From:	Gutierrez, Mauricio
To:	FREGONESE, Victor (vxf@nei.org)
Cc:	Holonich, Joseph
Subject:	NRC Follow-up Action: Provide References on Definition of CCF to NEI
Date:	Thursday, September 14, 2017 3:56:00 PM
Attachments:	Common_Cause_Failure_Definitions.pdf

Vic,

At the September 7 meeting, we had a follow-up action to provide you with references with definitions of CCF for NEI to consider for use in NEI 16-16.

The attachment provides the references we mentioned to you and other references we reviewed this week. Our recommendation (the MP1B team reviewing NEI 16-16) is to use the first definition of CCF provided in IEEE 7-4.3.2, Annex G:

> Loss of function to multiple structures, systems, or components due to a shared root cause.

The attached document lists and provides the definitions of CCF in various sources we looked at (including those we recommended you look during the September 7, 2017 meeting).

Please note that this e-mail and the attachment will be placed in ADAMS. I'll send the accession number when it becomes available.

Mauricio R. Gutierrez
Instrumentations, Controls, and Electrical Engineering Branch
Office of Nuclear Regulatory Research, TWFN 10B03
Phone: 301-415-1925
email: Mauricio.Gutierrez@nrc.gov

Common Cause Failure Definitions in Various Sources

The MP1B team recommends adopting the first definition provided in IEEE 7-4.3.2, Annex G:

> **Loss of function to multiple structures, systems, or components due to a shared root cause.**

Definitions of CCF considered follow. All information is provided are quotations from listed references.

1. IEEE 7-4.3.2, Annex G

   Loss of function to multiple structures, systems, or components due to a shared root cause. (IEEE Std 603-2009)**.** Multiple failures of structures, systems, or components as a result of a single phenomenon. (IEEE Std 497™-2010 [B16])

2. NUREG 7007 (ML100541256) – Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems.

   Failure in redundant channels of the safe safety function.

   CCF is defined by the International Atomic Energy Agency (IAEA) as a "failure of two or more structures, systems or components due to a single specific event or cause" [10]. The IEC further adds to the CCF definition by noting that the "coincidental failure of two or more structures, systems or components is caused by any latent deficiency from design or manufacturing, from operation or maintenance errors, and which is triggered by any event induced by natural phenomenon, plant process operation, or action caused by man or by any internal event in the I&C system" [11]. CCF is a class of dependent failures in which the probability of failure is not expressible as the simple product of the unconditional failure probabilities of the individual events. Common-mode failure (CMF) is a subset of CCF and occurs when two or more systems or components fail in the same way. Source: IAEA S-G-1.3 – "Radiation Aspects of Design for Nuclear power Plants"

3. NEI 01-01 (ML020860169) - Guideline on Licensing Digital Upgrades TR-102348 Revision 1 NEI 01-01

   Failures of equipment or systems that occur as a consequence of the same cause. The term is usually used with reference to redundant equipment or systems or to uses of identical equipment in multiple systems. Common cause failures can occur due to design, operational, environmental, or human factor initiators. Common cause failures in redundant systems compromise safety if the failures are *concurrent failures,* that is, failures which occur over a time interval during which it is not plausible that the failures would be corrected.

   Common mode failure, by strict interpretation, has a meaning that is somewhat different from common cause failure because failure mode refers to the manner in which a component fails rather than the cause of the failure. However, because the discussions

in this guideline are concerned with failures that can compromise safety and disable redundant systems or disable multiple systems using the same equipment, regardless of whether they are common mode or common cause, the two terms are used interchangeably in this document. [Definitions adapted from the EPRI Equipment Qualification Reference Manual TR-100516 and ANSI/IEEE 352-1987]

4. NUREG 6303 (ML071790509) – Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems

   Common-mode failures (CMFs) are causally related failures of redundant or separate equipment. For example, (1) A CMF of identical subsystems across redundant divisions defeats the purpose of redundancy, or (2) A CMF of different subsystems or echelons of defense defeats the use of defense-in-depth. CMF embraces all causal relations, including severe environments, design errors, calibration and maintenance errors, and consequential failures. Common-mode failure is further elaborated in Guideline 3, and discussed in detail with respect to rules for postulating it in Guideline 6.

5. NUREG 2122 (ML13311A353) - Glossary of Risk-Related Terms in Support of Risk-Informed Decisionmaking

   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.

   The CCF term is often incorrectly used interchangeably with common-mode failure (CMF). CCF only accounts for the SSCs failing because of the same, single cause, not if they ultimately fail in the same manner (or in the same mode), which is CMF. In data provided to quantify CCF events, the failure mode is usually presented (i.e., failure to start, fail to run), and the cause is not always provided about why the failure mode occurs. There could be multiple causes lumped into the data presentation for a given failure mode. Thus, the available failure data dictate whether the PRA model is modeling CCF or CMF.

6. IEEE Std 379-2014 – IEEE Standard for Application of the Single Failure Criterion to Nuclear Power Generating station Safety Systems.

   Loss of function to multiple structures, systems, or components due to a shared root cause.

7. NUREG/CR 6268 (ML072970404) - Common-Cause Failure Database and Analysis System: Event Data Collection, Classification, and Coding

CCF events are component failures that satisfy four criteria: (1) two or more individual components fail, are degraded (including failures during demand or in-service testing), or have deficiencies that would result in component failures if a demand signal had been received; (2) components fail within a selected period of time such that success of the probabilistic risk assessment (PRA) mission would be uncertain; (3) components fail because of a single shared cause and coupling mechanism; and (4) components fail within the established component boundary.

8. IEEE 100-2000 The Authoritative Dictionary of IEEE Standards Terms

   Common-cause failure (1) (reliability data for pumps and drivers, valve actuators, and valves) Two or more redundant component failures due to a single cause. The common cause events that cause multiple failures are usually secondary events or events that exceed the design envelope of the component. (PE/NP) 500-1984w. (2) (nuclear power generating station safety systems) Multiple failures attributable to a common cause.

9. Methods for Assuring Safety and Dependability when Applying Digital Instrumentation and Control System – EPRI "CCF Guide"

   Concurrent failures (that is, multiple failures which occur over a time interval during which it is not plausible that the failures would be corrected) of multiple systems, structures or components (SSCs) that occur as a consequence of a single event, cause or activating condition. Malfunctions of multiple SSCs are considered CCFs. A CCF may be a failure of multiple SSCs within a single train system, in redundant divisions of a multi-train system, or in multiple plant systems. Note: I&C components and systems, and in some cases operators are SSCs (in the sense that they manipulate controlled SSCs in response to indications and alarms provided by the I&C components and systems).

10. IAEA Safety Glossary (http://www-pub.iaea.org/MTCD/publications/PDF/Pub1290_web.pdf)

    Common Cause Failure. Failure of two or more structures, systems and components due to a single specific event or cause**.** For example, a design deficiency, a manufacturing deficiency, operation and maintenance errors, a natural phenomenon, a human induced event, saturation of signals, or an unintended cascading effect from any other operation or failure within the plant or from a change in ambient conditions.

    Common Mode Failure. Failure of two or more structures, systems and components in the same manner or mode due to a single event or cause. i.e., common mode failure is a type of common cause failure in which the structures, systems and components fail in the same way.

11. IEC 62340 (2007)

    Failure of two or more structures, systems or components due to a single specific event or cause [IAEA Safety Glossary, Ed. 2.0, 2006]

    NOTE 1 The coincidental failure of two or more structures, systems or components is caused by any latent deficiency from design or manufacturing, from operation or maintenance errors, and which is triggered by any event induced by natural

phenomenon, plant process operation or an action caused by man or by any internal event in the I&C system.

NOTE 2 Coincidental failure is interpreted in a way which covers also a sequence of system or component failures when the time interval between the failures is too short to set up repair measures.

12. IEC 61513

Failure of two or more structures, systems or components due to a single event or cause [IAEA Safety Glossary 2007 edition, modified]

NOTE 1 Common causes may be internal or external to an I&C system.
NOTE 2 The IEC definition differs from the IAEA definition in two points:
1) The term “specific” was deleted because otherwise the definition of CCF is not consistent with the definition of CMF “Common mode failure”. Furthermore, this additional word is not necessary in order to understand the definition.
2) The word “and” was replaced by “or” because IEC/SC 45A experts thought it was a typing fault. In the online IAEA dictionary (NUSAFE) this correction was already done.