NEI PROPOSED REVISIONS
(Document Date: September 19, 2016)

2 DEFINITIONS

This section provides definitions for key terms that are important when using this appendix, and supplement those terms defined in the main body of NEI 96-07, Section 3.

~~**2.1 Common Cause Failure (CCF):** Postulated or actual concurrent failures where the first and second~~ or ~~multiple failures occur within a time interval that is less than that to detect the first failure and prevent subsequent failures of multiple systems, structures or components (SSCs) possessing the same undetected defect that manifests itself from a single event or cause. A single event or cause can be from a software defect, hardware failure, maintenance activity error, or an unanticipated consequence of combining multiple systems or components that previously functioned separately.~~

~~**2.2 Common Cause Failure Susceptibility Analysis:** An analysis that considers potential failure sources within an I&C system and identifies any existing preventive measures or limiting measures for each failure source. This analysis also identifies the SSC failure(s) caused by an I&C failure if the likelihood of the SSC failure(s) is not sufficiently low for each specific failure source.~~

~~There are two possible conclusions from a CCF Susceptibility Analysis: "CCF Unlikely" and "CCF Not Unlikely" (See separate definitions for each conclusion.)~~

~~**2.3 Common Cause Failure Susceptibility Analysis Conclusions:**~~

~~**(1) "CCF Unlikely" (Technical Conclusion):** Obtained from the CCF Susceptibility Analysis, a technical conclusion of "CCF Unlikely" is equivalent to a licensing condition of *NOT credible* and/or *NOT as likely to happen as those malfunctions previously considered and/or described in the UFSAR* .~~

~~**(2) "CCF Not Unlikely" (Technical Conclusion):** Obtained from the CCF Susceptibility Analysis, a technical conclusion of "CCF not unlikely" is equivalent to a licensing condition of *credible* and/or *as likely to happen as those malfunctions described in the UFSAR.*~~

2.4 Coping ~~Analysis~~ Strategy Categories: ~~An analysis that shows whether the mitigative measures are adequate to manage the undesirable effects of a failure (or misbehavior or CCF), assuming the measures that are in place to prevent the failure are not effective~~. Coping strategies can be placed the

following categories: Physical and Operational. Physical coping strategies involve physical modifications to the facility (including changes to Input Parameters) that would be implemented as part of the digital modification. Operational coping strategies involve modifications to how the facility is operated (as described in procedures) that would be implemented as part of the digital modification.

2.5 **Data**: A representation of facts, concepts, or instructions in a manner suitable for communication, interpretation, or processing by humans or by automatic means.

2.6 **Dependability:** A broad concept incorporating various characteristics of digital equipment, including reliability, safety, availability, and maintainability. This term reflects the notion that assurance of adequate quality and low likelihood of failure is derived from a qualitative assessment of the design process and the system design features.

The term *dependability* also reflects the importance of ensuring that the system performs its functions in a consistent and repeatable manner and its behavior is predictable. A *reliable* system that performs its intended function, but exhibits other undesirable behaviors, is not *dependable*.

2.7 **Digital modification**: A modification to a plant system or component which involves computers, computer programs, data (and its presentation), embedded digital devices, software, firmware, hardware, the human-system interface, microprocessors and programmable digital devices (e.g., Programmable Logic Devices and Field Programmable Gate Arrays). These modifications are often made to plant instrumentation and control (I&C) systems, but the term as used in this document also applies to mechanical or electrical equipment when the new equipment contains a computer (e.g., installation of a new heating and ventilation system which includes controls that use one or more embedded microprocessors).

~~**2.8** **Hazard Analysis:** (1) A process that explores and identifies conditions that are not identified by the normal design review and testing process. The scope of hazard analysis extends beyond plant *design basis* events by including abnormal events and plant operations with degraded equipment and plant systems. Hazard analysis focuses on system failure mechanisms rather than verifying correct system operation; (2) The process of identifying hazards and their potential causal factors. Conceptually, "hazard analysis" may be considered somewhat broader than "failure analysis" in the sense that it also considers situations in which there can be losses in the absence of any failures of systems, subsystems or components. This document uses the two terms interchangeably in the broader context.~~

Formatted: Font: Times, Bold, Italic

Formatted: Normal, Indent: Left: 0", First line: 0", Space Before: 0 pt, Widow/Orphan control, Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

NEI PROPOSED REVISIONS
(Document Date: September 19, 2016)

2.9 Human-System Interface (HSI): All interfaces between the digital system and plant personnel including operators, maintenance technicians, and engineering personnel (e.g., display or control interfaces, test panels, configuration terminals, etc.). These interfaces include information and control resources used by plant personnel to perform their duties and tasks. Currently, HSI is the term that is synonymous with and replaces human-machine interface (HMI) and man-machine interface (MMI). Principal HSIs are: alarms, information displays and controls. A HSI may be made up of hardware and software components and is characterized in terms of its physical and functional characteristics.

~~**2.10 Layers of Design:** This phrase will be used in the Screen Phase (Section 3) discussion regarding the consideration of possible adverse effects due to the combination of components and/or functions and refers to a licensing concept. Examples of *layers of design* are *independence* (e.g., two components with no commonality), *separation* (e.g., different physical locations or use of individual components), *redundancy* (e.g., duplication of equipment) and multiple sources (e.g., multiple electrical power sources, such as normal off-site power, and emergency on-site power provided by diesel generators and batteries; or multiple cooling water sources, such as normal make-up tanks, fire water tanks, refueling water tanks, cooling tower ponds and emergency off-site sources such as lakes, rivers and ponds).~~

2.w Structure, System and Component (SSC) Types: Due to the unique nature of digital modifications, including the use of software, specific SSC types will be defined, as follows:

(1) Duplicate vs. Redundant SSCs:

i. Duplicate SSCs: The term *duplicate SSCs* refers to SSCs that exist in multiple locations, but are not subject to single failure criteria. Examples of *duplicate SSCs* would be the two main feedwater pump control systems, one for each of the two main feedwater pumps. In this case, the main feedwater pump control systems and the main feedwater pumps are NOT subject to single failure criteria.

ii. Redundant SSCs: The term *redundant SSCs* refers to SSCs that exist in multiple locations and are subject to single failure criteria. Examples of *redundant SSCs* would be the two containment emergency chiller control systems, one for each of the two emergency chillers. In this case, both emergency chillers possess 100% capacity (of which only one is credited in safety analyses), and the control systems and the containment emergency chillers ARE subject to single failure criteria.

(2) Equivalent vs. Identical vs. Similar SSCs

(i) Equivalent SSCs: Equivalent SSCs possess unique characteristics (e.g., form, fit and function). Hardware is an example of *equivalent SSCs*. An example of equivalent hardware SSCs would be two or more different hardware Platforms (e.g., Platform X and Platform Y), each containing a set of unique parts that perform the same function, but are physically different. Software is also an example of *equivalent SSCs*. An example of equivalent software SSCs would be two or more different software Packages (e.g., Package A and Package B), each containing a unique set of coding that performs the same function.

(ii) Identical SSCs: Identical SSCs possess the exact same characteristics. Software is an example of an identical SSC (i.e., each copy of the software is exactly the same as all the other copies).

(iii) Similar SSCs: Similar SSCs possess common characteristics. Hardware is an example of *similar SSCs*. An example of similar hardware SSCs would be two or more hardware Platform Xs, each containing a set of common parts that perform the same function and are physically the same.

2.x Sufficiently Low: This phrase refers to the magnitude of the likelihood of a failure (e.g., a software common cause failure) that describes a likelihood of failure that is much lower than the likelihood of failures that are considered in the UFSAR (e.g., single failures) and comparable to other common cause failures that are not considered in the UFSAR (e.g., design flaws, maintenance errors and calibration errors).

~~**2.11 Variety:** This word will be used in the Screen Phase (Section 3) discussion regarding the consideration of possible adverse effects due to the combination of components and/or functions and refers to a licensing concept. An example of *variety* as a licensing concept is that a facility may have both *motor-driven* and *steam-driven* auxiliary feedwater pumps.~~