NUCLEAR ENERGY INSTITUTE

Vic Fregonese
Nuclear Energy Institute

November 2, 2017

MEETING BETWEEN THE U.S. NUCLEAR REGULATORY COMMISSION STAFF AND THE NUCLEAR ENERGY INSTITUTE TO DISCUSS NEI 16-16, "GUIDANCE FOR ADDRESSING DIGITAL COMMON CAUSE FAILURE"

Topics for Discussion

Follow on to September 7 meeting topics, discuss further areas to be clarified:

- Purpose/Intent of NEI 16-16
- Definition of Common Cause Failure
- Residual Uncertainty in CCF Sufficiently Low Conclusion
- Relaxed Acceptance Criteria and Technical Basis for Beyond Design Basis Events
- Technical Basis for CCF Sufficiently Low

NEI

Purpose/Intent of NEI 16-16

See marked-up handout.

Definition of Common Cause Failure

Proposed Definitions Developed by Staff and Industry

NRC Staff Proposal

Common Cause Failure (CCF)

"Loss of function to multiple structures, systems or components due to a shared root cause" (IEEE Std. 603-2009).

Industry Proposal

Common Cause Failure (CCF)

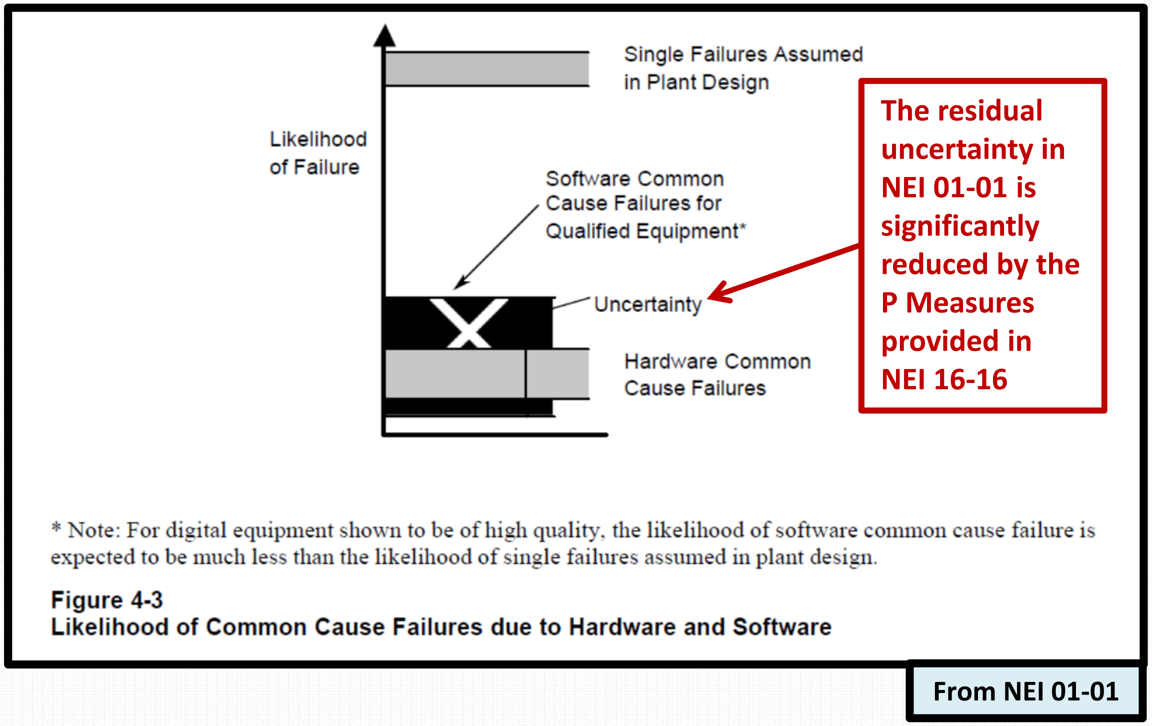
"Loss of function to multiple structures, systems or components due to a shared root cause" (IEEE Std. 603-2009).

For this guideline, the following notes apply: 1) Loss of function means a malfunction of multiple SSCs caused by a specific I&C failure source. 2) Shared root cause is limited to I&C failure sources, including single random hardware component failure, an environmental disturbance, a software design defect, and a human error.

We are adding these notes so the definition is constrained to the usage in NEI 16-16

Residual Uncertainty in CCF Sufficiently Low Conclusion

The information on this slide was presented in the September 7 meeting


Single Failures Assumed in Plant Design
Likelihood of Failure
Software Common Cause Failures for Qualified Equipment*
Uncertainty
X
Hardware Common Cause Failures

The residual uncertainty in NEI 01-01 is significantly reduced by the P Measures provided in NEI 16-16

* Note: For digital equipment shown to be of high quality, the likelihood of software common cause failure is expected to be much less than the likelihood of single failures assumed in plant design.

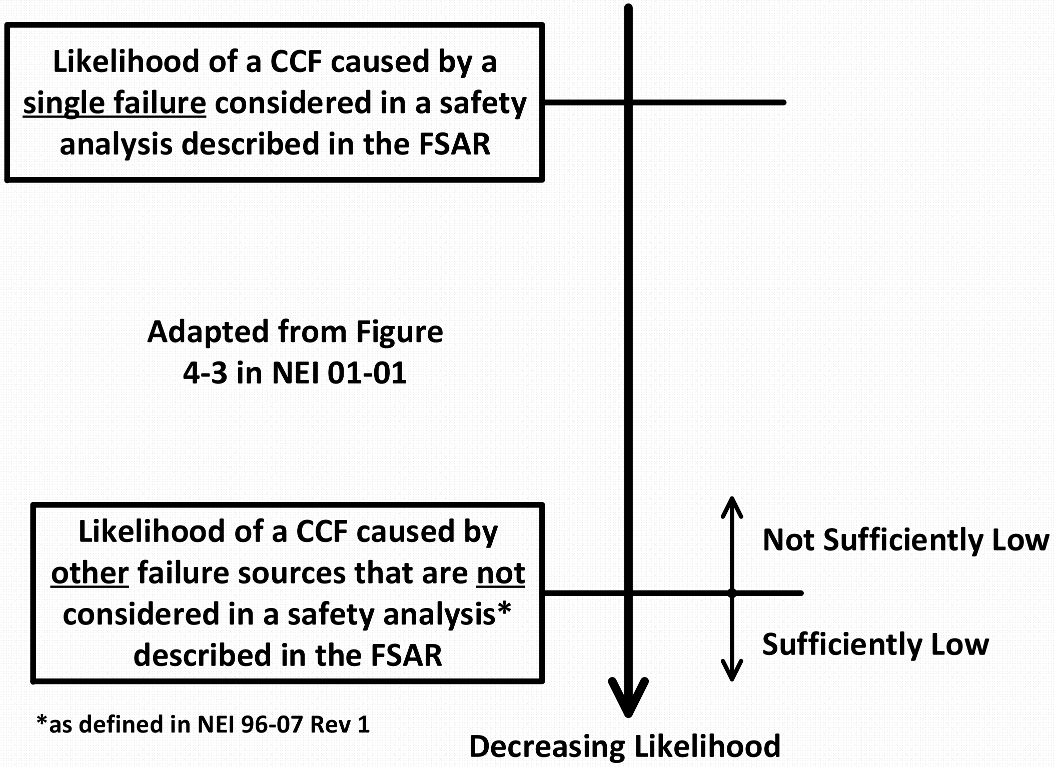
Figure 4-3
Likelihood of Common Cause Failures due to Hardware and Software

From NEI 01-01

It is helpful to compare NEI 16-16 to NEI 01-01. The residual uncertainty of software CCF in NEI 01-01 is based on uncertainties in quality and design processes for software. NEI 16-16 applies quality (as well as independence) as a ***Likelihood Reduction*** measure only, leaving the CCF as not sufficiently low. ***Preventive Measures*** in NEI 16-16 use quality, independence, and *additional design attributes* (such as avoiding concurrent triggers) to further reduce the software CCF likelihood so that the residual uncertainty of software CCF is no more significant than the residual uncertainty of hardware CCF, which is considered sufficiently low.

CCF "Sufficiently Low"

NEI 16-16 Uses the term "not credible". Now propose to use "Sufficiently Low" from draft Appendix D of NEI 96-07



Likelihood of a CCF caused by a single failure considered in a safety analysis described in the FSAR

Adapted from Figure 4-3 in NEI 01-01

Not Sufficiently Low

Likelihood of a CCF caused by other failure sources that are not considered in a safety analysis* described in the FSAR

Sufficiently Low

Decreasing Likelihood

***as defined in NEI 96-07 Rev 1**

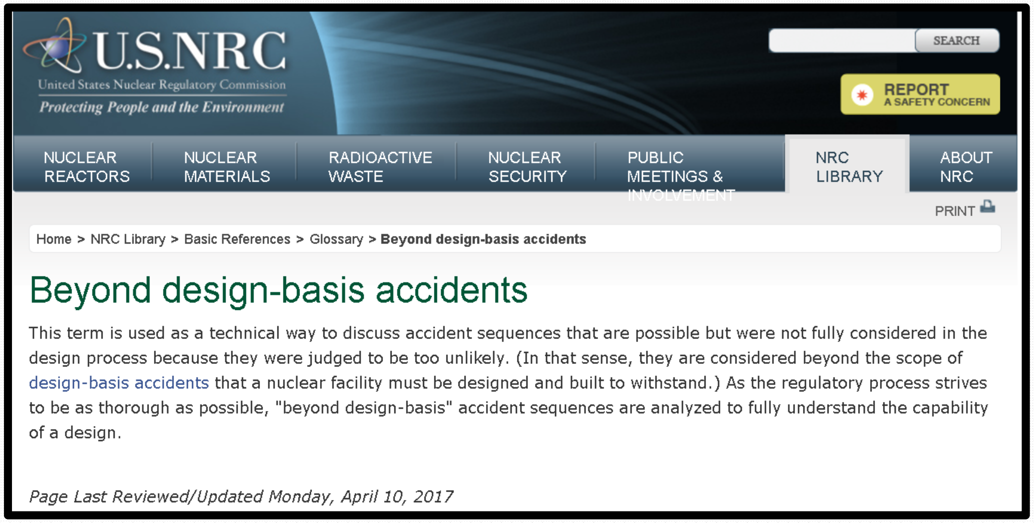
NEI 96-07 Appendix D:
3.15 Sufficiently Low
Sufficiently low means much lower than the likelihood of failures that are considered in the UFSAR (e.g., single failures) and comparable to other common cause failures that are not considered in the UFSAR (e.g., design flaws, maintenance errors, and calibration errors).

Technical Basis for BDBE

Presented at September 7 Meeting

With [an] *added degree of uncertainty regarding failures due to software, additional measures are appropriate for systems that are highly safety significant (i.e., high consequences on Figure 3-2) to achieve an acceptable level of risk. For digital upgrades to such systems, the defense- in-depth and diversity in the overall plant design are analyzed to assure that where there are vulnerabilities to common cause software failure, the plant has adequate capability to cope with these vulnerabilities (see Section 5.2). This defense-in-depth and diversity analysis is considered **a beyond design basis concern**, reflecting an understanding that while not quantifiable,* ***the likelihood of a common cause software failure in a high quality digital system is significantly below that of a single active hardware failure.***

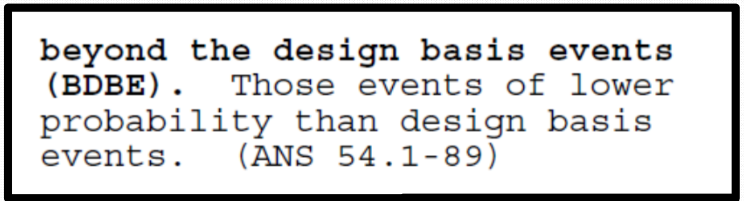
From NEI 01-01 Section 3.3.2


U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment
SEARCH
REPORT A SAFETY CONCERN
NUCLEAR REACTORS
NUCLEAR MATERIALS
RADIOACTIVE WASTE
NUCLEAR SECURITY
PUBLIC MEETINGS & INVOLVEMENT
NRC LIBRARY
ABOUT NRC
PRINT
Home > NRC Library > Basic References > Glossary > Beyond design-basis accidents

Beyond design-basis accidents

This term is used as a technical way to discuss accident sequences that are possible but were not fully considered in the design process because they were judged to be too unlikely. (In that sense, they are considered beyond the scope of design-basis accidents that a nuclear facility must be designed and built to withstand.) As the regulatory process strives to be as thorough as possible, "beyond design-basis" accident sequences are analyzed to fully understand the capability of a design.

Page Last Reviewed/Updated Monday, April 10, 2017



beyond the design basis events (BDBE). Those events of lower probability than design basis events. (ANS 54.1-89)

From ANS Glossary 2009

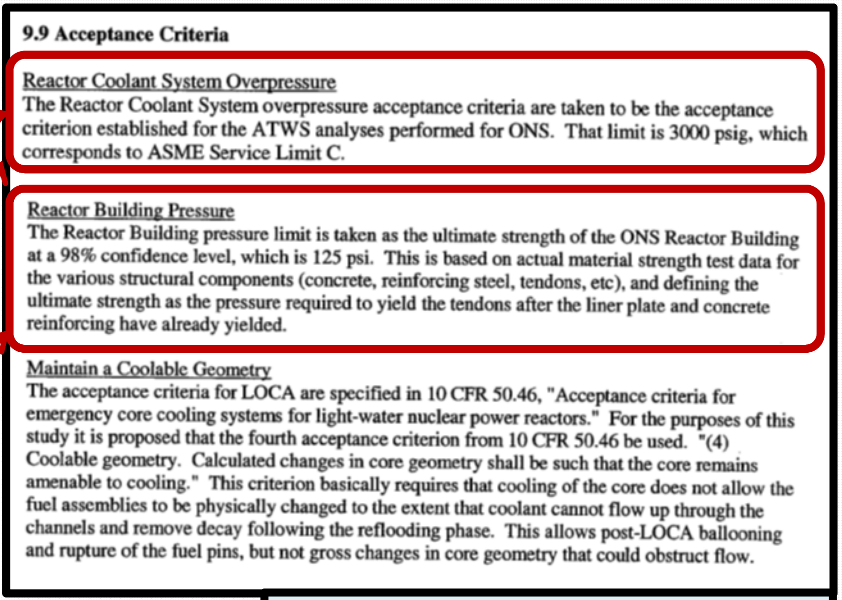
Acceptance Criteria for Beyond Design Basis Event (BDBE)

Presented at September 7 Meeting

Acceptance Criteria

1. For each anticipated operational occurrence in the design basis occurring in conjunction with each single postulated CCF, the plant response calculated using realistic assumptions should not result in radiation release exceeding 10 percent of the applicable siting dose guideline values or violation of the integrity of the primary coolant pressure boundary.
2. For each postulated accident in the design basis occurring in conjunction with each single postulated CCF, the plant response calculated using realistic assumptions should not result in radiation release exceeding the applicable siting dose guideline values, violation of the integrity of the primary coolant pressure boundary, or violation of the integrity of the containment (i.e., exceeding coolant system or containment design limits)

From BTP 7-19 Rev. 7 (ML16019A344)



9.9 Acceptance Criteria

Reactor Coolant System Overpressure

The Reactor Coolant System overpressure acceptance criteria are taken to be the acceptance criterion established for the ATWS analyses performed for ONS. That limit is 3000 psig, which corresponds to ASME Service Limit C.

Reactor Building Pressure

The Reactor Building pressure limit is taken as the ultimate strength of the ONS Reactor Building at a 98% confidence level, which is 125 psi. This is based on actual material strength test data for the various structural components (concrete, reinforcing steel, tendons, etc), and defining the ultimate strength as the pressure required to yield the tendons after the liner plate and concrete reinforcing have already yielded.

Maintain a Coolable Geometry

The acceptance criteria for LOCA are specified in 10 CFR 50.46, "Acceptance criteria for emergency core cooling systems for light-water nuclear power reactors." For the purposes of this study it is proposed that the fourth acceptance criterion from 10 CFR 50.46 be used. "(4) Coolable geometry. Calculated changes in core geometry shall be such that the core remains amenable to cooling." This criterion basically requires that cooling of the core does not allow the fuel assemblies to be physically changed to the extent that coolant cannot flow up through the channels and remove decay following the reflooding phase. This allows post-LOCA ballooning and rupture of the fuel pins, but not gross changes in core geometry that could obstruct flow.

From Oconee D3 Assessment (ML030920676)

"The ONS RPS/ESPS design includes diverse means to provide all required safety functions in the event of a software CCF. Safety functions that ***adequately address each licensing basis event*** *are provided in the design of the Diverse Actuation System. Based on this information, the NRC staff has determined that the proposed modification to the RPS/ESPS system complies with* [ISG 2 Staff Position 4, Effects of Common Cause Failure] *and is, therefore, approved."*

From Oconee RPS/ESFAS SER (ML100220016)

See Also:
- **ML060340449**
- **ML090510384**

NEI

Technical Basis for CCF Sufficiently Low (1 of 3)

Presented at September 7 Meeting

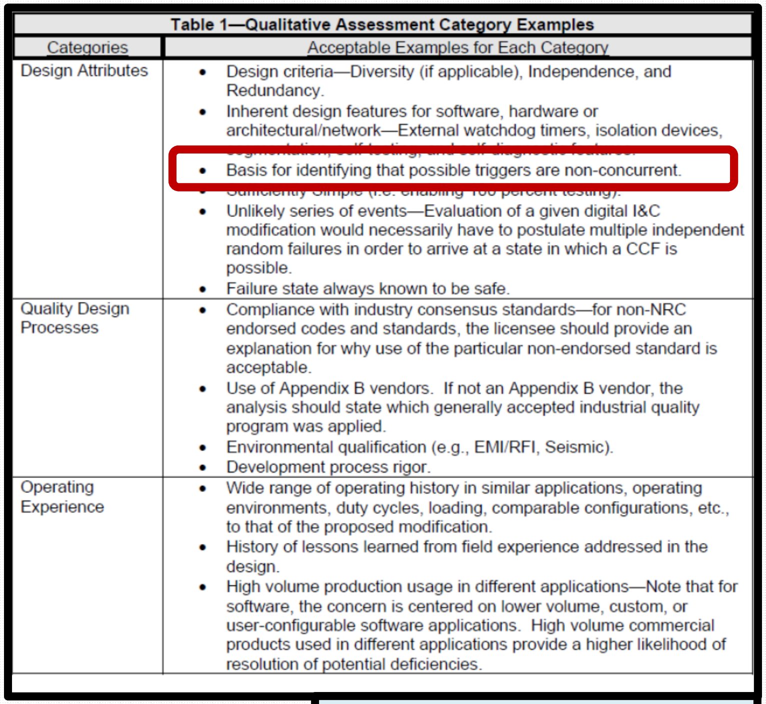
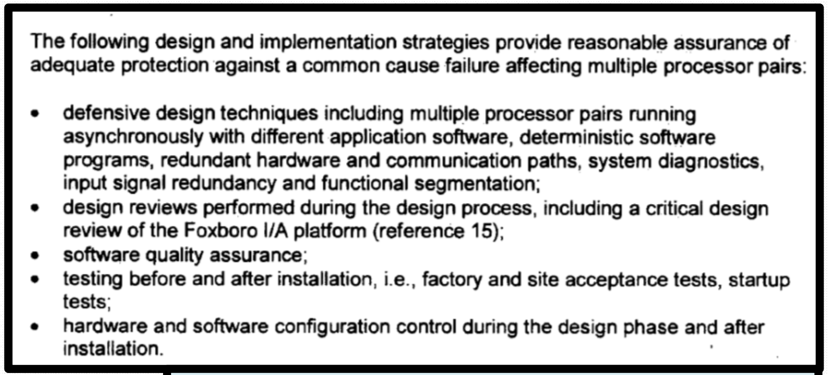


Table 1—Qualitative Assessment Category Examples

Categories	Acceptable Examples for Each Category
Design Attributes	• Design criteria—Diversity (if applicable), Independence, and Redundancy. • Inherent design features for software, hardware or architectural/network—External watchdog timers, isolation devices, segmentation, self-testing, and self-diagnostic features. • Basis for identifying that possible triggers are non-concurrent. • Sufficiently Simple (i.e. enabling 100 percent testing). • Unlikely series of events—Evaluation of a given digital I&C modification would necessarily have to postulate multiple independent random failures in order to arrive at a state in which a CCF is possible. • Failure state always known to be safe.
Quality Design Processes	• Compliance with industry consensus standards—for non-NRC endorsed codes and standards, the licensee should provide an explanation for why use of the particular non-endorsed standard is acceptable. • Use of Appendix B vendors. If not an Appendix B vendor, the analysis should state which generally accepted industrial quality program was applied. • Environmental qualification (e.g., EMI/RFI, Seismic). • Development process rigor.
Operating Experience	• Wide range of operating history in similar applications, operating environments, duty cycles, loading, comparable configurations, etc., to that of the proposed modification. • History of lessons learned from field experience addressed in the design. • High volume production usage in different applications—Note that for software, the concern is centered on lower volume, custom, or user-configurable software applications. High volume commercial products used in different applications provide a higher likelihood of resolution of potential deficiencies.

From RIS 2017-XX (ML17102B507)

Software CCF = Defect + Concurrent Trigger



The following design and implementation strategies provide reasonable assurance of adequate protection against a common cause failure affecting multiple processor pairs:

- defensive design techniques including multiple processor pairs running asynchronously with different application software, deterministic software programs, redundant hardware and communication paths, system diagnostics, input signal redundancy and functional segmentation;
- design reviews performed during the design process, including a critical design review of the Foxboro I/A platform (reference 15);
- software quality assurance;
- testing before and after installation, i.e., factory and site acceptance tests, startup tests;
- hardware and software configuration control during the design phase and after installation.

From WBN2 Segmentation Analysis (ML102240384)

*"In contrast with the degradation-caused fault modes of traditional hardware characterized in Section 2.1, logic does not wear and tear from repeated usage. If a system fails because of logic, it had some fault (**defect** or deficiency or weakness) from the time of introduction, but this fault remained latent until the occurrence of a **triggering** or enabling combination of inputs, state of the environment, state of the DI&C system, and state of the faulty logic."*

From NUREG/IA-0254 (ML11201A179)

*"Logic does not fail in the traditional sense of degradation of a hardware component but the system could fail, due to a pre-existing logic **fault**, **triggered** by some combination of inputs and system-internal conditions."*

From RIL-1002 (ML14197A201)

See Also:

- **ML16232A118**
- **ML15118A015**
- **ML072970404**

Technical Basis for CCF Sufficiently Low (2 of 3) Presented at September 7 Meeting

An example, about concurrent triggers

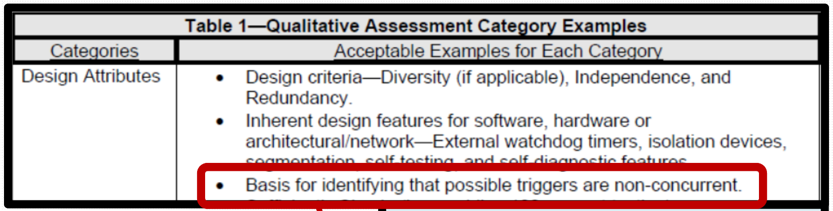


Table 1—Qualitative Assessment Category Examples

Categories	Acceptable Examples for Each Category
Design Attributes	• Design criteria—Diversity (if applicable), Independence, and Redundancy. • Inherent design features for software, hardware or architectural/network—External watchdog timers, isolation devices, segmentation, self-testing, and self-diagnostic features. • Basis for identifying that possible triggers are non-concurrent.

From RIS 2017-XX (ML17102B507)

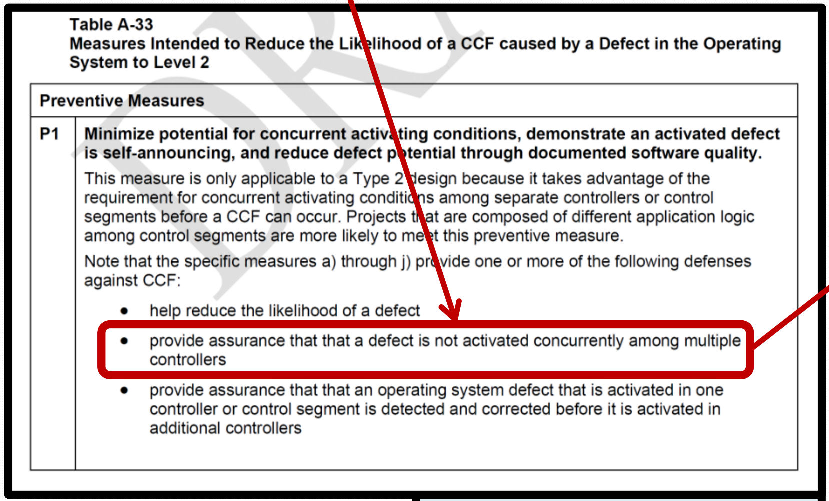


Table A-33
Measures Intended to Reduce the Likelihood of a CCF caused by a Defect in the Operating System to Level 2

Preventive Measures

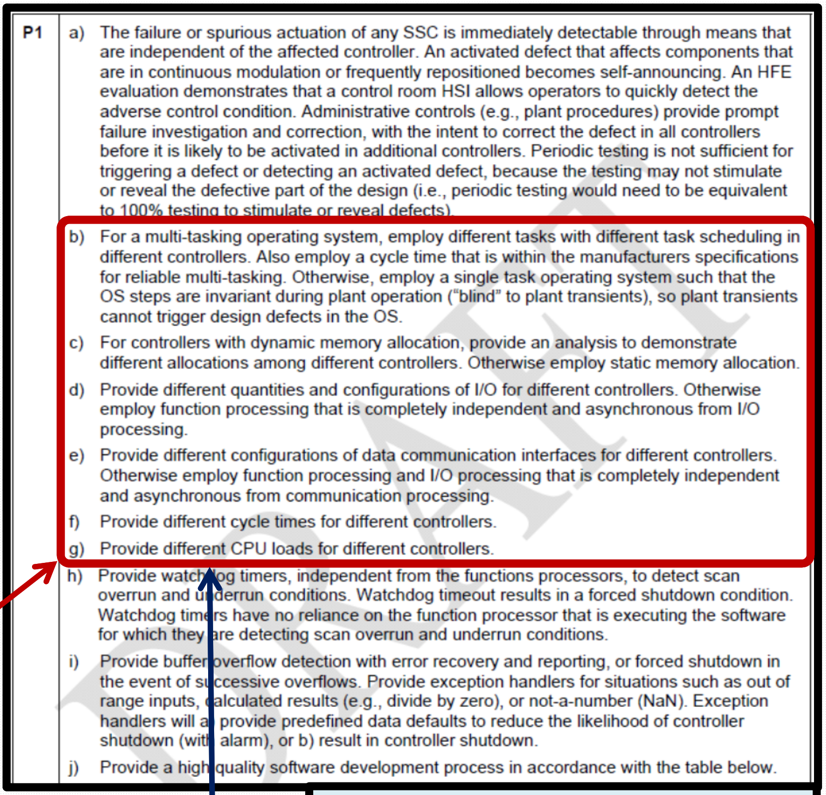
P1 **Minimize potential for concurrent activating conditions, demonstrate an activated defect is self-announcing, and reduce defect potential through documented software quality.**

This measure is only applicable to a Type 2 design because it takes advantage of the requirement for concurrent activating conditions among separate controllers or control segments before a CCF can occur. Projects that are composed of different application logic among control segments are more likely to meet this preventive measure.

Note that the specific measures a) through j) provide one or more of the following defenses against CCF:

- help reduce the likelihood of a defect
- provide assurance that that a defect is not activated concurrently among multiple controllers
- provide assurance that that an operating system defect that is activated in one controller or control segment is detected and corrected before it is activated in additional controllers

From NEI 16-16 Appendix A…



P1

a) The failure or spurious actuation of any SSC is immediately detectable through means that are independent of the affected controller. An activated defect that affects components that are in continuous modulation or frequently repositioned becomes self-announcing. An HFE evaluation demonstrates that a control room HSI allows operators to quickly detect the adverse control condition. Administrative controls (e.g., plant procedures) provide prompt failure investigation and correction, with the intent to correct the defect in all controllers before it is likely to be activated in additional controllers. Periodic testing is not sufficient for triggering a defect or detecting an activated defect, because the testing may not stimulate or reveal the defective part of the design (i.e., periodic testing would need to be equivalent to 100% testing to stimulate or reveal defects).

b) For a multi-tasking operating system, employ different tasks with different task scheduling in different controllers. Also employ a cycle time that is within the manufacturers specifications for reliable multi-tasking. Otherwise, employ a single task operating system such that the OS steps are invariant during plant operation ("blind" to plant transients), so plant transients cannot trigger design defects in the OS.

c) For controllers with dynamic memory allocation, provide an analysis to demonstrate different allocations among different controllers. Otherwise employ static memory allocation.

d) Provide different quantities and configurations of I/O for different controllers. Otherwise employ function processing that is completely independent and asynchronous from I/O processing.

e) Provide different configurations of data communication interfaces for different controllers. Otherwise employ function processing and I/O processing that is completely independent and asynchronous from communication processing.

f) Provide different cycle times for different controllers.

g) Provide different CPU loads for different controllers.

h) Provide watchdog timers, independent from the functions processors, to detect scan overrun and underrun conditions. Watchdog timeout results in a forced shutdown condition. Watchdog timers have no reliance on the function processor that is executing the software for which they are detecting scan overrun and underrun conditions.

i) Provide buffer overflow detection with error recovery and reporting, or forced shutdown in the event of successive overflows. Provide exception handlers for situations such as out of range inputs, calculated results (e.g., divide by zero), or not-a-number (NaN). Exception handlers will a) provide predefined data defaults to reduce the likelihood of controller shutdown (with alarm), or b) result in controller shutdown.

j) Provide a high quality software development process in accordance with the table below.

…continued from NEI 16-16 Appendix A

The configuration differences between controllers provide the technical basis for reasonable assurance that triggers are non-concurrent

Technical Basis for CCF Sufficiently Low (3 of 3)

“Consistent with the guidance provided in NEI 01-01, this attachment specifies three general categories of proposed design-related characteristics (described in Table 1 below) that can be used to develop justifications that demonstrate low likelihood of failure for a proposed modification. The aggregate of the three qualitative assessment categories form the technical basis for developing justifications based upon the likelihood of failure (i.e., single failures and CCF) of a digital I&C modification to a system or components.”

From RIS 2017-XX (ML17102B507)

The underlying design details in NEI 16-16 Appendix A provide the technical basis for each preventive measure. Licensees may develop alternate measures, but they must also provide their own technical basis.

Review

- NEI provided responses to NRC "Regulatory Purpose Discussion" handout
- NEI 16-16 will use same definition of CCF as NRC proposed definition, but with notes to align with purpose of NEI 16-16
- NEI 16-16 will use the same definition of "sufficiently low" provided in Appendix D
- NEI 16-16 will incorporate a figure illustrating CCF likelihood, adapted from NEI 01-01, and using the definition of sufficiently low
- The technical basis for BDBE is well founded in existing guidance and precedents
- The design details provided in NEI 16-16 Appendix A form the technical bases to "*demonstrate low likelihood of failure for a proposed modification*" (draft RIS 2017-XX) as long as those design details are fully implemented. Alternate measures require their own justification.

Questions or Comments?