

## Information on Software Common-Cause Failure From Other Regulators\*

NRC Digital Instrument and Controls Meeting  
June 18, 2007

|         |         | Questions Asked of Regulators                        |  |   |   |   |
|---------|---------|--|--|---|---|---|
|         |         | Is diversity needed?                                 | Does the backup system need to be the same Safety Class? | Is Software Common Cause Failure (CCF) within Design Basis?                   | How is Probabilistic Safety Assessment (PSA) used for software? | Following an event, is there a minimum time until manual action can be considered? Is so, what? |
| Country | France  | Needed, but not required by regulation               | No   | No  | Not used  | Yes - 30 Min.   |
|         | Japan   | Needed, but not defined                              | No   | No (negotiated)   | Not required but done   | No  |
|         | Sweden  | Needed, but not specifically required by regulations | No   | No - Like Other Failures  | Impossible to do, not used                                      | Yes ≥ 30 Min.   |
|         | Germany | Yes  | Unknown  | No  | Not used  | Yes ≥ 30 Min.   |
|         | Taiwan  | Yes  | Depends  | Regulators - Yes<br>Vendors - No  | Qualitative, not Quantitative                                   | Unknown   |
|         | Canada  | Yes - Two diverse ways to shutdown reactor           | Yes - of same quality                                    | Based on Failure Frequency<br>>10 <sup>-6</sup> = design basis accident (DBA) | Software Reliability can't be measured                          | Yes - 15 Min.   |
|         | USA     | Yes  | No   | No  | Risk Informed but use Deterministic Process                     | No  |

\* Tabulated information represents answers gathered from verbal responses at a meeting among international regulators to discuss common-cause failures. Formal request for specific information may not have been requested of regulators in advance.