NEI 16-16 [Draft 1]

Guidance for Addressing Digital Common Cause Failure

December 2016

[BLANK PAGE]

NEI 16-16 [Draft 1]

Nuclear Energy Institute

Guidance for Addressing Digital Common Cause Failure

December 2016

Nuclear Energy Institute, 1201 F Street N. W., Suite 1100, Washington D.C. (202.739.8000)

NOTICE

Neither NEI, nor any of its employees, members, supporting organizations, contractors, or consultants make any warranty, expressed or implied, or assume any legal responsibility for the accuracy or completeness of, or assume any liability for damages resulting from any use of, any information apparatus, methods, or process disclosed in this report or that such may not infringe privately owned rights.

EXECUTIVE SUMMARY

Implementation of digital technology at nuclear power stations can provide significant benefits in component and system reliability which can result in improved plant safety and availability. However, an improperly designed digital system may introduce a safety hazard through a potential common cause failure (CCF). This document describes those potential hazards and effective techniques that can be employed to address them including (1) methods for analysis of the susceptibility of digital Instrumentation and Control (I&C) systems to CCF and (2) methods for analysis of the plant level CCF malfunction result should a digital CCF be determined to be credible.

CCF is a concern for digital equipment that is credited to mitigate plant events and for digital equipment that can initiate plant transients. The CCF susceptibility analysis is a systematic, documented assessment by a digital engineer of potential CCF sources and the built-in defensive measures to prevent a CCF from those sources. Appropriate documentation of the analyses, justifications, and conclusions of these methods as quality records is critical to the process.

Where the CCF susceptibility analysis determines that a CCF is credible, additional assessments determine the subsequent system and component level malfunction effect of that CCF which are the effects on the plant equipment controlled, either manually or automatically, by the digital I&C equipment. If that subsequent system or component level malfunction is not previously analyzed, the likelihood of the CCF is determined. These conclusions of the CCF susceptibility analysis provide input to the plant level analysis of the CCF malfunction result.

The analysis of a credible CCF malfunction result is typically conducted by a transient and accident analyst to determine the plant level end result of the CCF. This analysis determines if the end result of the CCF malfunction is bounded by other previously analyzed transients or accidents in the deterministic safety analyses for the plant or if additional deterministic plant level analysis needs to be conducted to demonstrate plant safety.

The conclusions of the CCF susceptibility analysis and the analysis of the CCF malfunction result provide input to licensing actions planned for NRC submittal, and for determining whether a digital upgrade can be implemented under 10 CFR 50.59 without prior staff approval.

This document was developed by the Technical Issues Focus Group, a subcommittee of the NEI Digital I&C Working Group, in support of the industry response to Modernization Plan #1 (MP#1) Protection Against Common Cause Failure in the NRC’s Integrated Strategy to Modernize the Nuclear Regulatory Commission’s Digital Instrumentation and Control Regulatory Infrastructure (SECY-16-0070, ADAMS Accession No. ML16126A140). MP#1, contained in Enclosure 1 of SECY-16-0070, is identified as a high priority within the NRC Action Plan.

[BLANK PAGE]

TABLE OF CONTENTS

[BLANK PAGE]

[BLANK PAGE]

GUIDANCE FOR ADDRESSING DIGITAL COMMON CAUSE FAILURE

1 INTRODUCTION

1.1 OVERVIEW

The nuclear industry has been slow to adopt digital technology despite the need to take advantage of the benefits that digital technology can provide in improved component and system reliability, resulting in plant safety and availability gains, including through the replacement of obsolete analog and early digital components with modern technology. One of the primary barriers is the current regulatory position on mitigating software (SW) common-cause failure (CCF) in I&C designs does not align with industry positions on CCF likelihood, impact, and methods to prevent or mitigate a CCF.

This has resulted in regulatory uncertainty to both new plants and operating stations and has led many nuclear stations to avoid digital technology, except for limited applications, thus not fully realizing the safety and economic benefits available from digital technology. The adoption of additional measures to address CCF is needed to implement certain digital upgrades under the 10CFR50.59 process for operating plants and provide a more predictable regulatory approval process for digital systems for new plants, thus providing significant cost savings and schedule certainty for digital projects.

The current NRC policy on digital system CCF is within Staff Requirements Memorandum (SRM) to SECY-93-087, which, in conjunction with the staff's interpretation of the policy contained in NRC Branch Technical Position (BTP) 7-19, puts forth that there are only two design attributes that may be credited to eliminate the need for further consideration of CCF: diversity within the digital I&C system, or "testability" based on device simplicity. Neither of these defensive measures are practical for most applications necessitating the demonstration of coping with a CCF for which there is insufficient industry guidance.

The goal of this document is to provide a practical success path to address CCF, including defensive measures that can be credited to prevent CCF in addition to those in the current NRC policy for both operating and new plants. The methods presented are based on the recognition that improperly designed digital systems that have not adequately addressed CCF can challenge plant safety.

This document provides technical guidance for addressing CCF for compliance to deterministic licensing criteria and current NRC policies (e.g. SRM-SECY-93-087, BTP 7-19, and 10 CFR 50.59). This document does not contain risk insights, as risk insights are not credited when addressing these deterministic licensing criteria. NEI intends to pursue utilization of risk insights for inclusion in a future revision to this document.

1.2 PROCESS DESCRIPTION

The flow chart below summarizes the guidance in this document. The flow chart includes numbers that correlate to the sections of this document. Similarly, unless otherwise stated, references to Sections refer to sections within this document. The guidance depicted in the flow chart and described in this document is summarized as follows:

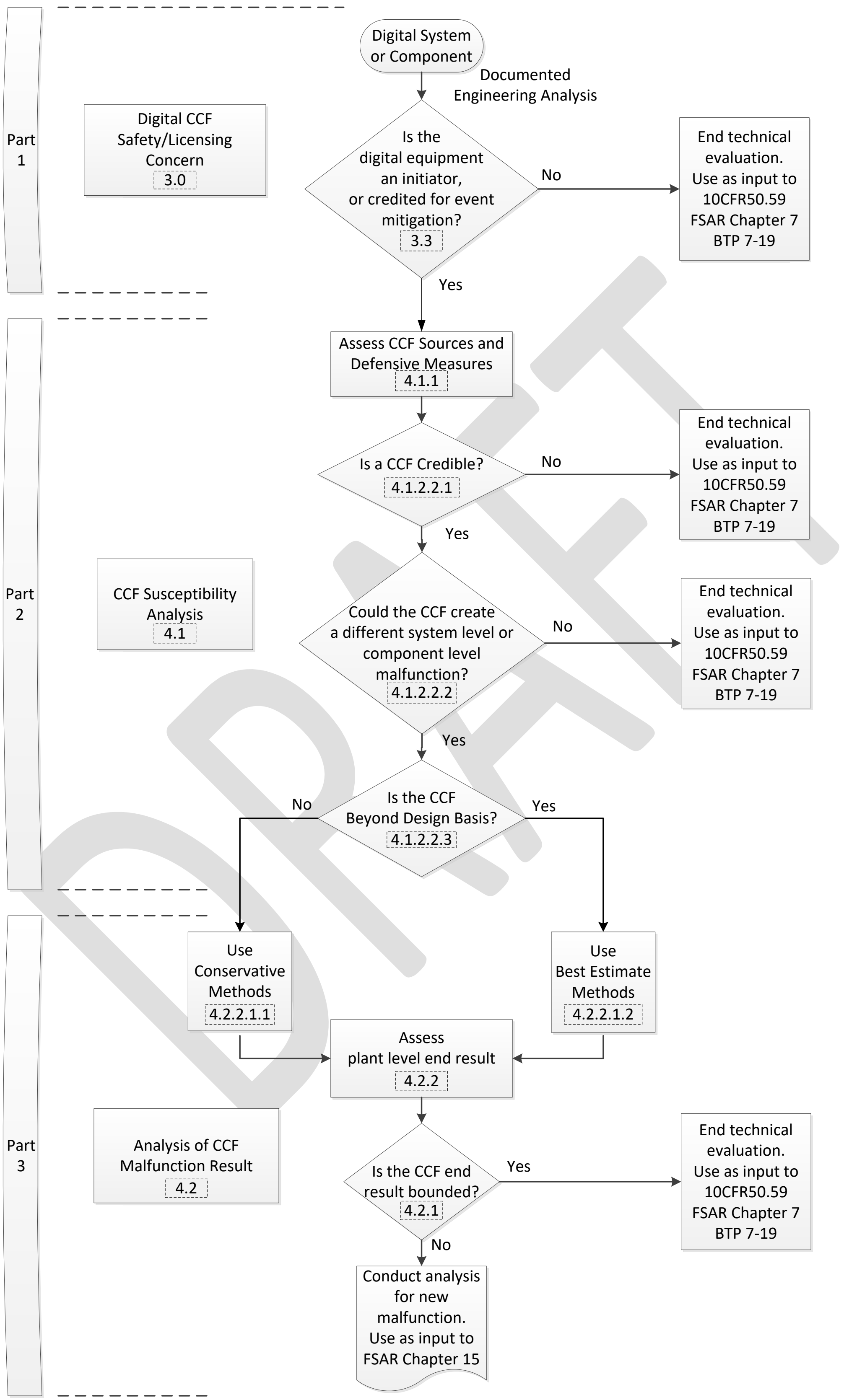
For digital I&C systems or components that can affect a design function described in the FSAR, a CCF analysis is documented. The documentation is maintained as a quality record. The CCF analysis has three parts:

1. Part 1 determines if a CCF in the target digital equipment is a safety or licensing concern; if not the analysis is complete. CCF is a concern for digital systems or components that are credited for abnormal event mitigation or for digital systems or components that can initiate transients. The basis for this concern is described in Section 3. Most important in understanding this CCF concern is that I&C equipment controls plant equipment (e.g., pumps, valves, electrical breakers), and when an I&C failure adversely affects multiple plant components (i.e., a CCF) there is the potential for an unanalyzed plant condition.

2. Part 2 is referred to as the CCF susceptibility analysis; the detail is described in Section 4.1. For digital equipment of concern from Part 1, a digital engineer conducts a systematic assessment of potential CCF sources and the built-in design and design process attributes that can prevent, limit or reduce the likelihood of that CCF; collectively, these attributes are referred to as defensive measures. Through the CCF susceptibility analysis the digital engineer determines the following:
   a. Is a CCF credible; if not, the analysis is complete.
   b. If the CCF is credible, are the subsequent malfunctions in systems or components effected by the target I&C equipment already included in a deterministic analysis within the FSAR; if so the analysis is complete.
   c. If the subsequent malfunctions are not included in the FSAR, additional deterministic plant level analysis is needed in Part 3. The Part 3 analysis uses methods and acceptance criteria that are dependent on whether the CCF is within the plant design basis or beyond design basis. The digital engineer makes this determination based on the likelihood of the CCF, which is dependent on the available defensive measures.

3. Part 3 is referred to as the analysis of the CCF malfunction result; the detail is described in Section 4.2. This analysis examines the system level and component level malfunctions that were not previously analyzed (from Part 2), to determine if those malfunctions result in plant level conditions that are bounded by a previous deterministic analysis within the FSAR; if so, the analysis is complete. If not, additional deterministic plant level analysis is needed to address the new malfunctions. When demonstrating bounding or when conducting additional analysis, the method of coping with the CCF is clearly documented. Sections 4.2.1 and 4.2.2 distinguish the analysis methods, acceptance criteria and acceptable coping methods for design basis versus beyond design basis CCFs, as discussed above. In addition, Section 4.2.2.2 describes analysis differences for systems that are credited to mitigate abnormal events and systems that can be transient initiators.

GUIDANCE FOR ADDRESSING DIGITAL COMMON CAUSE FAILURE


Part 1
Digital CCF Safety/Licensing Concern 3.0
Digital System or Component
Documented Engineering Analysis
Is the digital equipment an initiator, or credited for event mitigation? 3.3
No
End technical evaluation. Use as input to 10CFR50.59 FSAR Chapter 7 BTP 7-19
Yes
Part 2
Assess CCF Sources and Defensive Measures 4.1.1
Is a CCF Credible? 4.1.2.2.1
No
End technical evaluation. Use as input to 10CFR50.59 FSAR Chapter 7 BTP 7-19
Yes
CCF Susceptibility Analysis 4.1
Could the CCF create a different system level or component level malfunction? 4.1.2.2.2
No
End technical evaluation. Use as input to 10CFR50.59 FSAR Chapter 7 BTP 7-19
Yes
Is the CCF Beyond Design Basis? 4.1.2.2.3
No
Yes
Part 3
Use Conservative Methods 4.2.2.1.1
Use Best Estimate Methods 4.2.2.1.2
Assess plant level end result 4.2.2
Analysis of CCF Malfunction Result 4.2
Is the CCF end result bounded? 4.2.1
Yes
End technical evaluation. Use as input to 10CFR50.59 FSAR Chapter 7 BTP 7-19
No
Conduct analysis for new malfunction. Use as input to FSAR Chapter 15

2 DEFINITIONS

2.1 BEST ESTIMATE METHOD

A method of analysis that can employ realistic/nominal initial plant conditions and equipment performance, relaxed acceptance criteria, no other assumed equipment failures, credit for beneficial control system action, and allows conclusions based on qualitative expert judgment or quantitative analysis. Best estimate methods can be applied when a CCF is concluded to be beyond design basis. Best estimate methods are applicable when demonstrating a CCF is bounded by a previous analysis (e.g., to address 10 CFR 50.59 Question 6), and when conducting additional analysis.

2.2 BOUNDED

Refers to a potential conclusion from the analysis of a CCF malfunction result. A bounded conclusion means that the plant level results of the CCF malfunction are no worse than the plant level results of other malfunctions that have been previously analyzed in deterministic safety analyses.

2.3 COMMON CAUSE FAILURE

A CCF is the malfunction of two or more plant components or functions caused by a specific I&C failure source that is shared by those plant components or functions, or is common to those plant components or functions. I&C failure sources of particular concern are a single random hardware component failure, an environmental hazard, and a design defect, any of which can cause a CCF.

2.4 CCF BEYOND DESIGN BASIS

The likelihood of a CCF caused by an I&C failure source is significantly reduced (or less likely) compared to a CCF due to a single random hardware failure. A CCF beyond design basis conclusion is used only to determine the method and acceptance criteria for the analysis of a CCF malfunction result, not to preclude the need for that analysis.

2.5 CCF NOT CREDIBLE

The likelihood of a CCF caused by an I&C failure source is no greater than the likelihood of a CCF caused by other failure sources that are not considered in deterministic safety analysis. A CCF not credible conclusion means no further deterministic safety analysis is necessary, since reasonable assurance exists that the CCF is sufficiently unlikely. Otherwise, a deterministic analysis of the CCF malfunction result is necessary.

2.6 COPING

For a credible CCF, coping refers to (1) the event mitigation methods credited to demonstrate that the CCF malfunction result is bounded by a previous deterministic analysis, or (2) the event mitigation methods credited in an additional deterministic plant level analysis to demonstrate that the plant remains safe.

2.7 DEFENSIVE MEASURE

Design or design process attributes that can be assembled together to establish a P, L or LR measure. Defensive measures refer to design attributes within the target digital equipment to prevent, limit or reduce the likelihood of a CCF. Defensive measures are distinguished from coping or mitigating measures, which are external to the target digital equipment and credited to maintain the plant in a safe condition after the CCF occurs.

2.8 DIGITAL ENGINEER

Digital engineer is used only to distinguish the analysis activities typically conducted by an I&C engineer skilled in digital design practices, from analysis activities conducted by others. There are no formally defined digital engineer qualifications.

2.9 DETERMINISTIC ANALYSIS

This refers to analyses that do not employ probabilistic or risk informed methods.

2.10 LIMITING MEASURE

A limiting (L) measure is a set of defensive measures that when applied as a set, provide a predictable component level malfunction for a credible CCF.

2.11 LIKELIHOOD REDUCTION MEASURE

A likelihood reduction (LR) measure is a set of defensive measures that when applied as a set, reduce the likelihood of a credible CCF.

2.12 PREVENTIVE MEASURE

A preventive (P) measure is a set of defensive measures that when applied as a set, provide reasonable assurance that a CCF potentially caused by a specific I&C failure source is not credible.

3 BACKGROUND

3.1 POTENTIAL SAFETY ISSUE WITH CCF

Plant safety is assured for events that have been considered in the deterministic analyses within the plant's FSAR; these have been the transient and accident analyses (in Chapter 15 for recent plants), and a few other specific events described in other chapters of the FSAR, such as a Station Blackout (in Chapter 8 for recent plants). While the plant may be safe for other events that are not considered in these traditional deterministic safety analyses, there is no certainty of safety without additional deterministic analysis.

A CCF is the malfunction of two or more plant components or functions caused by a specific I&C failure source. CCFs in safety and non-safety systems are not considered in the traditional deterministic safety analyses, except for a few very specific cases.

With the exception of the CCFs that lead to Anticipated Transient Without Scram (ATWS) and Station Blackout (SBO), the Anticipated Operational Occurrences (AOO) and Postulated Accidents (PA) in the FSAR are analyzed with a concurrent failure in one safety division of the credited mitigation functions. For other AOOs and PAs, a concurrent failure that affects multiple divisions of a system or function credited for mitigation (i.e., a CCF) would result in an accident condition that has not been considered in deterministic safety analyses.

The analyzed AOOs are the plant transients that are expected to occur during the life of the plant. Due to the inherent partitioning forced by analog technology, these AOOs are typically the transients that are expected due to the malfunction of a single plant component, system or function. With current digital technology, the concern is an I&C failure that affects multiple plant components, systems or functions (i.e., a CCF) and thus has the potential to cause unanalyzed plant transients.

3.2 POTENTIAL CHALLENGES PRESENTED BY DIGITAL DESIGN

Digital technology makes it possible to allocate multiple controlled plant components to a single control segment (i.e., one non-redundant or redundant controller and its peripherals, controlling multiple plant components). Analog controls could only be constructed with a limited combination of functions. Therefore, due to the inherent capability of digital technology compared to its analog predecessor, digital systems typically have:

1. More shared hardware resources (e.g., controllers, networks, workstations),
2. More complex designs (i.e., greater likelihood for a design defect)

Therefore, an improperly designed digital system may introduce a safety hazard through a greater potential for a common cause failure (CCF), and the potential for greater consequences, than for their analog predecessors. A CCF can pose a potential safety hazard that is often not well understood and overshadowed by the more recognized enhancement to plant safety and availability from the use of digital technology. Appropriate defensive measures and the evaluations necessary to apply them are discussed in this document.

3.3 Digital Systems and Functions for which CCF is a Safety and Licensing Concern

CCF is a safety and licensing concern for any digital equipment that has the potential to affect components, systems, or functions described in the FSAR, regardless of the equipment safety classification, if:

1. The component, system or function is credited for AOO and PA mitigation, or
2. The component system or function is credited to not complicate that mitigation, or
3. The component, system or function can initiate a plant transient

Item 1 above includes support systems whose function is required for the operation of a component, system or function that is directly credited in an FSAR safety analysis. For example, support systems would include cooling water and heating, ventilating and air conditioning support systems.

3.4 Digital CCF Affects the Plant's Licensing Basis and Design Basis

If no P measures are included in the design to address the applicable CCF sources, a digital CCF is credible. Therefore, the potential CCF is within the plant licensing basis. P measures that can be credited to reach a conclusion that a CCF is not credible are described in Appendix A. The use of other defensive measures is described in Section 4.1.1.

A credible digital CCF is considered to be either within the design basis or beyond design basis, depending on the likelihood of the CCF. For example:

- A credible CCF caused by the random failure of a single shared hardware resource (e.g., erroneous operation of a redundant or non-redundant controller that controls multiple plant components) is within the design basis, because single random hardware failures are expected during the life of the plant.
- On the other hand, a credible CCF caused by some other failure sources (e.g., a design defect) can be considered beyond design basis (and analyzed accordingly) if certain defensive measures are employed to:
    1. Significantly reduce the likelihood of the I&C failure source (e.g., a structured design process), and
    2. Significantly reduce the likelihood of a CCF caused by that I&C failure source (e.g., independence or segmentation of control functions).

  These defensive measures are referred to as LR measures.

4 CCF ANALYSES

For the systems and components that need to be considered, as defined in Section 3.3, a CCF susceptibility analysis is provided. If that analysis concludes that a CCF is credible, an analysis of the CCF malfunction result is provided. Both analyses are described in the sections that follow. [Note: Additional detail will be added to the sections below as the need for additional detail is identified through NRC and industry review.]

4.1 CCF SUSCEPTIBILITY ANALYSIS

A CCF Susceptibility Analysis is performed for each I&C system or component that can affect a design function described in the FSAR. The digital engineer systematically assesses each failure source to:

1. Determine the applicability of the failure source, and
2. Determine if a CCF from each applicable source is credible, or not.

4.1.1 Process and Conclusions

Some failure sources may not be applicable while other sources are applicable. To ensure a complete analysis, the basis for a CCF source being not applicable is briefly described in the CCF susceptibility analysis documentation. Similarly, the digital engineer identifies any other potential sources of CCF that may be unique to a specific application.

For each applicable CCF source, the digital engineer confirms the applicability of at least one P measure, L measure, or LR measure from Appendix A. If an alternate P, L, or LR measure is credited, other than one of the complete measures provided in Appendix A, the digital engineer is responsible for providing documented justification for each alternate measure. A P, L or LR measure that is applied without including all of the elements in the set of defensive measures that constitute that P, L or LR measure, as defined in Appendix A (e.g., a partial P measure), is also considered an alternate measure, which requires documented justification.

If a defensive measure is added to a digital system to address a CCF source, either a measure from Appendix A or an alternate measure, the digital engineer is responsible to ensure the defensive measure is appropriate for the specific application (e.g., does not adversely affect equipment availability).

It is important to emphasize that the assessment of CCF sources and defensive measures is not a check list, but rather a comprehensive systematic assessment of the digital design. As an alternative, the digital engineer may elect to forgo this part of the CCF susceptibility analysis and simply assume that a CCF is credible.

A CCF that is not credible requires no further assessment in order to obtain or maintain a facility license. Of course, further analysis of the CCF may be appropriate in the plant probabilistic risk assessment (PRA); the PRA is outside the scope of this document.

For a credible CCF, the subsequent system level or component level malfunction(s) is identified; these are the effects on the plant equipment controlled, either manually or automatically, by the digital I&C equipment. The FSAR is then reviewed to determine if that malfunction is different than the system level or component level malfunction(s) included in a previous deterministic analysis. For example, if the CCF causes a subsequent loss of all main feedwater, and the loss of all main feedwater is already analyzed, and the CCF does not affect other systems or components whose malfunction is not described (e.g., the auxiliary feedwater system, which is credited for mitigation of this event), then there is not a different CCF malfunction result. For an operating plant, this facilitates a "no" answer to 10 CFR 50.59 Question 6. For a new plant, this precludes the need to add an additional analysis to the FSAR. If the FSAR identifies a system level malfunction, with or without a description of component level malfunctions that can lead to this system level malfunction, only the system level malfunction is pertinent to this CCF malfunction assessment.

A credible CCF for which the subsequent system level or component level malfunction is different than the malfunction(s) included in a previous deterministic FSAR analysis, requires further analysis to determine if the plant level CCF malfunction end result is bounded by previous deterministic analysis (see Section 4.2). This plant level analysis uses analytical methods (and related acceptance criteria) commensurate with the CCF likelihood. Therefore, if a CCF is credible and the subsequent malfunction is different at the system or component level, the digital engineer assesses the likelihood of the CCF based on available defensive measures, to determine the appropriate method and acceptance criteria for the analysis of the plant level CCF malfunction result, which follows (see Section 4.2). This plant level analysis of the CCF malfunction result is typically conducted by others (e.g., a transient analyst), not the digital engineer.

4.1.2 CCF Sources and Defensive Measures

4.1.2.1 CCF Sources

Potential CCF sources addressed in this document and to be addressed in the CCF susceptibility analysis, are:

1. A shared hardware resource (e.g., power supply, sensor, controller, data communication interface, workstation)
2. A common environment (e.g., temperature and humidity, seismic, electromagnetic interference)
3. A common design (e.g., design requirements, platform hardware, platform software, application software and configuration, data communication)

A common design would apply to any digital device, including a component with an embedded digital device, such as a power supply, a protective relay or a chiller controller.

Fire and human performance errors are also a source of CCF, but they are addressed through other industry documents. Therefore, fire and human performance errors are not included in this digital I&C CCF susceptibility analysis.

4.1.2.2 CCF Defensive Measures

This section describes the three types of defensive measures (P, L and LR) that can be credited in a CCF susceptibility analysis. P, L and LR measures are described in Sections 4.1.2.2.1 through 4.1.2.2.3.

Section 4.1.2.2.4 describes the graded approach applied in the definition of these defensive measures. This includes a distinction in the sources of CCF that are already dealt with by other processes, such as equipment qualification for safety systems to address environmental hazards.

The actual P, L and LR measures for each CCF source are described in Appendix A. Examples of digital systems that employ these defensive measures are provided in Appendix B, which is only an informative part of this NEI 16-16 guidance.

4.1.2.2.1 Preventive Measures

A P measure is a set of defensive measures that when applied as a set, provide reasonable assurance that a CCF from a specific I&C failure source is not credible. This method does not guarantee 100% CCF prevention assurance, because 100% assurance cannot be achieved, nor is it necessary or required.

When a CCF from a specific failure source is not credible, it means that the likelihood of a CCF from that failure source is as low as other failure sources that are not considered in deterministic safety analysis. For example, a CCF due to a seismic event or electromagnetic interference hazard that exceed the equipment qualification envelopes, or a human error that installs an incorrect setpoint, are all potential sources of CCF that are not considered in deterministic safety analysis.

A CCF not credible conclusion precludes the need for further deterministic analysis of the CCF malfunction result (i.e., “no further consideration of CCF”, as stated in NRC BTP 7-19). Of course, further analysis of the CCF may be appropriate in the plant probabilistic risk assessment (PRA); the PRA is outside the scope of this document.

Appendix A describes the specific P measures that can be credited for each applicable failure source.

4.1.2.2.2 Limiting Measures

In the absence of the specific defensive measures that constitute a P measure (i.e., when a CCF is credible for any given applicable failure source), the designer may elect to design the I&C system so that the resulting effect of an I&C failure on the controlled components, systems or functions is limited.

An L measure limits the number of controlled components, systems or functions that are affected; it forces a preferred malfunction state; or it forces a combination of both limits and states. An L measure may limit the CCF to a system or component level malfunction that is included in a previous deterministic FSAR analysis, or the L measure may simplify the plant level analysis of the CCF malfunction result. An L measure would not preclude the need for assessing the CCF malfunction result through deterministic analysis, as would application of a P measure.

Appendix A describes the specific L measures that can be credited for each applicable failure source.

4.1.2.2.3 Likelihood Reduction Measures

In the absence of the specific defensive measures that constitute a P measure (i.e., when a CCF is credible for any given applicable failure source), the designer may elect to design the I&C system so that the likelihood of a CCF is significantly reduced, when compared to a CCF due to a single random failure. For example, for a design defect:

1. A structured design process is applied, thereby supporting a much lower expectation of a design defect than the expectation of a random hardware failure, and

2. There is sufficient independence or segmentation to prevent a failure caused by the design defect from propagating to multiple plant components or functions, or occurring concurrently in multiple independent digital devices

An LR measure allows the CCF to be considered beyond design basis, and thereby allows the use of best estimate analysis methods and acceptance criteria for the analysis of the CCF malfunction result. Best estimate methods are less conservative than design basis methods; therefore, they are appropriate for assuring plant safety for a CCF whose likelihood is significantly less than the failures for which design basis methods are applied. While best estimate methods may be less conservative than design basis methods, they still require thorough documentation to support their conclusions.

Appendix A describes the specific LR measures that can be credited for each applicable failure source.

4.1.2.2.4 Graded Approach to Defensive Measures

The designs and design processes for safety systems have historically required more conservative attributes and design methods than for non-safety systems. This precedence is applied within this methodology in the definition of P, L and LR measures, and thus provides a graded approach based only on safety classification. Two examples of this graded approach follow:

1. CCF due to failure of a shared hardware resource

   Prevention of CCF of multiple safety divisions caused by a single shared hardware resource requires compliance to the Single Failure Criterion, including consideration of active and passive failures, and the application of independence criteria for electrical faults.

   Prevention of CCF of multiple non-safety components caused by a single shared hardware resource requires consideration of only active component failures.

2. CCF due to an environmental hazard

> Prevention of CCF of multiple safety divisions caused by an environmental hazard requires formal equipment qualification in accordance with industry standards.
>
> Prevention of CCF of multiple non-safety components caused by an environmental hazard requires environmental specifications and demonstration of compliance by factory environmental tests.

Another way of looking at this graded approach is that the P measures for non-safety systems, described in the examples above, are less onerous than for safety systems, due to the likelihood threshold of “as low as other failure sources that are not considered in deterministic safety analysis”, as described in Section 4.1.2.2.1, above. For Example 1 above, passive failures and electrical faults are not considered in deterministic safety analysis for non-safety systems.

However, although less onerous P measures are applicable to non-safety systems, an assessment of these P measures may require additional effort. For example, additional assessment of a safety system’s environmental durability would not be required for the CCF susceptibility analysis, since equipment qualification for safety systems is dealt with by other processes. But environmental durability for a non-safety system may require additional assessment that had not been previously considered.

This graded approach to defensive measures does not employ risk insights, because regulators have not permitted risk insights to be credited when addressing deterministic licensing criteria. Should this policy change for the short term, risk insights will be added to this document. Otherwise NEI will continue to pursue inclusion of risk insights for longer term efforts.

4.2 ANALYSIS OF CCF MALFUNCTION RESULT

An analysis of the CCF malfunction result determines if the plant level end result of the malfunction is bounded by a previous deterministic analysis in the FSAR. For an operating plant, a bounded end result facilitates a “no” answer to 10 CFR 50.59 Question 6, in accordance with Section 4.3.6, bullet 2 of NEI 96-07. For a new plant, a bounded result precludes the need to add an additional analysis to the FSAR.

If the plant level end result of the malfunction is not bounded by a previous deterministic analysis described in the FSAR, an additional deterministic plant level analysis is needed for the new CCF malfunction result. For an operating plant, this additional analysis requires an LAR for NRC approval. For a new plant, this additional analysis is included in the FSAR, either as a revision to a current analysis or a new analysis.

When demonstrating bounding, or in conducting a new analysis for an LAR, the method of coping with the CCF is documented and justified. This may include credit for automated or manual actions that are not adversely impacted by the same CCF source.

4.2.1 Bounded Criteria

The plant level end result due to a CCF malfunction is considered bounded if all the following criteria are met:

1. If the same type of transient or accident is already included in the deterministic safety analyses of the FSAR (e.g., excess feedwater event),
2. If only systems previously described in the FSAR are credited for mitigation, and
3. If there is no more than a minimal reduction in margin to the critical safety limit(s) in the applicable transient or accident from Item 1, above (e.g., departure from nucleate boiling ratio or containment pressure).

For a CCF in a support system whose function is required for the operation of a component, system or function that is directly credited in an FSAR safety analysis, the plant level end result is considered bounded if those directly credited systems are still capable of performing their credited safety function.

Bounded is demonstrated using the analytical methods and acceptance criteria described in Section 4.2.2. These methods are dependent on (1) the design basis or beyond design basis categorization of the CCF, and (2) whether the target digital equipment is a mitigator or initiator.

4.2.2 Analysis Method, Acceptance Criteria and Plant Conditions

The method and acceptance criteria for the analysis of the CCF malfunction result depend on the likelihood of the CCF source, as identified in the CCF susceptibility analysis, see Section 4.1. The likelihood effect on the analysis of the CCF malfunction result is described in Section 4.2.2.1.

The plant conditions for which the CCF is analyzed depend on the type of system affected by the CCF (i.e., an initiator or mitigator, as described in Section 4.2.2.2). The way the type of system affects the analysis of the CCF malfunction result is described in Section 4.2.2.2.

4.2.2.1 Likelihood Effect on Analysis Method and Acceptance Criteria

CCFs that are within the design basis require more conservative analysis methods and acceptance criteria than CCFs that are beyond design basis.

4.2.2.1.1 Design Basis CCFs

If a credible CCF is in the design basis, the following analysis methods and acceptance criteria are applied:

- Design basis methods and acceptance criteria, as currently used in the AOOs and PAs of the FSAR. This is typically a quantitative analysis using computer codes.
- Mitigating systems (also referred to as systems used to cope with the CCF) must be safety related

- Bounding (i.e., answer to 10 CFR 50.59 Question 6) is based on previously analyzed AOOs. The analysis cannot use PA acceptance criteria, because a design basis CCF is an AOO.

4.2.2.1.2 Beyond Design Basis CCFs

If a credible CCF is beyond design basis, the following analysis methods and acceptance criteria are applied:

- Design basis or best estimate methods. Best estimate methods can employ realistic and nominal initial plant conditions and equipment performance, relaxed acceptance criteria, no other assumed equipment failures, credit for beneficial control system action, and allow conclusions based on qualitative expert judgment or quantitative analysis.
- Mitigating systems (also referred to as systems used to cope with the CCF) can be safety related, or non-safety related with suitable attributes.
- Bounding (i.e., answer to 10 CFR 50.59 Question 6) is based on previously analyzed AOOs or PAs.
- If not bounded, analysis uses AOO or PA acceptance criteria, or the following acceptance criteria:
    - coolable core geometry,
    - containment integrity, and
    - releases do not exceed 100% of 10 CFR Part 100 limits

The thermal hydraulic analyses performed as part of the PRA may provide useful input to the deterministic analysis of beyond design basis CCFs.

4.2.2.2 System Effect on Plant Conditions to be Analyzed

CCFs in systems credited to mitigate plant events are analyzed with different concurrent plant conditions than CCFs in systems that can initiate a plant transient, because a CCF in a mitigating system can remain hidden.

4.2.2.2.1 Event Initiators

CCFs in systems that initiate plant transients (e.g., malfunctions due to a control system CCF) are analyzed with no other coincident event (e.g., no other AOO or PA) and no other CCF (e.g., no unrelated CCF in a safety system).

The basis is that these CCFs are typically self-announcing due to the resulting plant transient, alarms or component state changes; therefore, they can be mitigated prior to any other plant event. Put another way, if a control system CCF is self-announcing, then there is no need to consider a control system CCF coincident with each AOO or PA or another CCF, because the CCF would be detected and corrected before an unrelated AOO, PA, or digital CCF would occur.

There is the potential for a CCF in an event initiator that may result in a fail as-is condition with no alarms, which is not immediately self-announcing. For example, this could occur in steam or feedwater bypass valves that are normally not repositioned during stable plant operation. Even though this CCF is not immediately self-announcing, this CCF would be revealed when there is a change in plant power or operating mode. Although this CCF could coexist at the time of an AOO or PA, these systems are not credited for event mitigation and a fail as-is condition would not complicate that mitigation.

4.2.2.2.2 Event Mitigators

CCFs in systems that are credited for event mitigation (e.g., malfunctions due to a safety system CCF) are analyzed coincident with each AOO and PA. The basis is that these CCFs are not self-announcing; therefore, they can remain hidden and coexist at the time of an unrelated AOO or PA.

However, a beyond design basis CCF is not analyzed coincident with each AOO and PA, and with a concurrent loss of offsite power (LOOP). The basis is that since all current US plants have two independent grid connections, a LOOP is a CCF, and the low likelihood of two unrelated CCFs, including one that is beyond design basis (i.e., not expected during the life of the plant), does not require further consideration. However, a LOOP by itself is an AOO, therefore a LOOP alone with concurrent beyond design basis digital CCF is analyzed. This non-concurrent LOOP analysis position does not apply to a design basis CCF, because a design basis CCF would be expected during the life of the plant.

Similarly, a beyond design basis digital CCF is not analyzed coincident with an SBO, because an SBO is a beyond design basis CCF, and the low likelihood of two unrelated CCFs, including both that are beyond design basis (i.e., not expected during the life of the plant), does not require further consideration.

5 REFERENCES

To be developed.

APPENDIX A: DEFENSIVE MEASURES

To be developed.

APPENDIX B: EXAMPLES

To be developed.

[BLANK PAGE]