| | |
|---|---|
| **From:** | Carolyn Lauron |
| **To:** | Justin Hawkins |
| **Cc:** | Demetrius Murray; Greg Cranston; Andrew Brenner; Michael Dudek |
| **Subject:** | NRC Staff response to questions re: Common-Cause Failure, Common Mode-Failure, and Level/Pressure/Temperature Transmitters |
| **Date:** | Thursday, October 27, 2022 4:37:00 PM |

Hi Justin –

Please see the staff's responses below to the subject questions.
Please let us know if you need additional information.

Thank you,
Carolyn Lauron
USNRC

---

**Questions**:

1. Is there mention of CCF and/or CMF in the regulations?

   The reason we ask is because we are trying to determine if we're missing something when it comes to defining, and then applying the definitions in order to design-out CCFs and CMFs in our design.

   From NUREG-2225, CMF seems to be defined as: multiple failures which are dependent, thereby causing the joint failure probability to increase. The multiple failures are common mode or dependent because they result from a single initiating cause.

   From NRC ADMIN LTR 98-04, A CCF event consists of component failures that meet four criteria:
   (1) two or more individual components fail or are degraded, including failures during demand, failures during inservice testing, or deficiencies that would have resulted in a failure if a demand signal had been received;
   (2) components fail or are degraded within a selected period, such that success of the PRA mission would be uncertain;
   (3) component failures result from a single shared cause and coupling mechanism; and
   (4) a component failure occurs within the established component boundary.

   Are these definitions accurate?

2. Is there NRC guidance (RGs, NUREGs, etc.) that discusses what the NRC is looking for in the design, specifically when it comes to level/pressure/temperature transmitters that feed multiple safety systems for system initiation?

3. Related to Question #2 - Is there a limit on the number of ESF signals that can be fed from a single set of level/pressure/temperature transmitters (assuming the design doesn't violate design basis and has acceptable PRA parameters)? (inter-system common cause and common mode failures that impact multiple safety related systems or safety related functions)

**NRC Staff Response:**

1. There are a few references to “common-cause” and “common-mode” in the regulations, but the terms were not defined in the regulations (i.e., 10 CFR 50.2, 50.69, and 70.4). The CMF definition from NUREG-2225 and the four criteria are an accurate reflection of the terms.

   However, NUREG-2122, “Glossary of Risk-Related Terms in Support of Risk-Informed Decisionmaking,” (ML13311A353) defined and distinguished the terms. The definitions along with a portion of the discussions had been copied here. There is also a useful table with examples in the NUREG.

   > Common-Cause Failure: A failure of two or more structures, systems, or components as a result of a single shared cause. In a PRA, common-cause failure (CCF) is a special form of dependent failure in which the failure of the structure, system, or component (SSC) has occurred from the same fault. CCF faults generally reflect errors occurring as a result of a common manufacturer, environment, maintenance, etc.
   >
   > Common-Mode Failure: A failure of two or more structures, systems, or components in the same manner or mode as the result of a single shared cause. In a PRA, common-mode failure (CMF) is a special form of dependent failure that reflects (1) a common manner of failure (e.g., failure to start, failure to run) and (2) failure from a common cause. Consequently, CMF is actually a type of common-cause failure (CCF) in which the SSCs fail in the same way and from the same cause. CMF and CCF are often incorrectly used interchangeably. However, CCF only addresses the cause of the failure, while CMF addresses both the cause and the manner.

   For instrumentation and controls, there is not a regulatory requirement that directly references I&C common cause failure. However, potential common cause failures of digital systems need to be addressed with an appropriate diversity and coping assessment to demonstrate, in part, how GDC 22 is achieved; and to address the specific Commission direction in SRM-93-087 for addressing CCF (ML003708021). NRC staff implementation of Commission direction and acceptance criteria (including the definition of digital CCF) can be found in NUREG-0800 (Standard Review Plan) Branch Technical Position 7-19, Revision 8, “Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems,” (ML20339A647) and the Design-Specific Review Standard for the NuScale Design, Section 7.1, “Instrumentation and Controls – Fundamental Design Principles,” (ML15363A293). Note that NRC staff recently submitted SECY-22-0076 (ML22193A290) to recommend updating the current policy from SRM-SECY-93-087. The staff has recommended that the Commission expand the current common cause failure (CCF) policy for further use of risk-informed approaches.

2. There is not a regulatory requirement which prevents the sharing of sensors between safety related systems. Many operating plants share sensors between RPS and EFSAS safety systems for instance. However, the criteria of IEEE 603 Sections 5.1, “Single Failure Criteria,” and 5.6, “Independence,” must still be met for each of the safety systems involved. Therefore, the effects of a single sensor failure must be considered, and those effects would likely be greater if the sensor signals are shared among two or more safety systems. The safety functions of all safety systems that share the sensors would need to be considered. Additionally, the independence criteria of Section 5.6 include criteria for independence between Safety Systems and

Other systems (5.6.3). The criteria state the following:

> "The safety system design shall be such that credible failures in and consequential actions by other systems, as documented in 4.8
> of the design basis, shall not prevent the safety systems from meeting the requirements of this standard."

All safety systems that share the sensor would be considered as "other systems" in this context. Therefore, independence between safety systems must still be maintained when sensor signals are shared between them. This is usually achieved through the use of multiple channel redundancies. A loss of one channel in a 2 of 4 safety function will not result in a loss of safety functionality because the remaining three channels can still perform the safety function in a 2 of 3 coincidence.

3. There is no limit to on the number of ESF signals that can be fed from a single set of level/pressure/temperature transmitters. See response to Question #2 above for more details.