The Evolution of System Safety in the Canadian Nuclear Industry

System Safety Society, Eastern Canada Chapter, June 18, 2009
Philip Webster; Director, Darlington Regulatory Program
Canadian Nuclear Safety Commission (CNSC)

- Canada’s nuclear watchdog
- Quasi-judicial body
- Independent of, but not isolated from, government

Regulates the use of nuclear energy and materials to protect the health, safety and security of persons and the environment; and to respect Canada’s international commitments on the peaceful use of nuclear energy
CNSC regulates all nuclear facilities and activities in Canada, including:

- Nuclear power plants
- Uranium mines & mills
- Uranium fuel fabrication and processing
- Nuclear substance processing
- Industrial and medical applications of nuclear substances, such as nuclear medicine and cancer treatment centers
- Research and educational facilities
- Import/export of nuclear and dual-use substances, equipment and technology
- Waste management facilities

...is a federal responsibility
Summary

• Initially little recognition of need for safety systems
• Need for safety systems to be independent
• Increasing complexity of safety systems
  – Multiplicity, availability, testability
• Contribution of support systems to safety
• Increasing analysis
• Probabilistic risk assessments
• Management systems approach
• Modern standards for design, analysis
• Licensees vs. Regulator
• Reactor started operation at CRNL in 1947
• Produced Pu, other isotopes, fuel testing, research
• Maintaining operation was important
• Combined control/shutdown rods
  – Manual procedures to withdraw them
  – Errors made during startup
  – Major power excursion, fuel melting
• Lessons learned:
  – Indicated need for fast shutdown capacity
  – Independent of any control system
Reactor Safety Criteria - 1964

- Process equipment
  - Equipment and systems for normal operation
- Protective devices
  - Prevent fuel damage from failure in process equipment
- Containment provisions
  - Limit or restrict release of radioactivity
- Structurally and operationally independent
  - Rate of cross-linked faults less than rate of coincident independent faults
Application of Reactor Safety Criteria

- Frequency of process failures < 1 in 3 years
- Unreliability of protective devices < 0.003
- Unreliability of containment < 0.003
- Safety systems to be physically and functionally independent from process systems and each other
- Safety systems must be testable to verify
- Exclusion zone
Two shutdown systems - 1977

- Regulatory Document R-10
- New reactors to have two shutdown systems
  - Independent, diverse
  - Physically and functionally separate
- All serious process failures can be handled by either one
  - Failure to shutdown is beyond design basis
- Unavailability of each < 1E-3 per year
- Testable, fail-safe
- Two diverse trip parameters for each SPF
• Dose limits: normal operation & accidents
• Five dose classes defined
  – Individual dose/Sum of probabilities
• Safety requirements for siting, design, safety analysis, construction, commissioning, operation, effluent and waste management, decommissioning.
• ALARA
Grouping and Separation

- **Group I**
  - SDS 1
  - ECCS
- **Group II**
  - SDS 2
  - Containment
- **Important process and SSS are triplicated**
  - Permits testing without making unavailable, or inadvertently triggering
  - 2oo3 logic
- **Two control rooms**
Probabilistic Safety Assessments

• Validate for completeness the list of design basis accidents
  – i.e. those identified for analysis
• Assist confirmation of accident sequence classification
• Identify dominant failure sequences
• Demonstrate cumulative frequencies of accidents are less than targets
<table>
<thead>
<tr>
<th>Multiple Tube Rupture in Any RCW-HX</th>
<th>Reactor Shutdown by RRS SDS1/SDS2</th>
<th>Pressure and Inventory Control System Available</th>
<th>Trip of PHT Pumps on Low PHT Pressure</th>
<th>PHT Loops Isolate at 5.32 MPa(g)</th>
<th>PHT Crash Cool Down Manually Operated</th>
<th>ECC Initiated by Operator, HP and MP Only are Available</th>
<th>Main or Aux. Feedwater System</th>
<th>Moderator Acts as Heat Sink</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOCA2-4</td>
<td>RT15</td>
<td>PIC16</td>
<td>HTT</td>
<td>LI</td>
<td>CCD-M</td>
<td>ECCHID-M</td>
<td>FW2L</td>
<td>MHS6</td>
</tr>
</tbody>
</table>

**SEQUENCE-NAMES**

1. LOCA2-4-001
2. LOCA2-4-002
3. LOCA2-4-003
4. LOCA2-4-004
5. LOCA2-4-005
6. LOCA2-4-006
7. LOCA2-4-007
8. LOCA2-4-008
9. LOCA2-4-009
10. LOCA2-4-010

**END-STATE-NAMES**
PSA – Fault Tree Example

System Safety Society, Eastern Canada Chapter, June 18, 2009 - 14
Defence-in-Depth NS-R-1 - 2000

1. Prevent deviations from normal operation & system failures
2. Intercept deviations to prevent AOOs escalating to accidents
3. Provide engineered safety features to control, cool and contain accidents
4. Mitigate consequences of severe accidents to prevent off-site release
5. Mitigate off-site radiological consequences
Implementation of D-i-D

1. Conservative design, documented procedures, well-trained operators
2. Inherently safe response and reliable control systems
3. Safety systems to give high confidence that credible accidents are controlled
4. Mitigation of core damage and containment of radioactivity to minimise releases
5. Emergency measures to protect public in the event of a significant release
Management Systems - 2005

- CSA-N286-05
  - ‘Management System Requirements for Nuclear Power Plants’
- Replaces N286.0 to .7 (1986-2000)
  - Quality Assurance for Nuclear Power Plants
- Same management requirements apply to each phase of plant life (siting to abandon)
- Activities for one phase may occur during another phase
Refurbishments – Late-2000s

- Pickering A, Bruce A, Point Lepreau
- Integrated Safety Review performed
  - Comparison of plant, programs, etc against modern safety goals, meets current standards and regulatory requirements for safe and secure long-term operation.
- Pickering B decision imminent
- Darlington, Bruce B, Gentilly-2 likely soon
New NPP Build - 2009

• Environmental Assessment needed
  – Before any licensing
  – Covers full life cycle of station
• Site Evaluation: RD-310
• Modern Design: RD-337
  – Applies to new reactors
  – Will apply in phased manner to existing
• Safety Analysis: RD-310
Safety Areas and Program Areas

- Comprehensive assessment of performance of all processes, programs, systems, etc relevant to safety
- Developed from IAEA
- Darlington overall ‘Fully Satisfactory’
- Annual NPP Performance Report
### Darlington

#### Compliance and Safety Performance in 2008

<table>
<thead>
<tr>
<th>Safety Area</th>
<th>Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating Performance</td>
<td>FS</td>
</tr>
<tr>
<td>Performance Assurance</td>
<td>SA</td>
</tr>
<tr>
<td>Design and Analysis</td>
<td>SA</td>
</tr>
<tr>
<td>Equipment Fitness for Service</td>
<td>SA</td>
</tr>
<tr>
<td>Emergency Preparedness</td>
<td>FS</td>
</tr>
<tr>
<td>Environmental Protection</td>
<td>SA</td>
</tr>
<tr>
<td>Radiation Protection</td>
<td>FS</td>
</tr>
<tr>
<td>Safeguards</td>
<td>FS</td>
</tr>
<tr>
<td>Safety Area</td>
<td>Program</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>Operating Performance</td>
<td>Organization and Plant Management</td>
</tr>
<tr>
<td></td>
<td>Operations</td>
</tr>
<tr>
<td></td>
<td>Occupational Health and Safety (non-radiological)</td>
</tr>
<tr>
<td>Performance Assurance</td>
<td>Quality Management</td>
</tr>
<tr>
<td></td>
<td>Human Factors</td>
</tr>
<tr>
<td></td>
<td>Training, Examination and Certification</td>
</tr>
<tr>
<td>Design and Analysis</td>
<td>Safety Analysis</td>
</tr>
<tr>
<td></td>
<td>Safety Issues</td>
</tr>
<tr>
<td></td>
<td>Design</td>
</tr>
<tr>
<td>Equipment Fitness for Service</td>
<td>Maintenance</td>
</tr>
<tr>
<td></td>
<td>Structural Integrity</td>
</tr>
<tr>
<td></td>
<td>Reliability</td>
</tr>
<tr>
<td></td>
<td>Equipment Qualification</td>
</tr>
<tr>
<td>Emergency Preparedness</td>
<td></td>
</tr>
<tr>
<td>Environmental Protection</td>
<td></td>
</tr>
<tr>
<td>Radiation Protection</td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td></td>
</tr>
<tr>
<td>Safeguards</td>
<td></td>
</tr>
</tbody>
</table>
Summary

- Moved from equipment to humans to management systems
- Full life-cycle considered for new NPPs
- Five levels of Defence-in-Depth
- Safety principles of separation, independence, redundancy, diversity
- Prevention of process system failures is fundamental
Barriers to Fission Produce Release

- Fuel matrix
- Welded sheath cladding
- Primary circuit pressure boundary
- Containment
- Exclusion zone, evacuation