CANDU Safety
#9 - Grouping & Separation

Dr. V.G. Snell
Director
Safety & Licensing
Purpose of Grouping & Separation

- protection against events affecting a limited area of the plant
- common cause failures:
  - turbine disintegration and resultant missiles
  - fires
  - small aircraft strikes
  - failure of common support system
  - common adverse environment
- ensure that functional interconnections between systems do not change effectiveness for accidents
**Two Group Design Philosophy**

- ensure two independent ways to achieve same safety functions:
  - shutdown
  - remove decay heat and/or prevent release of radioactivity
  - monitor the plant
- group safety-related systems into two groups
  - Group 1 and Group 2
- reactor building is a natural barrier for some common cause events
  - both Group 1 & Group 2 systems are within reactor building
Three Types of Safety-Related Systems

- special safety systems
  - shutdown system 1, shutdown system 2, ECC, containment
- safety support systems
  - provide electrical power, instrument air & cooling water to special safety systems
- safety-related process systems
  - process systems which can mitigate an accident
Grouping

- each safety-related system assigned to one Group
- each Group can independently perform all the safety functions
- Group 1
  - power production systems
  - some of the special safety systems
  - safety support systems required by these special safety systems
- Group 2
  - the remaining special safety systems
  - safety support systems required by these special safety systems
**Systems Within Groups**

**Group 1**
- Normally Operating Process Systems
- Shutdown System 1
- Emergency Core Cooling System
- Safety Support Systems

**Group 2**
- Shutdown System 2
- Containment
- Safety Support Systems (EPS, EWS)

Interconnection of support services:
- Group 1 to Group 2 in Normal Operation
- Group 2 to Group 1 in accidents
- Group 1 to Group 2 in accidents
# System Grouping by Safety Function

<table>
<thead>
<tr>
<th>Safety Function</th>
<th>Group 1 Systems</th>
<th>Group 2 Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Shutdown</strong></td>
<td>Reactor Control System</td>
<td>Shutdown System 2</td>
</tr>
<tr>
<td></td>
<td>Shutdown System 1</td>
<td></td>
</tr>
<tr>
<td><strong>Heat Removal From Fuel</strong></td>
<td>Heat Transport System</td>
<td>Emergency Water System</td>
</tr>
<tr>
<td></td>
<td>Steam &amp; Feedwater Systems</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Shutdown Cooling System</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ECC</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Moderator</td>
<td></td>
</tr>
<tr>
<td><strong>Contain Radioactivity</strong></td>
<td>Reactor building air coolers</td>
<td>Containment &amp; containment subsystems</td>
</tr>
<tr>
<td><strong>Monitoring &amp; Control</strong></td>
<td>Main Control Centre</td>
<td>Secondary Control Area</td>
</tr>
</tbody>
</table>
**Rationale**

- Two shutdown systems are in separate groups so that a single event cannot prevent shutdown.
- ECC and containment are in separate groups so that a single event cannot damage fuel and allow radioactivity to escape.
- On CANDU 9, the grouping of containment and ECC has been switched for convenience in cable routing.
### Safety Support Systems

<table>
<thead>
<tr>
<th>Safety Support Function</th>
<th>Group 1 Safety Support</th>
<th>Group 2 Safety Support</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Electrical power</strong></td>
<td>Class IV</td>
<td>EPS Diesels</td>
</tr>
<tr>
<td></td>
<td>Class III diesels</td>
<td>Class II</td>
</tr>
<tr>
<td></td>
<td>Class II</td>
<td>Class I</td>
</tr>
<tr>
<td></td>
<td>Class I</td>
<td></td>
</tr>
<tr>
<td><strong>Service Water</strong></td>
<td>Raw Service Water</td>
<td>Emergency Water System</td>
</tr>
<tr>
<td></td>
<td>Recirculating Service Water</td>
<td></td>
</tr>
<tr>
<td><strong>Instrument Air</strong></td>
<td>Instrument Air System</td>
<td>Local Air Tanks</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Separation Between Groups

- outside reactor building, Groups in different areas of the plant
- typically 90 degree separation
- separate buildings for Emergency Power System diesels, Emergency Water System
- inside reactor building: barriers and physical separation to extent practical
- separation barrier or distance assessed to show adequacy
  - fire, missiles, harsh environment
- main control room protected from steam line breaks and external events so operators can proceed to SCA; access route protected
Plant Layout
Avoidance of Common Cause Failures

- where specified separation cannot be achieved:
  - show no credible hazard in area
  - another Group 2 system outside the area will mitigate
  - system or component protected by barrier
  - system or component is fail safe
  - component designed to withstand hazard
- Group 2 systems generally seismically qualified
- location above flood levels
# Instrumentation Cable Designations

<table>
<thead>
<tr>
<th>System Group</th>
<th>System Name</th>
<th>Channel Designation</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Reactor Regulating System</td>
<td>A</td>
</tr>
<tr>
<td></td>
<td></td>
<td>B</td>
</tr>
<tr>
<td></td>
<td></td>
<td>C</td>
</tr>
<tr>
<td>1</td>
<td>Shutdown System No. 1</td>
<td>D</td>
</tr>
<tr>
<td></td>
<td></td>
<td>E</td>
</tr>
<tr>
<td></td>
<td></td>
<td>F</td>
</tr>
<tr>
<td>1</td>
<td>Emergency Core Cooling System</td>
<td>K</td>
</tr>
<tr>
<td></td>
<td></td>
<td>L</td>
</tr>
<tr>
<td></td>
<td></td>
<td>M</td>
</tr>
<tr>
<td>2</td>
<td>Shutdown System No. 2</td>
<td>G</td>
</tr>
<tr>
<td></td>
<td></td>
<td>H</td>
</tr>
<tr>
<td></td>
<td></td>
<td>J</td>
</tr>
<tr>
<td>2</td>
<td>Containment System</td>
<td>N</td>
</tr>
<tr>
<td></td>
<td></td>
<td>P</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Q</td>
</tr>
<tr>
<td>1</td>
<td>Emergency Core Cooling System</td>
<td>KK</td>
</tr>
<tr>
<td></td>
<td>(seismically qualified)</td>
<td>LL</td>
</tr>
<tr>
<td></td>
<td></td>
<td>MM</td>
</tr>
</tbody>
</table>
Separation Within Groups (Examples)

- safety system triplicated instrumentation channels within a group separated by 1.5 metres
- power supplies split into “ODD” & “EVEN” to serve redundant components within a Group
- “ODD” & “EVEN” cables separated by 1.5 metres
- single channels within same Group can share common routing (e.g., A, D, K)
- buffering of connections between Main Control Room & SCA
- power cables >600 volts must be 0.45m. above instrumentation cables
Isolatable or Buffered Interconnections - 1

- Buffered control and instrumentation cables between the Main Control Room and the Secondary Control Area
  - to enable Group 2 equipment to be controlled from the Main Control Room
- Buffered post-accident monitoring and control cables
- Electrical power supply from the grid or from the turbine generator to Group 2 components, where required for reliability
- Cooling water supply from Group 1 to Group 2 components, where Group 1 supplies remain available or can be re-established for long-term reliability
Isolatable or Buffered Interconnections - 2

- Compressed air supply from Group 1 for the supply of air storage tanks during normal operation of the plant
- Support services from Group 2 (i.e., EWS, EPS) to Group 1 Special Safety Systems and other safety related components (e.g., supplies to ECC)
- Interconnections must ensure that failures cannot propagate from one Group to the other
LWR Approach (simplified)

- Two to four spatially separated identical trains
- Little or no redundancy within a train
- Each train fully qualified
CANDU Approach (simplified)

- two diverse, separated Groups
- redundancy within each Group
- qualification determined by safety function
Summary

- Common cause failures handled by grouping & separating mitigating systems
- Each group can perform key safety functions
- Separation protects against common cause failures of both groups
- Groups have limited cross-connections to increase reliability of mitigation for more frequent events
- Diversity is more important than redundancy
- Qualification depends on each specific accident to be mitigated