~~OWNER EDITED WITH TRACK CHANGES~~
~~Combined Alphabetically~~
All Definitions from NEI 01-01 Plus All Definitions from Appendix D

Commented [CN1]: Purple text is from NEI's proposal.

~~2~~3 DEFINITIONS

This section provides definitions for key terms as they are used in this guideline. Where possible, the definition of a term is traceable to an authoritative reference source. When the definition is taken directly from another document, the source is noted in brackets [ ]. Where a word is not defined explicitly in this section, it is understood in terms of common usage as defined in mainstream dictionaries.

~~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.~~

Commented [CN2]: NRC Comment: NEI indicated that App. D does not repeat information (e.g., definitions) from the main body of NEI 96-07, Rev. 1, because unlike NEI 01-01 (which is a separate document), App. D would become part of NEI 96-07, Rev. 1. However, NEI 96-07, Rev. 1, guidance often builds upon information in preceding paragraphs and it is impractical for App. D users to repeatedly to refer back to the main body of NEI 96-07, Rev. 1, to ensure necessary detailed understanding. NEI 01-01 appropriately addresses this by starting each section with summary excerpts from NEI 96-07, Rev. 1, immediately followed by a description of how to apply the excerpts to the unique characteristics of digital activities.

For the time being we want to repeat definitions from NEI 96-07.

accident previously evaluated in the FSAR (as updated). A design basis accident or event described in the UFSAR including accidents, such as those typically analyzed in Chapters 6 and 15 of the UFSAR, and transients and events the facility is required to withstand such as floods, fires, earthquakes, other external hazards, anticipated transients without scram (ATWS) and station blackout (SBO). [NEI 96-07, Rev. 1]

> Discussion: The term "accidents" refers to the anticipated (or abnormal) operational transients and postulated design basis accidents that are analyzed to demonstrate that the facility can be operated without undue risk to the health and safety of the public. For purposes of 10 CFR 50.59, the term "accidents" encompasses other events for which the plant is required to cope and that are described in the UFSAR (e.g., turbine missiles, fire, earthquakes and flooding). Accidents also include new transients or postulated events added to the licensing basis based on new NRC requirements and reflected in the UFSAR pursuant to 10 CFR 50.71(e), e.g., ATWS and SBO. [NEI 96-07, Rev. 1]

Adverse effects. Effects of a design change on a UFSAR-described design function that have the potential to increase the likelihood of malfunctions, increase consequences, create new accidents or otherwise meet the 10 CFR 50.59 evaluation criteria in paragraph 50.59(c)(2). [Excerpted from NEI 96-07, Revision 1]

Basic component. When applied to nuclear power plants licensed pursuant to 10 CFR Part 50, basic component means a structure, system, or component, or part thereof that affects its safety function, necessary to assure the integrity of the reactor coolant pressure boundary; the capability to shut down the reactor and

maintain it in a safe shut down condition; or the capability to prevent or mitigate the consequences of accidents which could result in potential offsite exposures comparable to those referred to in 10 CFR 50.34(a)(1) or 10 CFR 100.11. Basic components are items designed and manufactured under a quality assurance program complying with 10 CFR 50 Appendix B, or commercial grade items which have successfully completed the dedication process. [10 CFR 21.3]

Change. A modification or addition to, or removal from, the facility or procedures that affects a design function, method of performing or controlling the function, or an evaluation that the intended functions will be accomplished. [10 CFR 50.59~~NEI 96-07, Revision 1~~]

Commercial grade item (CGI). When applied to nuclear power plants licensed pursuant to 10 CFR Part 50, commercial grade item (CGI) means a structure, system, or component, or part thereof that affects its safety function, that was not designed and manufactured as a basic component. Commercial grade items do not include items where the design and manufacturing process require in-process inspections and verifications to ensure that defects or failures to comply are identified and corrected (i.e., one or more critical characteristics of the item cannot be verified). [10 CFR 21.3]

Commercial grade item dedication. When applied to nuclear power plants licensed pursuant to 10 CFR Part 50, dedication is an acceptance process undertaken to provide reasonable assurance that a commercial grade item to be used as a basic component will perform its intended safety function and, in this respect, is deemed equivalent to an item designed and manufactured under a 10 CFR Part 50, Appendix B, quality assurance program. This assurance is achieved by identifying the critical characteristics of the item and verifying their acceptability by inspections, tests, or analyses performed by the purchaser or third-party dedicating entity after delivery, supplemented as necessary by one or more of the following: commercial grade surveys; product inspections or witness at hold points at the manufacturer's facility; and analysis of historical records for acceptable performance. In all cases, the dedication process is conducted in accordance with the applicable provisions of 10 CFR Part50, Appendix B. The process is considered complete when the item is designated for use as a basic component. [10 CFR 21.3]

Common cause failure~~s~~. Multiple failures of structures, systems, or components as a result of a single phenomenon. [IEEE 497-2002]

Discussion: ~~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. The result of an event which, because of dependencies, causes a coincidence of failure states of components in two or more separate channels of a redundant system, leading to the failure of the defined system to perform its intended function. [SRP 15.0]

Discussion: *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]~~

Computer. A device that consists of one or more associated processing units and peripheral units, that is controlled by internally stored programs, and that can perform substantial computations, including numerous arithmetic operations, or logic operations, without human intervention during a run. Note: May be stand alone, or may consist of several interconnected units. [IEEE 100-2000]
~~Used broadly in this document to refer to any device which includes digital computer hardware, software (including firmware), and interfaces. [Derived from IEEE 74.3.2-1993] A microprocessor is considered as one type of computer.~~

Computer program. A combination of computer instructions and data definitions that enable computer hardware to perform computational or control functions. [IEEE 100-2000~~ANSI/IEEE 610.12-1990~~]

Consequences. In 10 CFR 50.59, the term consequences refers to radiological doses, to either the public or the control room operators, as a result of any accident evaluated in the UFSAR, but does not apply to the occupational exposures resulting from routine operations, maintenance, testing, etc. [Excerpted from NEI 96-07, Revision 1]

~~**Coping Strategy Categories.** 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.~~

Commented [BD3]: NRC Comment: Technical definitions must be from an authoritative technical reference.

~~**Data.** A representation of facts, concepts, or instructions in a manner suitable for communication, interpretation, or processing by humans or by automatic means. [ANSI/IEEE 610.12-1990]~~

Data. A representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by a programmable digital computer.~~humans or by automatic means.~~ [IEEE 100-2000]

Defense-in-depth. A concentric arrangement of protective barriers or means, all of which must be breached before a hazardous material or dangerous energy can adversely affect human beings or the environment. For instrumentation and control systems, the application of the defense in depth concept includes the control system; the reactor, trip, or scram system; the Engineered Safety Features Actuation System (ESFAS); the Anticipated Transients without Scram (ATWS); and the monitoring and indicator system and operator actions based on existing plant procedures. The echelons may be considered to be concentrically arranged in that when the control system fails, the reactor trip system shuts down reactivity; when both the control system and the reactor trip system fail, the ESFAS continues to support the physical barriers to radiological release by cooling the fuel, thus allowing time for other measures to be taken by reactor operators to reduce reactivity. [NUREG/CR-6303]

~~**Dependability.** As used in this document, a broad concept incorporating various characteristics of digital equipment, including reliability, safety, availability, maintainability, and others. [EPRI TR-106439 (adapted from NUREG/CR-6294)]~~

Dependability. A broad concept incorporating various characteristics of digital equipment, including reliability, safety, availability, ~~and~~ maintainability, and others. [EPRI TR-106439 (adapted from NUREG/CR-6294)]

Discussion: As used in the guideline, ~~T~~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.

Commented [BD4]: "Discussion" is an excerpt from NEI 01-01, 5.3.1 Factors that Affect Dependability.

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*.

Design bases. That information which identifies the specific functions to be performed by a structure, system, or component (SSC) of a facility, and the specific values or ranges of values chosen for controlling parameters as reference bounds for design. These values may be (1) restraints derived from generally accepted "state of the art" practices for achieving functional goals, or (2) requirements derived from

analysis (based on calculation and/or experiments) of the effects of a postulated accident for which a structure, system, or component must meet its functional goals. [10 CFR 50.2]

Design function. UFSAR-described design bases functions and other SSC functions described in the UFSAR that support or impact design bases functions. Implicitly included within the meaning of design function are the conditions under which intended functions are required to be performed, such as equipment response times, process conditions, equipment qualification and single failure. [NEI 96-07, Revision 1]

Discussion: Design bases functions are functions performed by systems, structures and components (SSCs) that are (1) required by, or otherwise necessary to comply with, regulations, license conditions, orders or technical specifications, or (2) credited in licensee safety analyses to meet NRC requirements.

UFSAR description of design functions may identify what SSCs are intended to do, when and how design functions are to be performed, and under what conditions. Design functions may be performed by safety-related SSCs or nonsafety-related SSCs and include functions that, if not performed, would initiate a transient or accident that the plant is required to withstand.

As used above, "credited in the safety analyses" means that, if the SSC were not to perform its design bases function in the manner described, the assumed initial conditions, mitigative actions or other information in the analyses would no longer be within the range evaluated (i.e., the analysis results would be called into question). The phrase "support or impact design bases functions" refers both to those SSCs needed to support design bases functions (cooling, power, environmental control, etc.) and to SSCs whose operation or malfunction could adversely affect the performance of design bases functions (for instance, control systems and physical arrangements). Thus, both safety-related and nonsafety-related SSCs may perform design functions.

Method of performing or controlling a function means how a design function is accomplished as credited in the safety analyses, including specific operator actions, procedural step or sequence, or whether a specific function is to be initiated by manual versus automatic means. For example, substituting a manual actuation for automatic would constitute a change to the method of performing or controlling the function.

Evaluation that demonstrates that intended functions will be accomplished means the method(s) used to perform the evaluation (as discussed in Section

3.10). Example: a thermodynamic calculation that demonstrates the emergency core cooling system has sufficient heat removal capacity for responding to a postulated accident.

[above discussion from NEI 96-07, Rev. 1]

~~**Digital upgrade.** A modification to a plant system or component which involves installation of equipment containing one or more computers (see above definition of computer). These upgrades are often made to plant instrumentation and control (I&C) systems, but the term as used in this document also applies to the replacement of 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).~~

Digital modification. As used in this guideline, this term means a~~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)

Diversity. (software) In fault tolerance, realization of the same function by different means. For example, use of different processors, storage media, programming languages, algorithms, or development teams. [IEEE 100-2000]

~~**Diversity.** The use of at least two different means for performing the same function.~~ Discussion: This can include diversity in *how* the function is performed (e.g., different algorithms, different variables sensed or physical principles applied, manual versus automatic) or in the *equipment* (different technologies, different hardware and/or software, different actuation means) used to perform the function. [Derived ~~from IEC 880, the EPRI Equipment Qualification Reference Manual TR 100516, NUREG/CR-6303, and~~ NUREG 0800 Branch Technical Position (BTP) 7-19, Rev. 7~~/HICB-19~~]

Diverse instrumentation and control systems (diverse I&C). Those systems provided expressly for diverse backup of the reactor trip system and engineered safety features actuation systems. Diverse I&C systems account for the possibility of common-mode failures in the protection systems. Diverse I&C systems include the anticipated transient without scram (ATWS) mitigation system as required by 10 CFR 50.62. For plants with digital computer-based instrumentation and

controls, diverse I&C systems may also include hardwired manual controls, diverse displays, and any other systems specifically installed to meet the guidance of the staff Requirements Memorandum on SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs." [NUREG-0800, Appendix 7-B - Acronyms, Abbreviations, and Glossary, SRP 7.8]

Electromagnetic compatibility (EMC). The capability of electronic equipment or systems to be operated in the intended operational electromagnetic environment at designed levels of efficiency. [IEEE 1050-1996] ~~The ability of equipment to function satisfactorily in its electromagnetic environment without introducing intolerable disturbances to that environment or to other equipment. [IEC 801-3-1984]~~

Electromagnetic interference (EMI). Impairment of a wanted electromagnetic signal by an electromagnetic disturbance. [IEEE 1050-1996] ~~Electromagnetic disturbance which manifests itself in performance degradation, malfunction, or failure of electrical or electronic equipment.~~
~~[IEC 801-3-1984]~~

Facility as described in the final safety analysis report (as updated).
(i) The structures, systems, and components (SSC) that are described in the final safety analysis report (FSAR) (as updated),
(ii) The design and performance requirements for such SSCs described in the FSAR (as updated), and
(iii) The evaluations or methods of evaluation included in the FSAR (as updated) for such SSCs which demonstrate that their intended function(s) will be accomplished.
[10 CFR 50.59]

Final Safety Analysis Report (as updated), The Final Safety Analysis Report (or Final Hazards Summary Report) submitted in accordance with 10 CFR 50.34, as amended and supplemented, and as updated per the requirements of 10 CFR 50.71(e) or 10 CFR 50.71(f), as applicable. [10 CFR 50.59]

~~**Final Safety Analysis Report (FSAR).** The original FSAR is submitted with the application for the operating license and reviewed by the NRC in granting the initial license to operate the facility. The updated FSAR (UFSAR) is the original FSAR as periodically updated per the requirements of 10 CFR 50.71(e).~~ Discussion: The UFSAR describes the design bases, safety analyses, and facility operation under conditions of normal operation, anticipated operational occurrences, design basis accidents, external events, and natural phenomena for which the plant is designed to function. The safety analyses described in the UFSAR demonstrate the integrity of the reactor coolant pressure boundary, the capability to shut down the reactor

and maintain it in a safe shutdown condition, and the capability to prevent or mitigate the consequences of accidents. [The above discussion was adapted from NEI 98-03, Revision 1]

Firmware. The combination of a hardware device and computer instructions and data that reside as read-only software on that device. [IEEE 1012-2004]~~Software that resides in read-only memory. [Adapted from IEEE 7-4.3.2-1993] An example is programmable read-only memory (PROM).~~

Hardware. Physical equipment used to process, store, or transmit computer programs or data. [IEEE 100-2000]~~ANSI/IEEE 610.12-1990~~]

Human-system interface (HSI). The interaction between workers and their equipment. This interaction requires information to flow in two directions. The system provides status information to the user, and the user provides control information to the system. [IEEE 100-2000]

> ~~**Human-System Interface (HSI).**~~ Discussion: HSI includes ~~A~~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.

Malfunction. In the context of 50.59, malfunction means the failure of a structure, system, or component to perform its intended design functions as described in the UFSAR (whether or not classified as safety-related in accordance with 10 CFR 50, Appendix B). [NEI 96-07, Revision 1]

Microprocessor. See computer.

~~**Radio-frequency interference (RFI).** A form of electromagnetic interference (EMI). EMI is a broader definition which includes the entire electromagnetic spectrum, whereas RFI is more restricted to the radio-frequency band, generally considered to be between 10 kHz and 50 GHz. These terms (RFI and EMI) have been superseded by the broader term electromagnetic compatibility EMC.~~

~~**Redundancy.** The provision of alternative (identical or diverse) equipment or systems so that any one can perform the required function, regardless of the state of operation or failure of any other. [Derived from EEC 880]~~

redundant equipment or system. A piece of equipment or a system that duplicates the essential function of another piece of equipment or system to the extent that either may perform the required function, regardless of the state of operation or failure of the other.
NOTE: Redundancy can be accomplished by the use of identical equipment, equipment diversity, or functional diversity. [IEEE Std 603-1991 (incorporated by reference into 10 CFR 50.55a)]

Reliability. The characteristic of an item or system expressed by the probability that it will perform a required mission under stated conditions for a stated mission time.
The characteristic of an item or system expressed by the probability that it will perform a required mission under stated conditions for a stated mission time. [IEEE 100-2000~~-577-1991 and IEEE 352-1987~~]

Safety related. See safety related systems, structures, and components.

Safety related systems, structures, and components (SSCs). Those systems, structures, and components that are relied upon to remain functional during and following design basis events to ensure (1) the integrity of the reactor coolant pressure boundary, (2) the capability to shut down the reactor and maintain it in a safe shutdown condition, or (3) the capability to prevent or mitigate the consequences of accidents that could result in potential offsite exposures comparable to the applicable guideline exposures set forth in section 50.34 (a)(1) or section 100.11 of 10 CFR. [10 CFR 50.2]

Screening. The process used to determine whether a proposed change (for which 10 CFR 50.59 is applicable) requires a 10 CFR 50.59 evaluation to be performed. [NEI 96-07, Revision 1]

Software. Computer programs, procedures, and possibly associated documentation and data pertaining to the operation of a computer system. ~~[ANSI/IEEE 610.12-1990]~~ [IEEE 829-2008]

Software safety analysis. The process of identifying and analyzing potential hazards (which may result either from failures of the digital system or from external conditions or events) that can affect the safety of the system and the plant. The process focuses on identifying requirements that are needed in order to prevent or mitigate hazards. Regulatory review guidance in BTP~~/HICB~~7-14 and in Regulatory Guide 1.173 states that there should be a defined safety analysis process

in which responsibilities and activities are defined for each phase of the development process. Software safety analysis can be a part of the broader failure analysis. , which is discussed in Section 5.

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.

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

Commented [BD5]: NRC Comment: Deleted proposed definition because it unnecessarily introduces new definition that is not used in endorsed technical or regulatory guidance. In other sections, simply state that a system is not subject to single failure criteria. .

Commented [BD6]: NRC Comment: Deleted proposed definition because it unnecessarily introduces new definition that is not used in endorsed technical or regulatory guidance. In other sections, simply use plain language descriptions, In addition, "equivalency evaluations" are used to determine if the replacement parts are a design change that needs a 50.59. New technical guidance for digital equivalency evaluations would need to be submitted and endorsed.

~~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).~~

Verification and validation (V&V). The process of determining whether the requirements for a system or component are complete and correct, the products of each development phase fulfill the requirements or conditions imposed by the previous phase, and the final system or component complies with specified requirements. [ANSI/IEEE 610.12-1990]

Commented [BD7]: NRC Comment: Deleted proposed definition because it unnecessarily introduces new definition that is not used in endorsed technical or regulatory guidance. In other sections, simply use plain language descriptions,