Use of the Bowtie Methodology in the Generic Pre-Construction Safety Report (GDA PCSR) for Advanced Water Cooled NPPs

Fidel Ilizástigui Pérez
National Nuclear Safety Centre
Cuba
UK ONR: ‘Licensable’ organization

- Reactor design ‘Safety Case’
- Site suitability
- Organisational capability (to be in control of safety at point of licensing)
Licensee’s organizational capability

- The Safety Report is one of the important ways to demonstrate that safety is being properly managed.

- Licensees are responsible for the Safety Report and its adequacy.
  - Must develop GDA PCSR into a robust site specific version.
  - Must be able to fulfil ONR’s expectations regarding good quality Safety Reports.
UK ONR: Good quality Safety Reports

- ONR’s expectations on overall SC qualities:
  - Developed with licensee’s legal duties in mind.
  - Usable and accessible (to the ‘final users’).
  - Fit-for-purpose (demonstration).
  - An effective risk management tool.
  - A ‘living’ document
GDA Process, PCSR & Bowtie

- Early Licensee’s involvement in the GDA process is key with regard to the production of good quality PCSR:
  - BT methodology can be incorporated as part of the Safety Case production strategy
  - BT methodology will allow Licensee to apply an opposite mindset to that of the designer.
  - BT is a perfect tool to complement the Claims-Argument-Evidence (CAE) approach.
How Bowtie methodology can help?

- Avoiding known ‘shortcomings’ of the ‘Safety Case production’ industry:
  - Improved understanding, visibility and accessibility of Nuclear Safety Reports.
  - Improved workforce involvement and participation.
  - Promotes ‘active’ thinking on hazards and controls and a questioning and learning attitude.
How Bowtie methodology can help? - Con’t

- Links safety assessment with safety management.
- Allows a better consideration of human factors in nuclear reactor safety.
- Ensures implementation of modern barrier management.
Why is it called Bowtie?

- Oil & Gas
- Chemical
- Mining
- Aviation
- Medical
- Financial
- Government
- IT
Sample Bowtie diagram
Generic ABWR (I) – HPCF Line Break

Nuclear fuel contained within the fuel cladding (and cooled) during Reactor Power Operation

Hazard
(Potential to cause harm)

Top Event
(e.g. Bounding Fault)

HPCF system pipe breaks
Sample Bowtie Generic ABWR (II)

**Hazards**

- Material degradation (i.e. corrosion, crack growth, stress)
- Overpressure
- External Loads causing Reactor Building Vibration (i.e. Earthquake)

**Consequences**

- Nuclear fuel contained within the fuel cladding (and cooled) during Reactor Power Operation
- Power is not reduced to the decay heat level which leads to fuel cladding temperature exceeding design margins - Core damage potential
- Core becomes uncovered which leads to fuel cladding temperature exceeding design margins - Core damage potential
- Containment overpressure failure - Core damage potential

(Not all inclusive!)
Sample Bowtie diagram
Generic ABWR (III)

Prevention Controls
(Safety Measures)

Material degradation
(i.e. corrosion, crack growth, stress)

HPCF pipe is designed based on materials with low susceptibility to corrosion mechanisms and manufactured and assembled to reduce stress and crack initiation

CUW Reactor Water Cleanup System reduces impurities contained in the reactor water and maintains its quality

Reactor Water Chemistry regime is controlled by Operator as per Reactor Chemistry Manual/Technical Specifications

SAM alarms according to Reactor Chemistry Limits and Conditions and corrective actions carried out by the Operator

Results of the In-service Inspections (ISI) and corrective actions

Nuclear fuel contained within the fuel cladding during Reactor Power Operation

HPCF system pipe breaks leading to...
Sample Bowtie diagram
Generic ABWR (IV)

Recovery Controls (Safety Measures)

HPCF system pipe breaks leading to...

Safety System Logic and Control activates RCIC, ADS and RHR-LPFL on low reactor water level and high drywell pressure

RCIC Reactor Core Isolation Cooling System starts coolant injection on low reactor water level signal

ADS Automatic Depressurization System is activated on low reactor water level signal and high drywell pressure with 30 sec delay

RHR - LPCF (LPCI) Low Pressure Core Flooder Mode starts coolant injection to RPV on low reactor water level signal and high drywell pressure and provides long term heat removal via HEx

Core becomes uncovered which leads to fuel cladding temperature exceeding design margins - Core damage potential
Understandable, accessible and easy to use Safety Report

Understanding the whole scenario
HPCF Line Break (Medium) LOCA Accident Scenario
GDA Process and beyond: Linking to the Management System (Examination, Inspection, Maintenance, Testing)
GDA Process and beyond: Design information

Color legend of Effectivenesses
- <NULL> <No Value Assigned>
- Poor - Submissions are not addressing RO/RI
- Medium - Submissions are not fully addressing an RO/RI
- Good - The RO/RI is likely to be closed
- Very Good - No RO/RI issued

Safety Class, Category, Standards

Interaction with other Systems

Core becomes uncovered which leads to fuel cladding temperature exceeding design margins - Core damage potential

Nuclear fuel contained within the fuel cladding during Reactor Power Operation

HPCF system pipe breaks

Safety System Logic and Control activates RCIC, ADS and RHR-LPFL on low reactor water level and high drywell pressure

Category A, Class 1, IEC Nuclear Power Plant
- Safety Class 1 AC UPSs
- Safety Class 1 DC PSS
- HMI for SSLC
- Remote Shutdown Panel

RCIC Reactor Core Isolation Cooling System starts coolant injection on low reactor water level signal

Category A, Class 1, BS & ISO Standards
- Safety Class 1 DC PSS
- CST
- Suppression Pool

ADS Automatic Depressurization System is activated on low reactor water level signal and high drywell pressure with 30 sec delay

Category A, Class 1, BS & ISO Standards
- SRV Accumulator s for the ADS function

RHR - LPCF (LPCI) Low Pressure Core Flooder Mode starts coolant injection to RPV on low reactor water level signal and high drywell pressure and provides long term heat removal via HEx

Category A, Class 1, BS & ISO Standards
- Safety Class 1 Emergency Diesel Generator
- RBCW System
- RBEEEZ HVAC
GDA Process and beyond

H & O Factors

Nuclear fuel contained within the fuel cladding (and cooled) during Reactor Power Operation

RHR - LPCF (LPCI)
Low Pressure Core Flood Mode starts coolant injection to RPV on low reactor water level signal and high drywell pressure and provides long term heat removal via HEEx

Core becomes uncovered which leads to fuel cladding temperature exceeding design margins - Core damage potential

HPCF system pipe breaks

Degradation Factors Controls

Competence and Training for Emergencies
Advanced HMI design for CRT screens
No Operator's manual actions needed during the first 30 mins.

Degradation Factors

Human error during RHR long-term operation
A ‘living’ document & Line of sight

Back-fitting Bowties with: Incidents, Audits and OPEx

How controls are actually performing?
Bowtie Workshops

- The Bowtie diagram can be built by Responsible Party’s safety/engineering people and reviewed during a workshop session with Prospective Licensee’s people.

<table>
<thead>
<tr>
<th>Responsible Party</th>
<th>Prospective Licensee</th>
</tr>
</thead>
<tbody>
<tr>
<td>Responsible Engineers</td>
<td>Technical Topic Leads</td>
</tr>
<tr>
<td>Safety Case leads</td>
<td>PCSR chapter leads</td>
</tr>
<tr>
<td>SMEs</td>
<td>Operators</td>
</tr>
</tbody>
</table>
For Design Basis Faults – Bounding Faults
For Beyond Design Basis Faults
As part of the Design Authority Building Capability!
Conclusions

- ONR assesses whether the licence holder has demonstrated via the Safety Report that it understands the hazards associated with its activities and how to control them.

- BT methodology may help licensee to fulfil ONR’s expectations regarding good quality and fit-for-purpose Safety Reports.

- BT allows using the site-specific Safety Report as an effective risk management tool.
Thank you very much for your attention!

Fidel Ilizástigui Pérez
filizastigui@gmail.com
National Nuclear Safety Centre
Cuba