Control Room Chiller Example: Discussion Points

Public Meeting to Discuss the U.S. Nuclear Regulatory Commission (NRC) Staff Effort to Re-Evaluate its Position and Guidance on Digital Instrumentation and Controls Common Cause Failure

August 22, 2016
(Revision 1)

Agenda

- Summary of examples discussed at last CCF workshop
- Discussion points to address NRC staff specific questions about the Control Room HVAC Chiller example

Review of July 11 CCF Workshop Examples

- "Part 1" presented a representative industry example where the uncertainty about how to address CCF in the 50.59 process, and the potential need for an LAR and compliance with ISG-06, led to a decision to implement analog versus digital controls for a Chiller controls upgrade
- "Part 2" presented an industry proposed approach for some chiller applications*, which used techniques for susceptibility analysis, and demonstrated coping with the CCF to conclude that the resulting SSC malfunction is bounded by the current Safety Analysis (***Example 1***)
- "Part 3" presented industry proposed alternate approach for other chiller applications* which demonstrated "CCF not credible" through non-concurrent triggers, a "P" measure. CCF coping analysis not needed (***Example 2***)

**Note: Part 2 & Part 3 are different chiller applications that have distinct design and operational attributes*

Discussion Points

Industry will continue discussion of the Control Room Chiller Example, and address specific areas of interest identified by the NRC staff

- Design Basis
- Safety Analysis
- Safety Functions
- Adverse Impacts
- Technical Specifications
- Defense-in-Depth and Diversity
- Bounding Analyses
- Diverse Means
- Displays and Controls

Design Basis and Specific Safety Function

- **NRC Staff Question**: Please state the design basis for the plant system(s) being modified/proposed through the incorporation of new digital I&C technology
- **Industry Response**: To provide chilled water for HVAC for normal and accident conditions, with single failure criterion compliance (SFC) and compliance to qualification criteria for adverse environmental conditions. The plant's original chiller design basis does not require diversity at either the chiller or control system level.
- **NRC Staff Question**: Identify the specific safety functions required to be accomplished by the plant systems being modified.
- **Industry Response:** See above

Safety Analyses

- **NRC Staff Question**: Specifically, identify the plant safety analysis described in the FSAR that describes the need for the safety requirements that required to be accomplished by the new/modified safety system, and the events (AOOs and DBEs) that are required to be mitigated by the plant system(s) that require the use of the digital I&C technology
- **Industry Response**: The HVAC system is credited to keep the safety I&C and electro-mechanical mitigation systems within their temperature qualification envelope. It is also credited to maintain a habitable MCR environment for plant operators. Therefore, the chillers are credited for all AOOs and PAs as a support system.

Safety Function (1 of 2)

- **NRC Staff Question**: Please identify the specific safety functions within the modified plant system that are to be performed by the new digital I&C technology, and identify the consequences to the health and safety of plant workers and the environment, due to the failure to perform the required safety functions
- **Industry Response**: The chiller function is described on slide 4. If the chillers fail to perform their safety function, safety I&C and electro-mechanical mitigation SSCs could be adversely affected if the temperature exceeds qualification limits.

Safety Function (2 of 2)

- **NRC Staff Question**: If there are no direct safety functions being accomplished by the proposed new digital I&C technology, identify the indirect consequences of a failure or spurious actuation of the new digital I&C technology on the SSCs that are required to accomplish the safety functions
- **Industry Response**: See Slide 7 Response

Adverse Impact

- **NRC Staff Question**: Describe the adverse impact of these consequences to the health and safety of plant workers, the public, or the environment (e.g., 10 CFR Part 20, Part 100 consequences.)
- **Industry Response**: See response to the "Consequences" question on Slide 7

Technical Specifications

- **NRC Staff Question**: If there are any plant technical specifications associated with the SSCs that will require the operability of the digital I&C technology proposed, describe the Technical Specification Bases, and the operability requirements. Also describe the required actions to be taken if the required operability conditions cannot be met
- **Industry Response**: Westinghouse Standard Technical Specification 3.7.11 requires both trains of chillers to be operable. When one train is inoperable, restore operability within 30 days or the plant must be shutdown. With both trains inoperable, enter LCO 3.0.3 and proceed with a plant shutdown within 6 hours.

Defense-in-Depth and Diversity (1 of 3)

- **NRC Staff Question**: Perform an assessment of the defense-in-depth and diversity of the I&C system to demonstrate that vulnerabilities to CCF have been adequately addressed. Within this assessment, please specifically describe the effect of the potential CCF on the ability of the plant system to accomplish its required safety actions for each event (AOO or DBE) described in the safety analysis, using best estimate methods. Please demonstrate whether there is adequate diversity within the proposed design to be able to handle each event
- **Industry Response**: BTP 7-19, Point 1, allows demonstration that the "vulnerabilities to CCF have been adequately addressed" (i.e., a conclusion of CCF unlikely or not credible). Therefore, if there is no "potential CCF", it is not necessary to address the second sentence "describe the effect of the potential CCF on the ability of the plant system to accomplish its required safety actions for each event (AOO or DBE) described in the safety analysis, using best estimate methods", BTP 7-19, Point 2.

Defense-in-Depth and Diversity (2 of 3)

Industry Response: In addition, if there is no "potential CCF", it is not necessary to address the third sentence "demonstrate whether there is adequate diversity within the proposed design to be able to handle each event", BTP 7-19, Point 3. In *Example 2* from the July 11 workshop, we explained that for some chiller applications a CCF not credible conclusion can be reached by accepting the presence of a design defect and demonstrating that triggering of that defect in both safety divisions concurrently, is not credible.

Defense-in-Depth and Diversity (3 of 3)

Industry Response: In *Example 1* from the July 11 workshop, we explained for other chiller applications a CCF susceptibility analysis (i.e., "vulnerability to CCF") would conclude that a CCF is credible, BTP 7-19, Point 1. For these applications the second sentence, BTP 7-19, Point 2 would apply. We explained that the mitigation methods credited in Chapter 15 for AOOs and PAs would not be adversely affected, because "Operators can open safe shutdown equipment cabinet doors to reduce the local temperature rise caused by self-heating. Under these conditions, the equipment required for safe shutdown is not expected to reach their specified (best estimate) temperature limits (e.g., 60^{o}C for most electronic components). Based on this method of CCF coping, it is not necessary to address the third sentence "demonstrate whether there is adequate diversity within the proposed design to be able to handle each event", BTP 7-19, Point 3.

Bounding Analyses

- **NRC Staff Question**: Please identify whether, and if so, describe how, the failure of the proposed digital I&C technology may already be bounded by safety analyses currently described in the FSAR
- **Industry Response**:

  Referring to *Example 2*, a CCF of the chiller controls is not credible so there is no adverse effect on the systems credited in Ch. 15 to mitigate all AOOs and PAs. Referring to *Example 1*, a CCF of the chiller controls is credible but a best estimate analysis demonstrated that, through contingency actions, operators can cope with this CCF to prevent any adverse effect on the systems credited in Ch. 15 to mitigate all AOOs and PAs. Therefore, for both examples, since there is no adverse effect on the systems credited in Ch. 15 to mitigate all AOOs and PAs, there is no need for a bounding assessment.

  There is also no adverse effect on any system credited to reach safe shutdown.

Diverse Means

- **NRC Staff Question**: Please describe whether a postulated CCF could disable a safety function, and if so, whether a diverse means, with a documented basis that a diverse means is unlikely be subject to that same CCF, is available to perform either the same function, or a different function that results in mitigation of the AOO or DBE. Describe whether diverse or different function is performed by a safety or non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions. If it is a non-safety system, describe its quality to ensure it is sufficient to perform the necessary function under the associated event conditions
- **Industry Response**: For *Example 2*, a CCF of the chiller controls is not credible; therefore a safety function is not disabled. For *Example 1*, a CCF of the chiller controls is credible; therefore a safety function is disabled. But a best estimate analysis demonstrated that operators can cope with this CCF without a diverse means to perform the safety function. Therefore, for both examples, there is no need to perform an assessment to identify a diverse means to perform the safety function.

Displays and Controls (1 of 2)

NRC Staff Question:

Please describe whether there is a set of displays and controls located in the main control room which would enable the accomplishment of manual system level actuation and monitoring of the parameters that support the accomplishment of the required safety functions. Demonstrate whether any such displays and controls are independent and diverse from the safety system SSCs identified in item 2 above. Also, describe whether there are any alternate means for plant operators to be able to detect the failure of the proposed digital I&C and take timely action to accomplish the same safety functions to limit the consequences of a failure of the proposed digital I&C

Displays and Controls (2 of 2)

Industry Response:

- BTP 7-19 Point 4, applies to RTS and ESF actuation functions, and critical safety function monitoring, not to any specific plant component indications and controls.
- In the Chiller example, we demonstrated that BTP 7-19, Point 4 displays and controls are not adversely affected by the upgrade of the Chiller controls. In this case, we demonstrated this by no design commonality and no interactions.

Summary

In the July 11 CCF Table Top, industry provided two distinct chiller examples:

- *Example 1* concludes a CCF is credible but demonstrates that operators can cope with this CCF to ensure there is no adverse effect on any systems credited for AOO or PA mitigation, and no adverse effect on systems credited to achieve safe shutdown.
  - Therefore, this CCF is bounded by the current FSAR safety analyses.
- *Example 2* concludes a CCF is not credible based on the assumption of a design defect and demonstration that concurrent triggering of that defect in multiple safety divisions is not credible.
  - Single division failure of safety systems is a fundamental assumption of current FSAR safety analyses. Since there is no new malfunction, further assessment of the plant level effect is not applicable.