications in PSA – fit for this purpose? (event analysis)
  – Representative / up-to-date PSA
  – General quality, completeness of PSA
    • Affects results!
PSA based event analysis (4)

- **Insights**
  - Quantitative – CCPD, CLRP
  - Quantitative: likely paths to core damage / release, importances
  - Qualitative: study alternate similar scenarios, possible evolutions of event
Introduction to Risk Monitors – some history
THE ORIGINAL RISK MONITOR INTERFACE
1988 - ESSM

- Installed at Heysham 2 Power Station to assist the operator in managing outages of safety related plant.
- Addresses compliance with the station’s operating rules; carry out an ‘on-line’ risk assessment to demonstrate that the risk is acceptable.
- Available to operator and maintenance staff
- has the level 1 reactor PSA programmed within it in the form a single large logic tree.
1994 - Safety Monitor

- Installed at many plants in four countries after first installation at San Onofre.
- Core is PSA model (Level 1 and 2) for all plant operating modes and dual units.
- Carry out ‘on-line’ and off line risk assessment for current and future configurations.
- Available to all plant staff
- User group and continuous upgrading to meet user requirements
- has rule tracking for safety functions, tech spec, etc.
- Fast solution engine for each configuration
1998 - NRC Initiatives

➢ USNRC purchases Risk Monitor for use in training site inspectors and other staff. Develops models for each of the reactor types in US
➢ Maintenance Rule implementation and expansion
  – Assess & manage the risk increase - Full Power and Shutdown
  – Scope of structure, systems, and components (SSCs) may be limited
    • Risk-informed evaluation process
    • Significant to public health & safety
Key features (1)

• Usable by NPP staff such as control room staff, maintenance staff
  – Day to day use
  – Planning and evaluation of hypothetical situations

• Generate reports for plant management

• No detailed PSA knowledge should be required
Key features (2)

• NPP staff should be able to work with NPP terminology
  – Component names
  – Maintenance tags
  – Operational modes
  – RM hides details of PSA model

• Rapid feedback: model quantification typically < 1 minute

• Promotes understanding of risk leads to a reduction in risk of plant operation. Key example: refuelling outages of light water reactors.
RISK MONITOR MODES

- Schedule mode for planning risk management throughout an outage (longer term future timeframe)

- Real mode for assessing real time plant risk and recording past configurations and risk

- Hypothetical mode for looking at long and short term future timeframes, i.e., what-if maintenance scenarios and assessment of alternatives

- Different users may have access to different modes
DUAL UNITS

• A number of RMs are used at dual unit plants

• Risk tracked on both units

• Software should ensure consistency for availability of shared equipment
  – Shared items set as on maintenance by operator using Unit 1 Risk Monitor model
  – Consistency best achieved if software ensures that this equipment is marked as on maintenance in unit 2 model also
ENVIRONMENTAL AND TESTING FACTORS

• Modified IE frequencies when tests are in progress or under particular external environmental conditions
  – Maintenance induced initiating events more likely in certain shutdown states (e.g., loss of supports due to maintenance error, draindown or overdraining for a PWR, etc)
  – Bad weather increasing loss of offsite power frequency
  – etc

• These effects are typically smoothed out into averages in the Living PSA
  – Particularly full-power portion of LPSA

• Risk Monitor represents point-in-time situation by allowing application of environmental/testing factors
Risk Monitors Now: EXAMPLE SCREENSHOT - Risk Profile
Defense in depth

- Status views in RMs extended to deterministic system status
  - Colour coding of status – trains available, partial degradation of supports
  - Implemented by flexible safety function status trees
    - User defined
Risk Monitors Now:
EXAMPLE SCREENSHOT - Safety Functions

<table>
<thead>
<tr>
<th>Overall Status</th>
<th>August</th>
</tr>
</thead>
<tbody>
<tr>
<td>15</td>
<td></td>
</tr>
<tr>
<td>16</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td></td>
</tr>
<tr>
<td>18</td>
<td></td>
</tr>
<tr>
<td>19</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td></td>
</tr>
<tr>
<td>21</td>
<td></td>
</tr>
<tr>
<td>22</td>
<td></td>
</tr>
<tr>
<td>23</td>
<td></td>
</tr>
<tr>
<td>24</td>
<td></td>
</tr>
<tr>
<td>25</td>
<td></td>
</tr>
<tr>
<td>26</td>
<td></td>
</tr>
<tr>
<td>27</td>
<td></td>
</tr>
<tr>
<td>28</td>
<td></td>
</tr>
</tbody>
</table>

- PSA Results: On-Line
- Containment Pressure: On-Line
- Containment Isolation: On-Line
- Cooling Water: On-Line
- Emergency Core Cooling: Online
- Power Availability AC: Online
- Power Availability DC: Online
- Boration/RX Control: Online
- RX Coolant Pump Seals: Online
- RCS Integrity: On-Line
- Sec Side Heat Removal: Online

Legend:
- Green
- Yellow
- Orange
- Red
- (Alternate Mode)
Example risk profile report for management

Heat Exchanger Out Of Service

- ORAN: [1.0E-03]
- RED: [2.5E-04]
- YELLO: [7.1E-05]
Trends: Model Solution

• Processors getting faster & engines improving
  – Solution times reduced

• Multi-core PCs:
  – Standard solution engines use one core at a time
    • No speed up on multi-core
  – Solution: multi-threaded engine
    • Multi-threaded psimex in Safety Monitor
    • 2 cores – twice as fast
    • 4 cores – four times as fast
    • Etc

• Benefits of all this:
  – Little need for model optimisation/simplification
  – Huge benefit for schedule optimisation (volume of runs to analyse schedule)
Trends: Switch to Risk Informed Completion Times

- RMs traditionally generated an Allowed Configuration Time using a simple “allowed delta risk” / risk level calc

- Problems seen with clock resetting; clock started again if configuration changed
- Regulatory impression that use was not formalised

- In practice seen that many NPPs didn’t use ACTs

- Safety Monitor moving to Risk informed completion time – avoids clock resetting. Cumulative configuration risk will be used to generate limits – precise methodology likely to take account of NRC view

- In US this is driven by USNRC. NRC wants reporting of time in riskier configurations and targets applied and compliance with targets. (Initiative 4b)
SUMMARY OF KEY POINTS

• PSA Applications:
  – Variety of applications
  – PSA quality

• Risk monitors
  – access to risk calculations through an interface for non-specialist use
  – Risk profile taking account of equipment unavailabilities and environmental/testing/activity influences
  – Deterministic status (safety functions) also monitored
  – Can support applications, especially most “popular”
  – Many detailed features:
    • Scheduling
    • Hypothetical (what if) mode
    • Consistent treatment of dual units
    • Fast solution