NEI 16-16 [Draft 2]

Guidance for Addressing Digital Common Cause Failure

May 2017

[BLANK PAGE]

NEI 16-16 [Draft 2]

Nuclear Energy Institute

Guidance for Addressing Digital Common Cause Failure

May 2017

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

NOTICE

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 guideline 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 cause a CCF and (2) methods for analysis of the plant-level CCF malfunction result should a digital CCF be determined to be credible. For this guideline, a "digital CCF" means a CCF using the definition provided in Section 2, but limited to CCFs caused by a failure in a digital I&C source. Other CCFs, such as those that may occur among process, mechanical, or electrical systems and components, are not addressed in this guideline.

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 of potential I&C failure sources that can cause a CCF and the built-in defensive measures that may be available 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 in the FSAR, the likelihood of the CCF is determined. The conclusions of the CCF susceptibility analysis provide input to the plant-level analysis of the CCF malfunction result.

For this guideline, the term "FSAR" can refer to the Updated Final Safety Analysis Report (UFSAR) for an operating plant licensed under 10 CFR 50, or the Tier 2 portion of the Design Control Document (DCD) for a new plant licensed under 10 CFR 52.

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 described in the FSAR, or if another deterministic plant-level analysis needs to be conducted and added to the FSAR to demonstrate plant safety.

The conclusions of the CCF susceptibility analysis and the analysis of the CCF malfunction result provide input to the licensing process.

This document was developed by 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

1 INTRODUCTION 1
1.1 Overview 1
1.2 Summary of CCF Technical Evaluation Process 1
2 DEFINITIONS 5
3 BACKGROUND 8
3.1 Potential Safety and Licensing Issue with CCF 8
3.2 Potential Challenges Presented by Digital Design 8
3.3 Potential Benefits Presented by Digital Design 9
3.4 A Credible CCF Affects the Plant's Licensing Basis and Design Basis ... 9
4 CCF TECHNICAL EVALUATION 11
4.1 Part 1: Determine if the Digital System is an Initiator or a Mitigator 11
4.2 Part 2: CCF Susceptibility Analysis 12
4.2.1 Overview of CCF Susceptibility Analysis Method and Conclusions 12
4.2.2 Assess I&C Failure Sources and Available Defensive Measures 15
4.3 Part 3: Analysis of CCF Malfunction Result 22
4.3.1 Determine the Analysis Methods and Acceptance Criteria ... 23
4.3.2 Determine Plant Condition Assumptions 24
4.3.3 Bounded Criteria 25
5 REFERENCES 27
APPENDIX A: PREVENTIVE AND LIMITING MEASURES 28
APPENDIX B: LIKELIHOOD REDUCTION MEASURES 122
APPENDIX C: CCF SUSCEPTIBILITY ANALYSIS WORKSHEET 126
APPENDIX D: EXAMPLES 129

[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 replace obsolete analog and early digital components with modern technology, and take advantage of the benefits that digital technology can provide in improved component and system reliability, resulting in gains in plant safety, availability, and maintainability. 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 provide a more efficient and consistent outcome in licensing digital I&C projects in operating plants and new plants.

This guideline is applicable to facility changes done under 10 CFR 50.59 and facility changes that require a license amendment.

The current NRC policy on digital system CCF is based on Staff Requirements Memorandum (SRM) to SECY-93-087. The staff interpreted this policy via NRC Branch Technical Position (BTP) 7-19, which states 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 is practical for most applications necessitating the demonstration of coping with a CCF for which there is insufficient industry guidance.

This guideline provides 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 guidance 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 NRC policies and positions such as SRM-SECY-93-087 and BTP 7-19.

1.2 SUMMARY OF CCF TECHNICAL EVALUATION PROCESS

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 technical evaluation is documented. The documentation is maintained as a quality record. The CCF technical evaluation has three parts:

1. Part 1 determines if a CCF in the target digital equipment is a safety analysis or licensing concern; if not the analysis is complete. CCF is a concern for digital systems or components that can perform or affect design functions described in the FSAR. Such digital systems or components would be credited in the FSAR for abnormal event mitigation or for digital systems or components that can initiate transients described in the FSAR. The basis for this concern is described in Section 3. Guidance for determining if it is a concern is provided in Section 4.1. 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 a plant condition that is not previously analyzed and described in the FSAR.

2. Part 2 is referred to as the CCF susceptibility analysis; the detail is described in Section 4.2. For digital equipment of concern from Part 1, a design 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 design engineer determines the following:
    a. Whether a potential CCF is credible; if not, the analysis is complete. The term "CCF not credible" is defined in Section 2.
    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 described in the FSAR; if so the analysis is complete.
    c. If the subsequent system or component-level 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 design 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 4.3. 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 described in 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. Section 4.3.1 distinguishes the analysis methods, acceptance criteria and acceptable coping methods for design basis versus beyond design basis CCFs, as discussed above. In addition, Section 4.3.2 describes analysis differences for systems that are credited to mitigate abnormal events and systems that can be transient initiators.

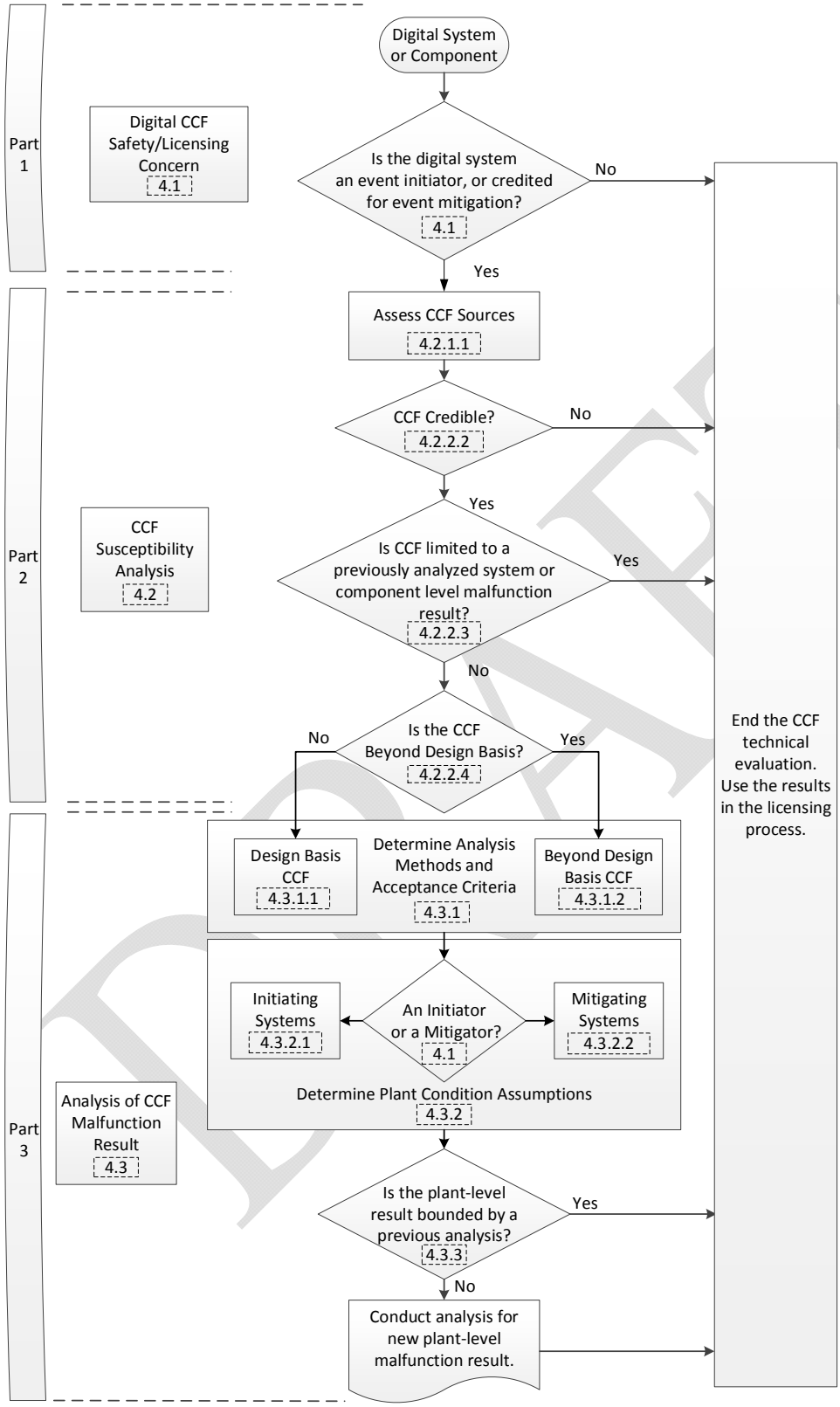


Figure 1 – CCF Technical Evaluation Process

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 as well as credit for operator actions not described in the FSAR, 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 and when conducting a new 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 the FSAR.

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 caused by a single random hardware failure. For this guideline, a CCF beyond the 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

A CCF can be considered not credible only if 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 a deterministic safety analysis described in the FSAR. A CCF not credible conclusion means no further technical evaluation is necessary, since reasonable assurance exists that the CCF is sufficiently unlikely. Otherwise, a deterministic analysis of the CCF malfunction result is necessary. Note that 'not credible' does not mean not possible and that it still may be appropriate to consider the CCF outside the licensing basis, such as in the PRA (which is outside the scope of this guideline).

2.6 COPING

For a credible CCF, coping refers to (1) the event mitigation methods (e.g., a mitigating system) credited to demonstrate that the CCF malfunction result is bounded by a previous deterministic analysis described in the FSAR, 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 within the target digital equipment to prevent, limit or reduce the likelihood of a CCF. Design or design process attributes can be assembled together to establish a preventive, limiting, or likelihood reduction measure. 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 DESIGN ENGINEER

Design engineer is used only to distinguish the analysis activities typically conducted by an I&C engineer skilled in digital design practices and analyses, from other analysis activities (such as safety analysis or PRA) conducted by others.

2.9 DETERMINISTIC ANALYSIS

A characteristic of decision-making in which results from engineering analyses, not involving probabilistic considerations, are used to support a decision.

2.10 LIMITING MEASURE

A limiting 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 measure is a set of defensive measures that when applied as a set reduce the likelihood of a credible CCF.

2.12 MITIGATING SYSTEM

A plant system designed to minimize the effects of initiating events. Front-line systems are mitigating systems that directly perform an accident mitigating function. Typically, support systems (e.g., electric power, control power, or cooling) are required to enable the operation of systems that directly perform an accident mitigating function. In this regard, support systems also may be considered mitigating systems.

2.13 PREVENTIVE MEASURE

A preventive 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 AND LICENSING ISSUE WITH CCF

Plant safety is assured for events that have been considered in the deterministic analyses within the facility 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 the potential for increased complexity, combining of functions and potential new misbehaviors of digital I&C may result in the need to consider the effects of malfunctions caused by the I&C that may not have been a part of the original plant licensing basis

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.

Except for the CCFs that lead to Anticipated Transient Without Scram (ATWS) and Station Blackout (SBO), the Anticipated Operational Occurrences (AOO) and Postulated Accidents (PA) described in the FSAR are analyzed with a concurrent single 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 an unanalyzed plant transient (i.e., a new AOO).

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 potential for a common cause failure (CCF), and the potential for

consequences, that may be greater than their analog predecessors. A CCF can pose a potential safety hazard that may not be well understood or is overlooked when designers focus primarily on taking advantage of the enhancements to plant safety and availability afforded by 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 guide.

3.3 Potential Benefits Presented by Digital Design

Compared to their analog counterparts, properly designed digital systems are generally more robust and more capable of preventing malfunctions of multiple controlled SSCs using redundancy, logic, and other design attributes that are described in this guide as preventive measures. For example, digital technology can be used to remove single point vulnerabilities that may be found in analog systems where a single random hardware failure would have caused an SSC malfunction that can now be prevented by a proper digital system design.

In addition, digital technology can be provided with the ability to select a preferred malfunction state on the controlled SSCs in the event of an I&C failure, thus giving the designer some alternatives that can improve the plant design. This advanced capability is found among some of the design attributes described in this guide as limiting measures.

3.4 A Credible CCF Affects the Plant's Licensing Basis and Design Basis

If no preventive measures are included in the I&C design to address the applicable CCF sources, a CCF is considered credible, and a credible CCF is within the plant licensing basis. Preventive measures that can be credited to reach a conclusion that a CCF is not credible are provided in Appendix A. A credible CCF can also be limited in terms of the number of affected SSCs (e.g., controlled components) or the resulting SSC states; accordingly, limiting measures are also provided in Appendix A.

A credible CCF is 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 can result in AOOs, which 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 at its source (e.g., a structured design process to assure high quality software; see Section 4.2.2.4 and Appendix B for details), 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 likelihood reduction measures.

4 CCF TECHNICAL EVALUATION

This section provides detailed guidance for all three parts of the CCF technical evaluation process. Note that criteria are provided for stopping the CCF technical evaluation at the end of each part, or proceeding to the next part. Subsequent parts depend on the results of prior parts. The design engineer should document the completed CCF technical evaluation, and preserve the document as a quality record. Future modifications should consider all previous CCF technical evaluations for systems that interface with or are affected by the future proposed modification.

4.1 PART 1: DETERMINE IF THE DIGITAL SYSTEM IS AN INITIATOR OR A MITIGATOR

As summarized in Section 1.2 and illustrated in Figure 1, the first part of the CCF technical evaluation process is to determine if the digital system has the potential to affect components, systems, or functions described in the FSAR, regardless of the equipment safety classification, using the following criteria:

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

Note that some components, systems or functions can be an initiator and a mitigator as described in the FSAR, but typically not in the same event scenario.

Item 2 above includes support systems whose function is required for the operation of a component, system or function that is directly credited in the FSAR.

> For example, support systems would include cooling water and heating, ventilating and air conditioning support systems that maintain the environment necessary for mitigating systems to function. Control room HVAC chillers fall into this category if they are credited in the FSAR for maintaining the environment necessary for mitigating systems such as (but not limited to) Post Accident Monitoring, RPS, or ESFAS equipment.

Item 3 above includes components, systems or functions that are assumed to perform a function or remain in an assumed state coincident with a mitigating system function.

> For example, the FSAR may credit a reactor trip via the RPS (a mitigating system) that occurs in response to an initiating event, and also credit the main feedwater control system to automatically reduce main feedwater flow to a value commensurate with decay heat load. If the main feedwater control system fails in a manner that causes main feedwater flow to stop, then the reactor trip is made complicated because the emergency feedwater system is required to respond.

Another example of Item 3, above, is an event described in the FSAR that assumes (or credits) the steam dump valves to remain closed. If the steam dump valves open during that event due to an I&C failure source, the event becomes complicated.

If the digital component, system or function meets any of the three conditions listed above, then proceed to Section 4.2. Otherwise, the CCF technical evaluation ends here. Document the results in either case.

4.2 PART 2: 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. Section 4.2.1 provides an overview of the CCF susceptibility analysis and conclusions that can be reached. Section 4.2.2 provides guidance on how to perform the CCF susceptibility analysis.

Note that the CCF susceptibility analysis can make use of a wide range of potentially applicable preventive or limiting measures provided in Appendix A, which is quite lengthy. A summary listing of the preventive and limiting measures is provided in an attachment to the PDF file for this guide, formatted as an ANSI Size D "poster" that can be printed on a large format printer and used as an aid. Note that the summary listing is just that; only the subject line of each preventive and limiting measure is provided. Users are cautioned to not consider the subject line of any given measure as the whole measure. The details of each measure in Appendix A must be carefully considered. Preventive and limiting measures are identified by their table and "P" or "L" number in Appendix A. For example, "A2-P1" identifies the first preventive measure provided in Table A-2 in Appendix A.

4.2.1 Overview of CCF Susceptibility Analysis Method and Conclusions

This section provides an overview of the CCF susceptibility analysis method and the conclusions that may be reached by the design engineer. Detailed guidance on each step of the method is provided in Section 4.2.2.

The CCF susceptibility analysis method first determines if any of the I&C failure sources described in Section 4.2.2.1 and listed in Appendix A are applicable in the I&C system or component design undergoing the analysis. Some I&C failure sources may not be applicable because the potential failure source does not exist in the proposed I&C design (data communications, for example). To ensure a complete analysis, the basis for an I&C failure source being not applicable is provided in the CCF susceptibility analysis documentation. Similarly, the design engineer identifies any other potential sources of CCF not listed in Appendix A that may be unique to a specific application.

For each applicable I&C failure source, the design engineer then determines the applicability of at least one preventive measure, limiting measure, or likelihood reduction measure from Appendices A and B of this guide. The full description of preventive, limiting, and likelihood reduction measures for each I&C failure source are provided in Appendices A and B. Examples of CCF susceptibility analyses that credit

these defensive measures are provided in Appendix D, which is only an informative part of this guidance.

If an alternate preventive, limiting or likelihood reduction measure is credited, other than one of the complete measures provided in Appendices A and B, the design engineer is responsible for providing documented justification for such a measure.

A specific preventive, limiting or likelihood reduction measure that is applied without including all the elements provided in Appendices A or B for that specific measure is considered an alternate measure, which requires documented justification.

> For example, preventive measure A2-P6 calls for one shared UPS for all controllers to prevent a CCF of multiple controlled SSCs in the event of an upstream power failure, which is a typical design for many digital I&C systems. However, A2-P6 also calls for an analysis and test of controller performance to demonstrate that the controllers can tolerate the worst-case noise and voltage fluctuations from the UPS. If the analysis and test is not performed, then A2-P6 is not met, but if the design engineer can provide a UPS and also provide an alternate method of demonstrating adequate controller performance, then it is an alternate preventive measure altogether that may be credited as long as documented justification is provided.

If a specific preventive, limiting or likelihood reduction measure is added to or identified within a proposed digital system to address an I&C failure source, the design engineer is responsible for ensuring that measure is appropriate for the specific application.

> For example, the generic limiting measure that limits the number of SSCs that can be affected by a single random hardware failure in a controller can be met in a control system that limits the number of control valves connected to that controller, such as the main turbine governor valves and the main turbine bypass valves. However, in this example the FSAR does not consider a CCF of all turbine control valves and all turbine bypass valves at the same time. The design engineer then has a choice between providing segmentation between the existing controller and an additional controller so the governor valves and bypass valves are on separate controllers, or asking for an additional safety analysis of a CCF of the governor valves concurrent with a CCF of the bypass valves to determine if the malfunction results are acceptable. Without an additional control segment or additional analysis, the generic limiting measure is not appropriate by itself.

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

> For example, a proposed digital I&C system design will provide control of all main turbine control valves, and nothing else, and a CCF of all main turbine control valves is described already in a previous analysis in the FSAR. In this case, it may be expedient for the design engineer to simply assume a CCF of all main turbine control valves is credible because it is already analyzed.

A CCF that is not credible requires no further assessment to obtain or maintain a facility license.

For a credible CCF, the subsequent system level or component level malfunction(s) is identified; these are the effects on the controlled SSCs (such as pumps, valves, control rods, breakers, etc.), either manually or automatically, caused by the I&C failure source. The FSAR is then reviewed to determine if the result of that malfunction is different than the system level or component level malfunction results included in a previous deterministic analysis.

> For example, if an I&C failure source can cause all the feedwater regulating valves to close and closure of all the feedwater regulating valves is already analyzed, then there is not a different CCF malfunction result (as long as the I&C failure does not also affect other systems or components, such as the auxiliary feedwater system, which is credited for mitigation of this event).

If the FSAR identifies a malfunction result at the plant system level, with or without a description of component level malfunctions that can lead to this plant system level malfunction result, only the plant system level malfunction result is pertinent to the CCF malfunction assessment.

Further analysis is required for a credible CCF when the subsequent system level malfunction result or component level malfunction result is different than the malfunction result(s) included in a previous deterministic analysis described in the FSAR, to determine if the plant-level end result is bounded by the previous deterministic analysis (see Section 4.3).

> For example, the FSAR for a three-loop pressurized water reactor describes an excess heat removal event that can be caused by excess feedwater flow to one of the three steam generators. The analysis states the plant-level end result for excess feedwater flow to one steam generator is a departure from nucleate boiling ratio (DNBR) of 1.3. A proposed digital feedwater control system design provides one controller for regulating feedwater flow to all three steam generators via the feedwater regulating valves, and does not have adequate preventive measures to make a CCF of all feedwater regulating valves non-credible. This proposed design can therefore cause a different feedwater system malfunction result because an I&C failure can cause excess flow to all three steam generators instead of one steam generator. Further analysis is required to determine if the plant-level end result is bounded by the

previous end result. If further analysis shows that DNBR is no lower than 1.3, then the new malfunction result is bounded at the plant-level as described in the FSAR.

The 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 result is different at the system or component level, the design engineer assesses the likelihood of the CCF based on available likelihood reduction measures to determine the appropriate method and acceptance criteria for the analysis of the plant-level CCF malfunction result, which follows, using the guidance in Section 4.3. This plant-level analysis of the CCF malfunction result is typically conducted by others (such as a safety analyst), not the design engineer.

4.2.2 Assess I&C Failure Sources and Available Defensive Measures

Potential I&C failure sources are described in Appendix A of this guide. The design engineer assesses each I&C failure source systematically to:

1. Determine the applicability of the failure source in the proposed I&C system or component design, and
2. Determine if a CCF from each applicable source is credible or not, and
3. Determine if each credible CCF is limited or not, and
4. Determine if the likelihood of each credible CCF is reduced or not, and
5. Determine the malfunctions that result from each credible CCF.

A suggested CCF susceptibility analysis worksheet template and instructions are provided in Appendix C.

4.2.2.1 Determine Applicability of I&C Failure Sources

The following potential I&C failure sources are described in Appendix A of this guide. Determine which of the following I&C failure sources are provided within the proposed digital I&C system or component design:

1. A shared I&C hardware resource (that is, a single I&C resource that multiple controlled SSCs depend upon for performing their design functions):
    i. Shared power supply
    ii. Shared sensor
    iii. Shared output module
    iv. Shared control signal
    v. Shared network or data link
    vi. Shared operator workstation
    vii. Shared engineering/maintenance workstation

viii. Shared controller

ix. Shared clock

2. An environmental disturbance that can affect one piece of I&C equipment shared by multiple controlled SSCs, or an environmental disturbance that can affect multiple pieces of I&C equipment that control multiple SSCs:
    i. High temperature or humidity
    ii. Electromagnetic interference
    iii. Seismic
    iv. Radiation
3. A common design in the I&C equipment (that is, an element that is identical in multiple pieces of I&C equipment):
    i. Operating system
    ii. Application software
    iii. Embedded Digital Device (EDD)
    iv. Requirements
    v. Data communications

Fire, smoke, and operations or maintenance human errors are also sources of CCF, but they are addressed through other industry guidance. Therefore, fire, smoke, and human error are not addressed in this guidance, although defensive measures for these issues are included in Appendix A for interested users.

If any of the I&C failure sources listed above are provided within the proposed I&C system or component design, then proceed to Section 4.2.2.2 for the applicable failure sources. If a proposed I&C system or component design has a failure source that is not on the list provided above, it should be identified and addressed using this guide. Document the results of the applicability determination using the worksheet and instructions provided in Appendix C. For the I&C failure sources that are not applicable, the CCF technical evaluation ends here.

4.2.2.2 Determine CCF Credibility via Applicable Preventive Measures

A preventive 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. A preventive measure does not guarantee absolute assurance that a CCF of multiple controlled SSCs will not happen. Absolute assurance cannot be achieved, nor is it necessary or required to obtain or maintain a facility license.

Using Appendix A of this guideline, determine which, if any, preventive measures are provided within the proposed I&C system or component design for the applicable I&C failure sources identified earlier (per Section 4.2.2.1). Document the results for each

applicable failure source using the worksheet and instructions provided in Appendix C. If an alternate preventive measure is devised as described in Section 4.2.1, then document the alternate measure and provide justification that the alternate measure is adequate to reach a CCF non-credible conclusion.

When a CCF from a specific failure source is not credible, it means that the likelihood of a CCF from that I&C failure source is no greater than that of other failure sources that are not considered in deterministic analyses described in the FSAR.

> For example, a CCF of multiple controlled SSCs caused by any of the following are not considered in the deterministic analyses described in an FSAR:
>
> - Multiple random hardware failures in the I&C equipment, or
> - A seismic event or electromagnetic interference hazard that exceeds the design basis qualification envelopes for the I&C equipment, or
> - A human error that installs an incorrect setpoint in more than one division of safety I&C equipment.

Document which preventive measures are applied for each applicable I&C failure source, and document the results using the worksheet and instructions provided in Appendix C. Note that it is necessary to determine the resulting states of controlled SSCs that are affected by each applicable I&C failure source.

If a preventive measure is available and applied within the proposed I&C system or component design for all applicable I&C failure sources, then a CCF of multiple controlled SSCs is not credible, and the CCF technical evaluation ends here. If a preventive measure is not available for one or more of the applicable I&C failure sources, then a CCF of multiple controlled SSCs is credible for those specific failure sources. Continue to Section 4.2.2.3 to determine if the resulting affects of those I&C failures on the controlled SSCs can be limited.

A CCF not credible conclusion precludes the need for further deterministic analysis of the CCF malfunction result (that is, "no further consideration of CCF", as stated in NRC BTP 7-19), to maintain or obtain a facility license.

4.2.2.3 Determine if a Credible CCF is Limited to a Previously Analyzed System or Component Level Malfunction Result via Applicable Limiting Measures

When a CCF is credible for any given applicable failure source, the design engineer may elect to design the I&C system so that the resulting effect of an I&C failure on the controlled SSCs is limited through the application of a limiting measure.

A limiting measure can limit the number of controlled components, systems or functions that are affected; it can force a preferred malfunction state; or it can force a combination of both. A limiting measure may limit the CCF to a system or component

level malfunction that is included in a previous analysis described in the FSAR, or the limiting measure may simplify the plant-level analysis of the CCF malfunction result.

A limiting measure does not support reaching a CCF not credible conclusion unlike the application of a preventive measure because preventive measures are formulated for driving the likelihood of a CCF to be no greater than other CCFs not considered in the FSAR, whereas limiting measures have no provision for reducing the likelihood. Therefore, limiting measures coincide with the need for further consideration of the CCF malfunction result.

Appendix A provides specific limiting measures that may be available within the proposed I&C system or component design, and therefore credited for each applicable I&C failure source.

> For example, to limit the effects of a single random hardware failure in a shared sensor, limiting measure A5-L1 provides two shared, redundant sensors, with dedicated signal validation for each sensor. The signal validation routine outputs the average of the process values originating from both physical sensors on the same process, when they are within their specified range and within deviation limits of each other. But when sensors deviate outside those limits, with only two sensors it is not possible to identify which sensor is correct. Therefore, the signal validation logic is designed to force the output to a predetermined state. The result is a CCF of all SSCs controlled by those shared sensors, but this predetermined state simplifies the analysis of the malfunction result.

Document which limiting measures are applied, if any, for each applicable I&C failure source, and document the results using the worksheet and instructions provided in Appendix C. Note that it is necessary to determine the resulting states of controlled SSCs that are affected by each applicable I&C failure source.

If the CCF is limited so that the states of the controlled SSCs result in a system or component level malfunction that is previously described and analyzed in the FSAR, then the CCF technical evaluation ends here because it is not a different malfunction result at the system or component level (and there is no need to determine bounding at the plant-level using the guidance in Section 4.3.3). Otherwise, proceed to Section 4.2.2.4 to determine if any CCF likelihood reduction measures are applicable.

4.2.2.4 Determine if a Credible CCF is Design Basis or Beyond Design Basis via Applicable Likelihood Reduction Measures

When a preventive measure for an applicable failure source is not available in the proposed I&C system or component design, then a CCF of multiple controlled SSCs is credible for that specific I&C failure source. However, the designer may elect to design

the I&C system so that the likelihood of a CCF is significantly less than the likelihood of a CCF caused by a single random hardware failure in the I&C.

> For example, to reduce the likelihood of a CCF caused by a design defect in the I&C to significantly less than the likelihood of a single random hardware failure in the I&C:
>
> 1. A structured design process is applied per Appendix B of this guideline, thereby supporting a much lower likelihood of a design defect than the likelihood 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 simultaneously in multiple independent digital devices.

A likelihood reduction measure allows a credible 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, but only for those failure sources that apply the likelihood reduction measure.

> For example, in a three-loop pressurized water reactor a failure of a single output module in a digital feedwater control system may affect one steam generator because the output modules are segmented in a manner such that a random failure of one output module only causes the main and bypass feedwater regulating valves on one steam generator to go fully open or fully closed. In this example, a CCF of both valves on one steam generator is credible because a preventive measure is not available for the output module, but the CCF malfunction result is limited to feedwater flow transients on one steam generator. Because the source of the CCF is a single failure in the I&C, it is considered within the design basis of the facility and therefore analyzed using conservative inputs, assumptions and acceptance criteria (i.e., as an anticipated operational occurrence).
>
> However, if a CCF of all feedwater regulating valves affecting all three loops due to a design defect activated in all three output modules is credible because the digital feedwater control system does not have adequate preventive measures for a design defect, and the likelihood reduction measures for a design defect are applied per Appendix B, then the malfunction result can be considered beyond design basis and analyzed using best estimate methods and acceptance criteria.

Best estimate methods are less conservative than design basis methods; therefore, they are appropriate for assuring plant safety only for a CCF whose likelihood is 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 B describes the specific likelihood reduction measures that can be credited for each applicable failure source. The analyst should document the results using the worksheet and instructions provided in Appendix C.

4.2.2.5 Graded Approach to Defensive Measures Based on Safety Classification

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 formulation of preventive, limiting and likelihood reduction measures, and thus provides a graded approach based on safety classification.

> For example, prevention of a 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. On the other hand, prevention of a CCF of multiple non-safety controlled SSCs caused by a single shared hardware resource requires consideration of only active component failures.
>
> In another example, prevention of CCF of multiple safety divisions caused by an environmental disturbance requires formal equipment qualification in accordance with rules (such as 10 CFR 50.49) and industry standards. Prevention of CCF of multiple non-safety components caused by an environmental hazard depends on environmental specifications and demonstration of compliance by factory environmental tests.

Another way of looking at this graded approach is that the preventive measures for non-safety systems, described in the examples above, are less onerous than for safety systems, because they are formulated such that a CCF is no more likely than other failure sources that are not considered in deterministic safety analysis described in the FSAR per Section 4.2.2.2 of this guideline (in other words, defense-in-depth is provided by safety systems that are designed with a higher quality process, equipment qualification, etc.). In the first example above, passive failures and electrical faults are not considered in deterministic safety analysis for non-safety systems (such as an electrical fault in a control system module that could propagate to other modules).

However, although less onerous preventive measures are applicable to non-safety systems, an *assessment* of these measures for a CCF technical evaluation may require more effort than applied in the past (although the level of effort to *apply* non-safety preventive measures during system design should be no different from normal plant practice).

> For example, assessment of a safety system's environmental durability is not necessary within the CCF susceptibility analysis itself, because equipment qualification for safety systems is provided by other technical evaluation processes. But environmental durability for a non-safety system

may require an assessment within the CCF susceptibility analysis method, such as a closer examination of commercial EMI certificates and related test reports provided by commercial vendors (this is not referring to equipment qualification per 10 CFR 50.49 because this example is about non-safety equipment), because other technical evaluation processes may not be adequate for demonstrating a CCF non-credible conclusion.

4.2.2.6 Use of Risk Insights

This guide does not address how to use quantitative PRA results when considering insights that could influence the design of digital I&C systems. However, for some I&C failure modes or effects, Appendix A provides some limited guidance on applying PRA risk insights.

For example, for examining the impact of a CCF caused by an erroneous command from a random failure of a shared operator workstation, Section A.4.1.6.3 of Appendix A provides guidance on use of an existing PRA model to identify potential combinations of SSC failure modes that may impact multiple trains or systems.

The PRA can be used at a system or functional level to identify combinations of failures that might be considered, or conversely, screened from further consideration in the design of a digital I&C system. In addition, a PRA model might be used to identify combinations of SSC failure modes that may only have impact when combined with additional independent random failures. The combination of a digital I&C system failure with failures of multiple independent components are not likely to be risk significant, as this is an indication that margin to loss of core cooling or containment release is provided using diverse equipment. Risk results that highlight a potential relationship between digital I&C systems and other mitigative systems could help identify combinations that result in unacceptable results, thereby influencing the design to limit the CCF potential.

The use of risk insights can serve as a valuable tool in that they may help to identify other SSCs or actions that may be credited for mitigation assuming the failure of an I&C system due to a CCF mechanism.

4.2.2.7 Completion of CCF Susceptibility Analysis

At this point in the CCF technical evaluation, the design engineer has completed the following tasks:

1. Determined the applicability of each I&C failure source in the proposed I&C system or component design using the guidance in Section 4.2.2.1.
2. For each applicable I&C failure source, determined whether or not a CCF of multiple controlled SSCs is credible (that is, whether or not a preventive measure is fully applied), using the guidance in Section 4.2.2.2.

3. For each credible CCF, determined whether or not the CCF malfunction result is limited to a specific set of SSCs and/or preferred SSC states (that is, whether or not a limiting measure is fully applied), using the guidance in Section 4.2.2.3.
4. For each credible CCF, determined if the CCF malfunction result can be analyzed using design basis inputs, assumptions and acceptance criteria, or beyond design basis inputs, assumptions and acceptance criteria (that is, whether or not a likelihood reduction measure is fully applied for each credible CCF) using the guidance in Section 4.2.2.4.

To complete the CCF susceptibility analysis, the design engineer should document the SSCs that are affected by each credible CCF, their resulting states, and if the analysis of each malfunction result should be performed using design basis methods or if it can be performed using beyond design basis methods.

A complete CCF susceptibility analysis worksheet (using the template provided in Appendix C) can inform the analysis of each resulting CCF (a malfunction of multiple controlled SSCs caused by an I&C failure) using the guidance in Section 4.3.

4.3 PART 3: 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 described in the FSAR. If the plant-level end result of the malfunction is not bounded by a previous deterministic analysis described in the FSAR, another deterministic plant-level analysis is needed for the new CCF malfunction result. This new deterministic plant-level analysis is performed using design basis or beyond design basis methods, depending on the results of Part 2 of the CCF technical evaluation (using the guidance in Section 4.2.2.4).

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

Use the guidance in Section 4.3.1 to determine the method and acceptance criteria for the analysis of the CCF malfunction result, which depends on the likelihood of the CCF.

Use the guidance in Section 4.3.2 to determine the plant conditions assumed for the analysis of the CCF malfunction result, which depends on the type of I&C system, an initiator or a mitigator that causes the CCF.

When the analysis of the CCF malfunction result is complete, use the guidance in Section 4.3.3 to determine if the CCF malfunction result is bounded by a previous analysis in the FSAR.

4.3.1 Determine the Analysis Methods and Acceptance Criteria

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

4.3.1.1 Design Basis CCF

In the absence of a fully applied likelihood reduction measure per Section 4.2.2.4, a credible CCF is in the design basis, and the following transient and accident analysis methods and acceptance criteria are applied:

- Design basis methods and acceptance criteria, as currently used in the AOOs and PAs described in the FSAR. This approach is typically a quantitative analysis using computer codes.
- Mitigating systems (also referred to as systems used to cope with the CCF) must be classified as safety related (note that this does not include systems credited for mitigating a beyond design basis CCF in a mitigating system concurrent with design basis AOOs and PAs, which is addressed in Section 4.3.1.2 below).
- For a CCF initiated by a random hardware failure in the I&C, bounding is based on previously analyzed AOOs. The analysis cannot use PA acceptance criteria, because a design basis CCF initiated by a random hardware failure in the I&C is an AOO.
- For a design basis CCF in a mitigating system concurrent with a PA, bounding is based on previously analyzed PAs.

4.3.1.2 Beyond Design Basis CCF

If a credible CCF is beyond design basis (that is, a likelihood reduction measure is fully applied using the guidance in Section 4.2.2.4), the following transient and accident 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. Operator action can be credited for mitigating a beyond design basis CCF if it can be detected and mitigated in time, with sufficient margin, to meet the acceptance criteria.
- Bounding is based on previously analyzed AOOs or PAs.

- If the plant-level CCF malfunction result is not bounded by a previous analysis, a new analysis can use design basis AOO or PA acceptance criteria, or the following acceptance criteria:
    - coolable core geometry,
    - reactor coolant pressure boundary integrity,
    - containment integrity, and
    - releases do not exceed 100% of 10 CFR Part 100 limits

The thermal hydraulic analyses performed as part of the PRA are acceptable in the deterministic analysis of beyond design basis CCFs.

4.3.2 Determine Plant Condition Assumptions

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. Use the results from the guidance in Section 4.1 to determine if the I&C system or component is an initiator or a mitigator.

4.3.2.1 Initiating Systems

CCFs in systems that initiate plant transient events, such as SSC malfunctions caused by an I&C failure in a control system, are analyzed with no other coincident event (such as another AOO or PA), and no other CCF (such as an unrelated CCF in a safety system).

The basis for no other coincident events or coincident CCF in other systems is that CCFs that result in an initiating event are typically self-announcing due to the resulting plant transient, alarms, or component state changes. If a control system CCF is self-announcing, then there is no need to consider this CCF coincident with each AOO or PA or another CCF in another system, because there is a high likelihood that the CCF would be detected and corrected before an unrelated AOO, PA, or CCF would occur in time.

However, there is still some 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, an I&C failure could cause a fail as-is condition in feedwater bypass valves that are normally closed at 100% power and not repositioned during stable plant operation. Even though this CCF malfunction result is not immediately self-announcing, it would be revealed when there is a change in plant power or operating mode. Although this CCF malfunction result could coexist at the time of an AOO or PA at 100% power, these particular valves are not credited for mitigating such events and a fail as-is condition should not complicate that mitigation, subject to evaluation.

4.3.2.2 Mitigating Systems

CCFs in I&C systems that are credited for event mitigation, such as malfunctions caused by a safety I&C system CCF, are analyzed coincident with each AOO and PA because these CCFs are typically not self-announcing. 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 a concurrent loss of offsite power (LOOP). The basis is that since all current US plants have two independent grid connections, a LOOP would require loss of both grid connections which is a CCF in itself, and the likelihood of a LOOP concurrent with a beyond design basis CCF in a mitigating system is very low and does not require further consideration (in the events that involve a plant trip, an analysis demonstrates that a plant trip will not cause a grid disturbance that can result in a LOOP). A beyond design basis CCF caused by an I&C failure in a mitigating system is still analyzed coincident with each AOO and PA.

Note that a LOOP by itself is an AOO; therefore, a LOOP alone with a credible and concurrent beyond design basis CCF in the I&C system is analyzed.

Similarly, a beyond design basis CCF caused by an I&C failure is not analyzed coincident with a Station Blackout (SBO) as defined in 10 CFR 50.63, because an SBO is a beyond design basis CCF in itself, and the low likelihood of two unrelated CCFs, both of which are beyond design basis does not require further consideration.

4.3.3 Bounded Criteria

The plant-level end result due to a CCF malfunction is considered bounded if all the following criteria are met, whether the CCF is design basis or beyond design basis:

1. If the same type of transient or accident is already included in the deterministic safety analyses described in the FSAR (for example, an excess feedwater event),
2. If only systems previously described in the FSAR are credited for event 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 described in the FSAR from Item 1, above (for example, departure from nucleate boiling ratio or containment pressure).

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

> For example, the plant-level end result of a CCF of both divisions in the main control room chiller system is bounded if the safety systems or

components that require cooling, such as RPS and ESFAS equipment located within the main control room envelope, are still capable of performing the safety functions credited in the FSAR.

Bounded is demonstrated using the guidance provided in Section 4.3.1.

At this point the CCF technical evaluation is complete, unless the design engineer and/or the safety analyst wish to perform another iteration in design and/or analysis activities to determine if any proposed design changes have increased or decreased CCF vulnerabilities, or provided more or less safety margin.

5 REFERENCES

5.1 *METHODS FOR ASSURING SAFETY AND DEPENDABILITY WHEN APPLYING DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS*. EPRI, PALO ALTO, CA: 2016. 3002005326.

5.2 US NRC SECY 16-0070, "*INTEGRATED STRATEGY TO MODERNIZE THE NUCLEAR REGULATORY COMMISSION'S DIGITAL INSTRUMENTATION AND CONTROL REGULATORY INFRASTRUCTURE,*" DATED MAY 31, 2016 (ML16126A140)

5.3 U SNRC SECY 93-087, "*POLICY, TECHNICAL AND LICENSING ISSUES PERTAINING TO EVOLUTIONARY AND ADVANCED LIGHT-WATER (ALWR) DESIGNS*," DATED APRIL 2, 1993

5.4 US NRC STAFF REQUIREMENTS MEMORANDUM IN RESPONSE TO SECY 93-087, LETTER TO JAMES M. TAYLOR, EXECUTIVE DIRECTOR OF OPERATIONS, "*POLICY, TECHNICAL AND LICENSING ISSUES PERTAINING TO EVOLUTIONARY AND ADVANCED LIGHT-WATER (ALWR) DESIGNS*," DATED JULY 21, 1993

5.5 USNRC NUREG 0800, THE STANDARD REVIEW PLAN, BRANCH TECHNICAL POSITION (BTP) 7-19, REV. 7 *"GUIDANCE FOR EVALUATION OF DIVERSITY AND DEFENSE-IN-DEPTH IN DIGITAL COMPUTER-BASED INSTRUMENTATION AND CONTROL SYSTEMS REVIEW RESPONSIBILITIES"* DATED AUGUST 2016

5.6 10 CFR 50.49, "*ENVIRONMENTAL QUALIFICATION OF ELECTRIC EQUIPMENT IMPORTANT TO SAFETY FOR NUCLEAR POWER PLANTS"*

5.7 10 CFR 100, "*REACTOR SITE CRITERIA*"

5.8 10 CFR 50.63, "*LOSS OF ALL ALTERNATING CURRENT*"

5.9 USNRC NUREG 2122, **"***GLOSSARY OF RISK-RELATED TERMS IN SUPPORT OF RISK- INFORMED DECISION MAKING*" DATED MAY 2013

5.10 USNRC GENERIC LETTER 84-01, "*NRC USE OF THE TERMS, "IMPORTANT TO SAFETY" AND "SAFETY RELATED*" DATED JANUARY 1984

5.11 IEEE STD. 603-1991, "*IEEE STANDARD CRITERIA FOR SAFETY SYSTEMS FOR NUCLEAR POWER GENERATING STATIONS*"

APPENDIX A: PREVENTIVE AND LIMITING MEASURES

This Appendix provides detailed preventive and limiting measures that may be applied to a proposed I&C system or component design. Use the guidance in Section 4.2.2 to determine how and when preventive and/or limiting measures are intended to be applied. Note that the preventive and limiting measures in this section are not meant to be an exhaustive or complete set. Alternate measures may be developed and applied as long as justification is provided. Any given preventive or limiting measure listed in this section is meant to be applied as a whole measure. An incomplete measure that is credited in the CCF susceptibility analysis is also an alternate measure that requires justification.

The material provided below is extracted from a report published by the Electric Power Research Corporation (EPRI), report number 3002005326, as cited in Reference 5.1. Appendix A from EPRI 3002005326 provides the following:

1. A detailed set of preventive measures that can be helpful to the design engineer because they can be used to drive the likelihood of a CCF of multiple controlled SSCs to be at or below that of failures considered sufficiently unlikely that they would not typically be postulated and analyzed as part of the plant safety analysis report, which is labelled as "Level 2" likelihood in the EPRI report. In NEI 16-16, this is taken as "non-credible" in terms of a likelihood that is low enough to obtain or maintain a facility license with no further consideration of CCF. There is no guarantee that a CCF cannot happen, but a preventive measure can be used to reach a low enough likelihood of CCF that it can be considered non-credible in licensing terms. Wherever "Level 2" is mentioned below, consider the likelihood of the CCF to be no more likely than other CCFs that are not considered in deterministic safety analyses.
2. In a similar manner, "Level 0" is mentioned below, which indicates "*the CCF likelihood is considered comparable to that of failures traditionally postulated in conservative safety analyses, such as single hardware failures and CCFs caused by single hardware failures*" per Section 2.2.5.1 of the EPRI report. In NEI 16-16, this is taken to mean the likelihood is comparable to that of an AOO in licensing terms so that the CCF susceptibility analysis can support a licensing determination. Wherever "Level 0" is mentioned below, consider the likelihood of the CCF to be as likely as AOOs that are considered in deterministic safety analyses.
3. A detailed set of limiting measures that can be helpful to the design engineer because they can be used to limit the effects of a CCF by forcing a preferred SSC malfunction state, limiting the number of affected SSCs, or a combination of both.
4. Guidance on coping methods and coping analysis for each category of I&C failure source. The term "coping analysis" is not used in the body of this guide, which uses "analysis of CCF malfunction result" instead. Wherever "coping analysis" is mentioned below, consider it to be synonymous with "analysis of CCF malfunction result" as used in NEI 16-16.

Note that the first paragraph below refers to "Section 3.3" of EPRI 3002005326, which is not extracted into this guide because the purpose of this guide is to provide CCF technical evaluation results that can support licensing determinations, whereas the purpose of EPRI

3002005326, as stated in Section 1.2 of that report, is to "*provide guidance that will help nuclear utilities systematically identify, assess, and manage failure susceptibilities of digital I&C systems and components.*" NEI 16-16, by design, provides technical guidance for addressing CCF for compliance to deterministic licensing criteria and current NRC policies (such as SRM-SECY-93-087 and BTP 7-19).

In addition, other references to sections within EPRI 3002005326 are provided below, such as "*Level 2 per Section 2.2.5.1 and 2.2.5.5*." As noted in item 1 above, Level 2 indicates the likelihood of the CCF to be no more likely than other CCFs that are not considered in deterministic safety analyses, which is consistent with the guidance provided in Section 4.2.2.3 of this guide on the use of preventive measures.

EPRI 3002005326 Appendix A (verbatim)

This appendix provides the detailed guidance for each preventive and limiting measure listed in the various tables provided in Section 3.3, where hyperlinks are provided for each measure. This Appendix is not intended to stand by itself; users are cautioned to use the guidance in Section 3.3 first, and allow the hyperlinks in that section to support navigation to the detailed guidance herein. Upon reading the detailed guidance in this Appendix, use the "Alt + Left Arrow" keys to jump back to the summary guidance in Section 3.3.

Note that some of the measures described below are provided with "caution" statements intended to warn the user that design tradeoffs should be carefully evaluated before selecting and applying the measure. While the defensive measures in this section are intended to prevent or limit CCFs, in some applications they may adversely affect malfunction frequency. In addition, a system is made up of many of the specific elements identified in each of the measures described below. Users should consider the tradeoffs among the defensive measures that are selected and applied, and be prepared to iterate the system design to optimize the measures in the aggregate.

Also note that some measures are provided with "confirm" statements that are intended to remind the user that equipment information, such as commercial specification sheets, should not be taken at face value without some additional indication that the information is valid. For example, preventive measure A23-P1 calls for a demonstration that a controller can operate without failure during a loss of HVAC. For safety systems, an equipment qualification program is credited toward assuring such a demonstration will occur through independent testing. However, for non-safety systems the user might "confirm" the manufacturer's equipment specifications by asking the vendor for design, test or analysis information. Such information is typically available upon request in the form of test certificates or test reports that are required by a third party (e.g., Underwriter's Lab, CE Mark service provider, etc.) before their mark can be affixed to the equipment nameplate.

A.1 CCF Caused by a Random Hardware Failure in a Shared Resource

This section applies to any hardware resource shared by multiple SSCs, either in a single controller shared by multiple SSCs (Type 1 Design in Figure A-1) or as a resource shared by multiple controllers (Type 2 Design in Figure A-1), each of which controls a single SSC. This distinction is important because the methods provided in this section assume there is only one SSC connected to each controller in the Type 2 design.

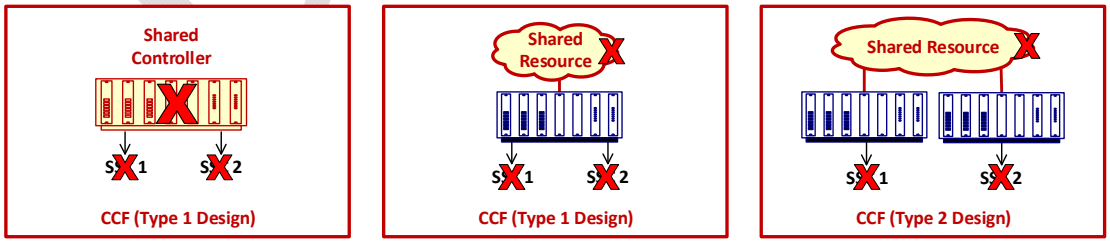


Figure A-1
CCFs Caused by a Random Hardware Failure in a Shared Resource

A shared resource in a Type 1 design can be the controller itself, including resources internal to the controller. Therefore, CCF preventive measures address any condition that could result in an out of service condition for that controller.

Note that Figure A-1 shows two SSCs for simplicity; a CCF could involve two or more controlled SSCs. For both design types, the two SSCs 1 and 2 shown in Figure A-1 are representative of any number of controlled SSCs, 1 thru N. The point of these figures is to simply show that multiple SSCs may be controlled by one controller or may be distributed to multiple controllers. Either configuration is likely to have one or multiple shared resources where a random hardware failure can lead to erroneous operation of more than one SSC (i.e., a CCF).

An "X" in Figure A-1, and subsequent figures as well, denotes a failure, and a yellow shape denotes the source of the failure. Multiple X's in a figure indicate a failure at the source and a malfunction of at least one affected SSC. If only one SSC is affected, then there is no CCF, and the result is shown as a "Single Effect" which is essentially the same result as a random hardware failure of the controlled SSC itself.

The term "controller" is used in this guidance to mean a single, duplex, or triplex configuration, except as specifically noted.

This section applies to non-safety equipment, as well as safety equipment within the same division. It is generally not applicable to safety equipment in separate divisions, because safety systems comply with the single failure criterion. Therefore, each safety division has its own resources to maintain independence; however, there are exceptions, as noted.

In this section random hardware failures are considered for active components only. CCFs caused by other passive failures that are considered when evaluating a safety system's compliance to the single failure criterion (e.g., IEEE-379 in the U.S.), such as shorts to ground, open wires/terminations and hot shorts, are considered to be no more likely than CCFs that are not considered in the traditional conservative safety analysis (i.e., Level 2 per Section 2.2.5.1). Therefore, these passive failures are not evaluated herein when assessing CCF likelihood. Shorts to ground, open circuits and hot shorts are considered if they can be caused by failure of an active component.

This section describes preventive measures that can substantially reduce the likelihood of CCFs caused by random hardware failures in various types of shared resources listed in Table A-1, to Level 2 per Sections 2.2.5.1 and 2.2.5.5. If those or comparable methods are not employed, and low likelihood cannot be assured, a coping analysis may be helpful in determining the acceptability of the resulting CCF.

Random component failures are typically considered in analyses to confirm that the plant design is sufficiently robust, using conservative acceptance criteria (i.e., their likelihood is at Level 0 per Section 2.2.5.1). Therefore, the consequences of SSC malfunctions resulting from random hardware failures in the I&C may already have been analyzed and found to be acceptable. If a random hardware failure in the new I&C design creates an unanalyzed malfunction, a new coping analysis should be performed using the same acceptance criteria.

Table A-1
Shared I&C Resources Whose Random Hardware Failure can Lead to a CCF of Controlled SSCs

Shared Resource Type
Power source
Sensor or associated input processing
Output module
Control signal originating in one controller
Data communication network or data link
Operator workstation with soft controls
Engineering/maintenance workstation
Controller
Clock

All of the Preventive and Limiting measures described in this section accommodate a random failure of an active component within the subject failure source. If any of these devices contain digital components (e.g., microprocessors, FPGAs), they should also be evaluated for a potential CCF caused by a *design defect*, as described in Section A.3, below. Digital components are becoming more common in devices such as power supplies and sensors.

A Generic Preventive Measure for Protecting Against Multiple SSC Malfunctions Caused by Accumulated Hardware Failures

Often, failures within the I&C are either self-announcing or detectable through periodic testing (assuming test cases are properly designed). Effectively, this is a generic preventive measure that protects against CCFs caused by accumulated random component failures, enabling component replacement and SSC function restoration before random hardware failures can accumulate to become CCFs. Failed components are replaceable, so the equipment can be restored to its original configuration (i.e., the ability to tolerate a single active component failure) without forcing other equipment to be out-of-service that has not already been affected by the original failure. For most failures this requires on-line hot swap capability.

A.1.1 Random Hardware Failure in a Shared Power Source

A random component failure in a shared power source can produce any of the following conditions:

Condition 1 Loss of voltage
Condition 2 Undervoltage
Condition 3 Overvoltage
Condition 4 Voltage oscillation (including noise and irregular harmonics)

Condition 1 results in a predictable failure state (loss of function). The failure states resulting from Condition 2 through Condition 4 are unpredictable (i.e., erroneous control actions, including spurious actuations).

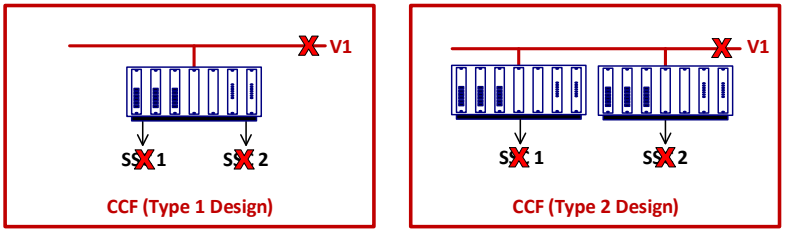


Figure A-2
CCF Caused by a Random Hardware Failure in a Shared Power Source

A.1.1.1 Measures Intended to Reduce the Likelihood of a CCF of Multiple Controlled SSCs Caused by a Random Hardware Failure in a Shared Power Source to Level 2

The design basis for Measures Intended to Reduce the likelihood of CCF of multiple controlled SSCs caused by a random failure of a shared power source to Level 2, is to provide each controller (including components of the controller required to operate the SSCs, such as CPU modules, input modules, output modules and communication modules) with a filtered, regulated, uninterruptable power source. To meet this design basis, using any one of the preventive measures listed in Table A-2 is recommended. All of the preventive measures (A2-P1 through A2-P6) provide uninterruptable power, but a UPS can only reduce the likelihood of Condition 1 in the list above. A2-P1 through A2-P5 also provide voltage regulation to reduce the likelihood of Conditions 2 through 4. A2-P6 shows that some controllers can be provided with their own internal voltage regulation.

The UPS configurations described in this section reduce the likelihood of a CCF of controlled SSCs caused by Condition 1 involving a random component failure or a Loss of Offsite Power (LOOP) event. A concurrent LOOP and UPS failure is considered to have a sufficiently low potential to be classified as Level 2 in this guideline. In systems with interdivisional independence, a separate UPS is provided for each division, again reducing the likelihood of a CCF in the event of a LOOP concurrent with a UPS failure, to Level 2.

Table A-2
Measures Intended to Reduce the Likelihood of a CCF Caused by a Component Failure in a Shared I&C Power Source to Level 2

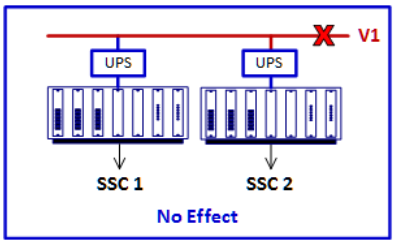
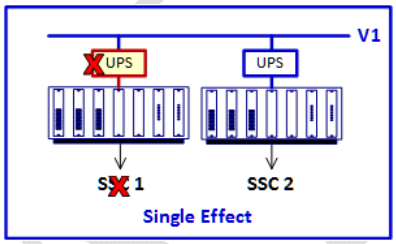
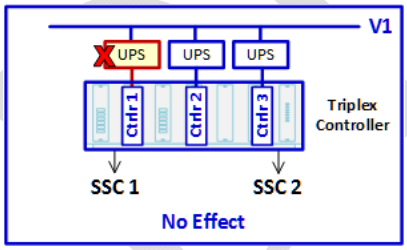
Preventive Measures	
P1	**Provide a dedicated, regulated uninterruptible power source (UPS) for each controller; each UPS includes voltage filtering and regulation.** An analysis demonstrates that bus voltage is restored prior to exhausting each UPS battery backup, and the mission time of the UPS is matched with the mission time of the SSC. Each UPS also provides a regulated output that blocks voltage disturbances from shared power source V1 that would otherwise negatively affect multiple controllers. The figure on the left shows that a random failure of a power bus V1 shared between two controllers results in no effect on SSCs 1 or 2 because the controllers are protected against the failure from V1 by the UPSs, which provide filtering, regulation and uninterruption. A random failure of a UPS (i.e., any Condition 1-4) will only affect one controller (spurious actuation or loss of function), as shown in the figure on the right. Since each controller controls only one SSC a UPS failure only affects one SSC (i.e., no CCF).   Note that this preventive measure **does not** reduce the likelihood of a CCF in a Type 1 design to less than Level 0, because as shown in Figure A-1, a random failure of the UPS affects all SSCs controlled by the same controller. To reduce the likelihood of a CCF caused by a shared power source in a Type 1 design to Level 2, also provide a controller with triplex redundancy and 2oo3 output voting, and power each redundancy as if it were a separate controller, per the description above and the figure below. This design measure prevents the CCF because a failure of one UPS will negatively affect only one controller and the erroneous signals from that one controller will get voted out in the triplex configuration. 

Table A-2 (continued)
Measures Intended to Reduce the Likelihood of a CCF Caused by a Component Failure in a Shared I&C Power Source to Level 2

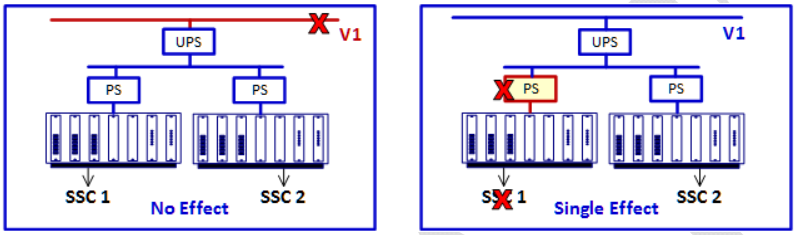
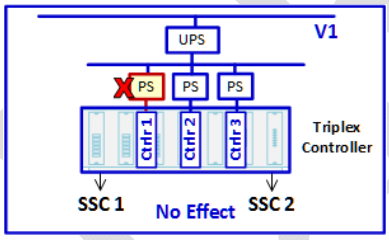
Preventive Measures	
P2	**Provide one shared UPS for all controllers, with a dedicated regulated power supply for each controller.** A failure analysis conducted for the UPS demonstrates that there is no single active component failure within the UPS that can result in a loss of power. An analysis demonstrates that bus voltage can be restored prior to exhausting the UPS battery backup, and the mission time of the UPS is matched with the mission time of the SSC. Each power supply provides input filtering and a regulated output that prevents voltage disturbances from the shared UPS that would otherwise negatively affect multiple controllers. The figure on the left shows a random hardware failure in bus V1 with no effect on controlled SSCs. The figure on the right shows a failure of a power supply (i.e., any Condition 1-4), with the result that only one controller is negatively affected.  Note that this preventive measure **does not** reduce the likelihood of a CCF in a Type 1 design to less than Level 0, because as shown in Figure A-1, a random failure of the regulated power supply affects all SSCs controlled by the same controller. To reduce the likelihood of a CCF caused by a shared power source in a Type 1 design to Level 2, provide a controller with triplex redundancy with 2oo3 output voting and power each redundancy as if it were a separate controller, per the description above and the figure below. This design measure reduces the CCF likelihood to Level 2 because there is no active component failure within the UPS that will result in a loss of power. In addition, a power supply failure will negatively affect only one controller and the erroneous signals from that one controller will get voted out in the triplex configuration. 

Table A-2 (continued)
Measures Intended to Reduce the Likelihood of a CCF Caused by a Component Failure in a Shared I&C Power Source to Level 2

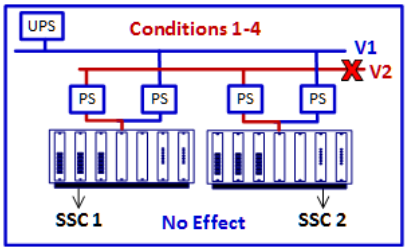
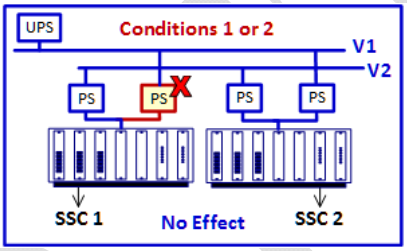
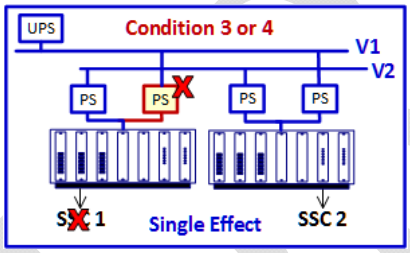
Preventive Measures	
P3	**Provide two auctioneered and regulated power supplies for each controller with each power supply powered from a different bus, and at least one bus is provided with a UPS.** An analysis demonstrates that the bus voltage can be restored prior to exhausting the UPS battery backup (which is provided to protect against a LOOP), and the mission time of the UPS is matched with the mission time of the controlled SSC. Each power supply provides input filtering and a regulated output that blocks voltage disturbances from a shared bus that would otherwise negatively affect multiple controllers. The figure on the left shows a random failure of one bus (i.e., any Condition 1-4), and the result is no SSCs are affected. Likewise, the figure on the right shows a random failure of a power supply (i.e., Conditions 1 or 2), with the same result.   Note that this preventive measure will not block an overvoltage condition or a voltage oscillation (i.e., Conditions 3 and 4) from a power supply pair because the controller sees the highest voltage of the auctioneered pair. Therefore, for Condition 3 or 4 a single SSC is negatively affected as shown in the figure below. Since only one SSC is affected, this defensive measure reduces the CCF likelihood to Level 2.  Note that this preventive measure **does not** reduce the likelihood of a CCF in a Type 1 design to less than Level 0, because as shown in Figure A-1, a random failure of the power supply (condition 3 or 4) affects all SSCs controlled by the same controller. To reduce the likelihood of a CCF caused by a shared power source in a Type 1 design to Level 2, provide a controller with triplex redundancy with 2oo3 output voting, and power each redundancy as if it were a separate controller, per the description above.

Table A-2 (continued)
Measures Intended to Reduce the Likelihood of a CCF Caused by a Component Failure in a Shared I&C Power Source to Level 2

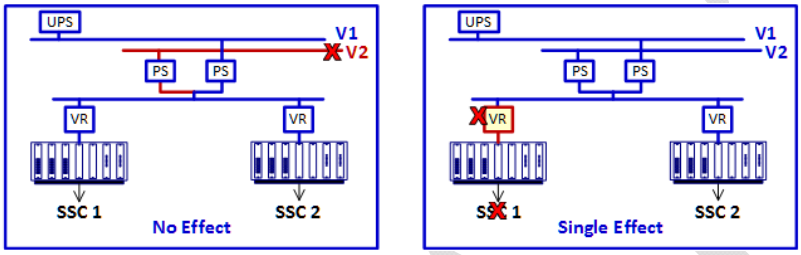
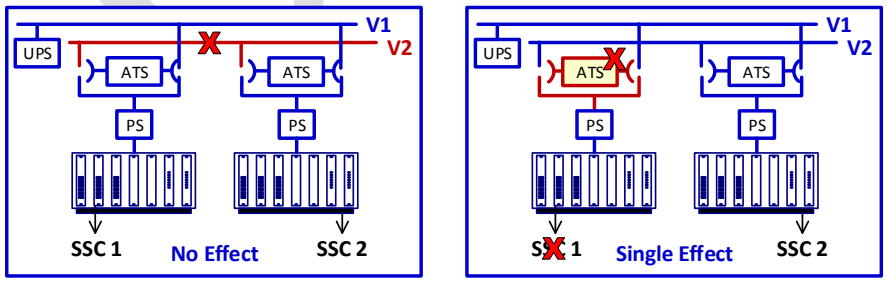
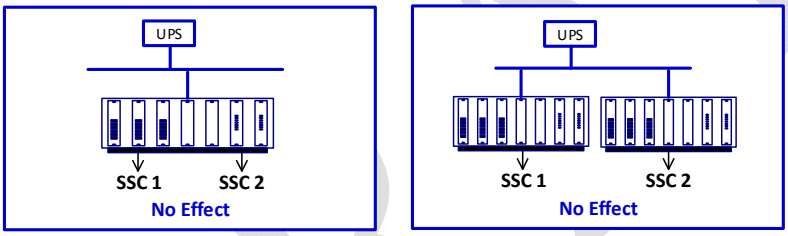
Preventive Measures	
P4	**Provide two auctioneered power supplies shared for all controllers, with each power supply powered from a different bus, at least one being from a UPS, and provide a separate voltage regulator for each controller**. An analysis demonstrates that the bus voltage can be restored prior to exhausting the UPS battery backup. The power supplies provide bus noise filtering. Each voltage regulator provides a regulated output that blocks voltage disturbances from the shared auctioneered power supplies that would otherwise negatively affect multiple controllers. The figure on the left shows a random failure of one bus or power supply (i.e., any Condition 1-4), and the result is no SSCs are affected. The figure on the right shows a failure of a voltage regulator (i.e., any Condition 1-4) with the result that only one controller is negatively affected.  Note that this preventive measure **does not** reduce the likelihood of a CCF in a Type 1 design to less than Level 0, because as shown in Figure A-1, a random failure of a voltage regulator affects all SSCs controlled by the same controller. To reduce the likelihood of a CCF caused by a shared voltage regulator in a Type 1 design to Level 2, provide a controller with triplex redundancy and 2oo3 output voting, and power each redundancy as if it were a separate controller, per the description above.
P5	**Provide two busses and an Automatic Transfer Switch (ATS) for each controller**. At least one bus is provided with a UPS, and a separate regulated power supply is provided for each controller. An analysis demonstrates that the bus voltage can be restored prior to exhausting the UPS battery backup. Each power supply provides input filtering and a regulated output that blocks voltage disturbances from the shared busses that would otherwise negatively affect multiple controllers. An analysis is performed to demonstrate that the regulated power supply output is not negatively affected by ATS actuation. The figure on the left shows a random failure of one bus (i.e., any Condition 1-4), and the result is no SSCs are affected. The figure on the right shows a failure of an ATS or a regulated power supply (i.e., any Condition 1-4) with the result that only one controller is negatively affected. 

Table A-2 (continued)
Measures Intended to Reduce the Likelihood of a CCF Caused by a Component Failure in a Shared I&C Power Source to Level 2

Preventive Measures	
P5	Caution: This preventive measure **does not** reduce the likelihood of a CCF in a Type 1 design to Level 2, because, as shown in Figure A-1, a random failure of an ATS or shared power supply affects all SSCs controlled by the same controller. To reduce the likelihood of a CCF caused by an ATS or shared power source in a Type 1 design to Level 2, provide a controller with triplex redundancy and 2oo3 output voting, and power each redundancy as if it were a separate controller, per the description above.
P6	**Provide one shared UPS for all controllers, with analysis of controller performance.** A failure analysis is conducted for the UPS to demonstrate that there is no active component failure within the UPS that can result in a loss of power (i.e., Condition 1). An analysis demonstrates that bus voltage can be restored prior to exhausting the UPS battery backup, and the mission time of the UPS is matched with the mission time of the SSC. A power source analysis specifies the worst case power supply disturbances during normal and UPS failure conditions. An analysis and test demonstrate that the controllers can tolerate the worst case noise and voltage fluctuations from the UPS (i.e., Conditions 2-4). Since the UPS has no failure that can result in loss of power and the controllers protect themselves from worst case UPS voltage fluctuations, there is no power source failure that negatively affects the controllers. This preventive measure is applicable to Type 1 and 2 designs as shown below. 

A.1.1.2 Limiting a CCF Caused by a Component Failure in a Shared Power Source

If no preventive measures described in Section A.1.1 are implemented, or if one is only partially implemented, then one of the limiting measures listed in Table A-3 may be helpful. The limiting measures in this section reduce the likelihood of a CCF of controlled SSCs caused by failure Conditions 2-4 (i.e., erroneous operation caused by power source anomalies). Eliminating these CCF conditions is helpful, because erroneous operation is difficult to predict and therefore difficult to analyze for multiple SSCs. However, these limiting measures do not reduce the likelihood of a CCF of controlled SSCs caused by Condition 1, because they do not include dual power sources or a UPS. Since the likelihood of a CCF of controlled SSCs is not considered to be Level 2 for a Loss of Offsite Power (LOOP) event or a random failure that leads to a complete loss of voltage condition, a CCF coping analysis is provided for these limiting measures to demonstrate that the loss of voltage condition for all SSCs is an acceptable CCF. Guidance for coping analysis is provided in Section A.1.1.3.

Table A-3
Measures for Limiting a CCF Caused by a Random Failure of a Shared Power Source

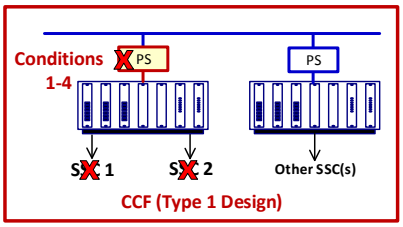
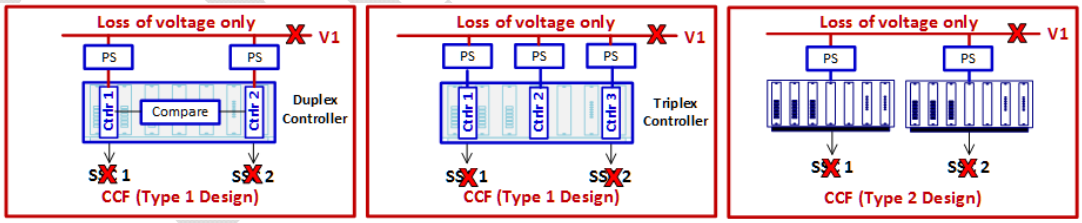
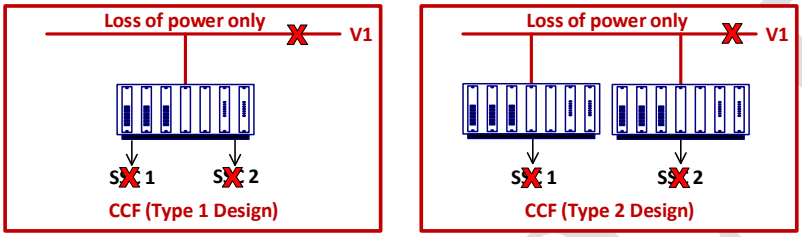
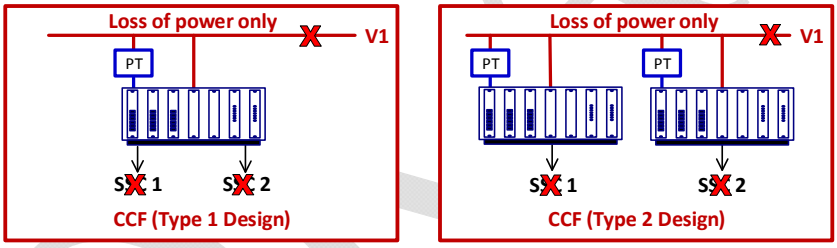
Limiting Measures	
L1	**Provide a shared power bus with a dedicated regulated power supply for each controller.** Each power supply provides input filtering and a regulated output that blocks voltage disturbances from the shared bus that would otherwise negatively affect multiple controllers. The figure below shows a failure of a power supply (i.e., any Condition 1-4) with the result that only one controller is negatively affected.  Caution: This design **does not** limit a CCF in a Type 1 design as shown in Figure A-1, because a random failure of the power supply affects all SSCs controlled by the same controller, and the controller behavior remains unpredictable for Conditions 1-3. To limit a CCF for a Type 1 design, provide a duplex controller with an output compare function (left figure below) or triplex redundancy with 2oo3 output voting (middle figure below) and power each redundancy as if it were a separate controller, per the description above. The output compare function continuously compares the redundant outputs of the duplex controller to detect differences and force both controllers to shut down. Therefore, if one of the duplex controllers is negatively affected by a power source anomaly, the controlled SSCs will be forced to their de-energized position. The figure on the right shows that even with this limiting measure a random failure of the shared power bus results in loss of power to both controllers in a Type 2 design. For this limiting measure, the regulated power supplies constrain the resulting CCF to a loss of voltage condition only (i.e., Condition 1), which results in *predictable* controller outputs. Undervoltage, overvoltage, and voltage oscillation conditions, which would otherwise result in a CCF with *unpredictable* controller outputs, are prevented because the power supplies maintain voltage within an acceptable range.  Therefore, given this limiting measure, a CCF coping analysis will only consider the loss of voltage condition and the resulting, predictable, controller outputs because the other unpredictable conditions are designed out of the system.

Table A-3 (continued)
Measures for Limiting a CCF Caused by a Random Failure of a Shared Power Source

Limiting Measures	
L2	**Demonstrate controller tolerance to power supply disturbances through design evaluation and documented testing.** A power source analysis specifies the worst case power supply disturbances during power source failure conditions. This allows an evaluation of the controller's voltage tolerance specification and design, and specification of test cases for controller testing to provide assurance that the controller can tolerate worst case power source disturbances with no erroneous SSC operation. Therefore, the CCF is limited to the loss of power condition. This limiting measure is applicable to Type 1 and 2 designs, as shown in the figures below. 
L3	**Monitor power source for intolerable power source conditions and force a predictable loss of voltage condition.** Intolerable power source conditions can include undervoltage, overvoltage, and voltage oscillations. Like L1 and L2, this limiting measure constrains the CCF to a loss of power condition only, which results in *predictable* controller outputs. Both figures show a potential transformer (PT) as an example method for monitoring the shared power source (an analog input or a voltage sensor could be used for DC supply monitoring). This limiting measure is applicable to Type 1 and 2 designs, as shown in the figures below. 

A.1.1.3 Coping with a CCF of Multiple Controlled SSCs Caused by a Predictable Loss of Power State

The limiting measures described in Section A.1.1.2 result in a CCF that is limited to the loss of voltage condition only. Since the loss of voltage condition results in predictable controller behavior, the CCF *coping analysis* is simplified compared to a CCF that results in unpredictable controller behavior.

Loss of voltage can affect the controller's inputs, its CPU, and/or its outputs, depending on the voltage source partitions (e.g. fuses, voltage regulators). For example if inputs, CPU and outputs are each fused separately, then each can fail separately and the failure effects will be different. Therefore the first step in this CCF *coping analysis* is to determine the power source partitions, the potential failures and the failure effects. Each is discussed, as follows:

Controller Outputs

If the output modules lose power, the outputs will transition to their de-energized output state. This CCF of the resulting positions of controlled SSCs may already be analyzed in the plant's safety analysis, in which case no additional *coping analysis* may be needed. For example, if a controller controls multiple main feedwater components (e.g., pumps and/or valves), multiple outputs that transition to the de-energized state may result in a loss of all main feedwater. The loss of all main feedwater is a condition that is analyzed for most (maybe all) plants in their safety analysis. Therefore, when conducting the CCF *coping analysis* it is important to determine what has already been analyzed and the similarities and differences between that analysis and this CCF.

Controller CPU

When the controller CPU loses power, but the controller outputs remain powered, the controller outputs may fail to their de-energized state, hold their current state or fail to a predetermined state, depending on the capabilities of the output modules and how those modules are configured. If the outputs hold their current state, then an immediate transient is avoided. The CCF *coping analysis* is limited to demonstrating that operators will be notified of this condition through alarms, and that they can manage the condition until power can be restored, without creating a plant transient. Since operators are monitoring the condition, they can detect an undesirable trend and can reduce the likelihood of the occurrence of a transient.

It is noted that a CPU failure typically affects both automatic and manual control for the controlled components (there are exceptions with unique designs). In such a case, the coping analysis would need to demonstrate the capability to use other plant components, not the ones controlled by the affected controller, in response to the CCF of the controlled SSCs. One acceptable coping method to reduce the likelihood of an unacceptable plant condition may be for operators to manually trip the plant or manually initiate a controlled shutdown when an undesirable trend is detected; the CCF coping analysis would then demonstrate the operator's ability to recognize the condition and take the appropriate actions, using HFE analysis methods.

In the U.S., Appendix 18-A of NUREG-0800 [6] provides a method for crediting manual operator actions.

Controller Inputs

When the input modules lose power, but the CPU and outputs remain powered, the control algorithm may execute with the last good input value, or a predetermined default input value. The resulting effects on the controller's outputs are dependent on the control algorithms. The CCF coping analysis is limited to demonstrating that operators will be notified of this condition through alarms, and that they can manage the condition until power can be restored, without creating a transient. Since operators would be monitoring the condition, they would be expected to detect an unacceptable trend and reduce the likelihood of the occurrence of a plant transient. This failure is not as challenging to plant operators as the CCF for failure of the controller outputs or the controller CPU, because the operators can still control the affected plant components manually, unless the input supports an equipment protection interlock that blocks component repositioning.

A.1.2 Random Hardware Failure in a Shared Sensor or Associated Input Processing

This section addresses random hardware failures in sensors and input processing. These components are also subject to drift that could commonly affect multiple redundant sensors. This is not a failure, but rather an expected condition that can lead to CCF. To maintain the likelihood of a CCF of controlled SSCs caused by drift at Level 2, sensors and input processing are periodically calibrated using a reference calibration standard.

A random failure of a shared sensor or associated input processing (e.g., signal conditioning, analog-to-digital conversion) can produce any of the following conditions:

Condition 1	Fail as-is
Condition 2	Fail Low (i.e., out of range low)
Condition 3	Fail High (i.e., out of range high)
Condition 4	Signal drift
Condition 5	Signal oscillation

Failure effects are predictable for single SSCs. As more SSCs are affected, the failure effects become more difficult to predict. Figure A-3 illustrates three examples of a shared sensor or shared input processing that could lead to a CCF.

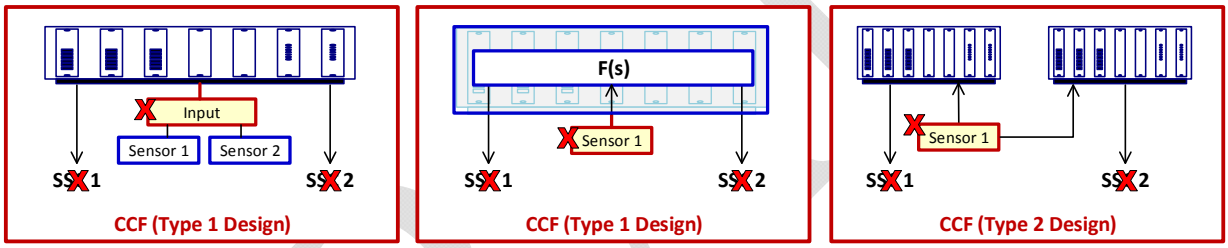


Figure A-3
CCF Caused by a Shared Sensor or Shared Input Processing

A.1.2.1 Measures Intended to Reduce the Likelihood of a CCF of Multiple Controlled SSCs caused by a Random Failure of a Shared Sensor or Associated Input Processing to Level 2

To reduce the likelihood of a CCF caused by a random failure of a shared sensor or associated input processing, applying one of the measures from Table A-4 (or comparable measures) is recommended.

Table A-4
Measures Intended to Reduce the Likelihood of a CCF caused by a Random Failure of a Shared Sensor or Associated Input Processing to Level 2

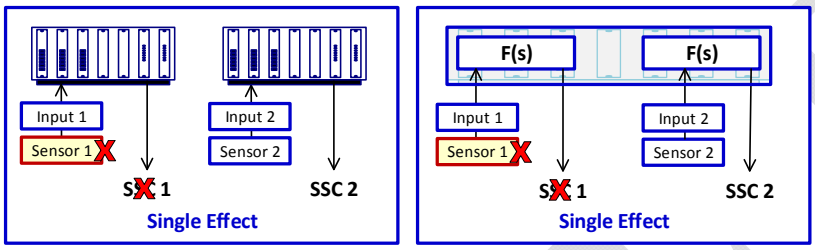
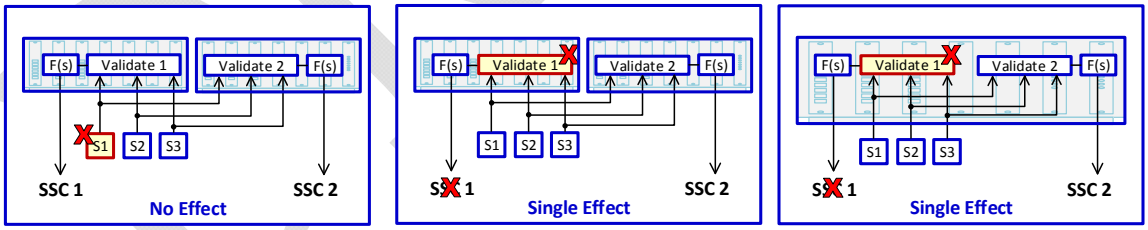
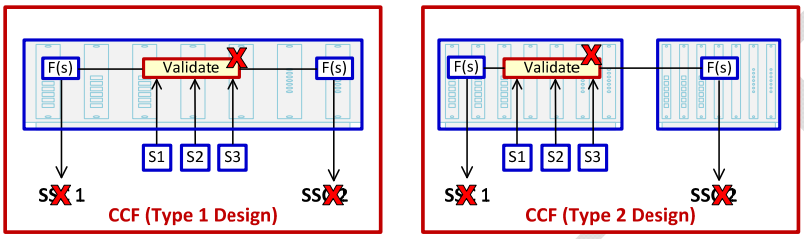
Preventive Measures	
P1	**Provide a separate sensor and associated input processing for each SSC with no shared resources.** For example, the figure on the left shows that a random failure of a sensor results in spurious actuation of a single SSC or loss of a single SSC in a Type 2 design. Likewise, the figure on the right shows that a random failure of a signal input device has the same result in a Type 1 design.  Caution: This measure is only effective, if there are no shared resources between these separate sensors, such as a shared power supply. If there are shared resources between sensors then those resources are examined for their potential to cause failure of multiple sensors, and the appropriate preventive measure(s) applied.
P2	**Provide three shared, redundant, sensors, with dedicated signal validation for each SSC.** The signal validation block is essentially a voter on the process values originating from three physical sensors on the same process. Typical signal validation methods include median select or averaging sensors that remain within deviation limits. For example, the figure on the left shows that a random failure of a sensor results in no effect on either SSC because the remaining sensors continue to support both SSCs. In the middle figure (Type 2 design) and the figure in the right (Type 1 design) a failed validation results in spurious actuation or loss of a single SSC; the remaining SSC is unaffected.  The figure on the right above shows separate validation functions. However, each separate validation function employs separate memory within the controller. If the same function blocks are employed to execute the validation function, it is likely that those function blocks can be negatively affected by a random hardware failure in the controller's memory, resulting in a CCF. See Section A.1.8 on controller internal error.

Table A-4 (continued)
Measures Intended to Reduce the Likelihood of a CCF caused by a Random Failure of a Shared Sensor or Associated Input Processing to Level 2

Preventive Measures	
	Caution: Note that in each figure above, the signal validation is separate for each SSC in order to avoid a CCF caused by a failure in a shared signal validation output. This CCF is illustrated in the following figure:  The figure on the right above shows separate validation functions. However, each separate validation function employs separate memory within the controller. If the same function blocks are employed to execute the validation function, it is likely that those function blocks can be negatively affected by a failure in the controller's memory, resulting in a CCF.

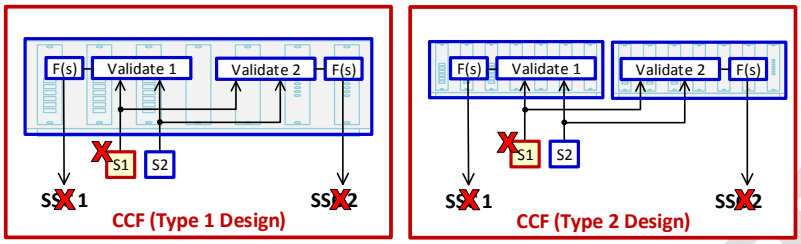
A.1.2.2 Limiting a CCF Caused by a Random Failure of a Shared Sensor or Associated Input Processing

If no preventive measures listed in Table A-4 are implemented, or if one is only partially implemented, then one of the limiting measures listed in Table A-5 may be helpful.

Table A-5
Measures for Limiting a CCF Caused by a Random Failure of a Shared Sensor or Associated Input Processing

Limiting Measures	
L1	**Provide two shared, redundant sensors, with dedicated signal validation for each SSC.** Signal validation is the average of the process values originating from both physical sensors on the same process, when they are within their specified range and within deviation limits of each other. But when sensors deviate outside those limits, with only two sensors it is not possible to identify which sensor is correct. Therefore, force the signal validation output to a predetermined state. The result is a CCF of all SSCs controlled by those shared sensors, as shown in the figures below; but this predetermined state simplifies the CCF analysis. Signal validation is separate for each SSC to avoid an unpredictable CCF caused by a failure in the signal validation output.

Table A-5 (continued)
Measures for Limiting a CCF Caused by a Random Failure of a Shared Sensor or Associated Input Processing

Limiting Measures	
	 **Caution:** The figure on the left above shows separate validation functions. However, each separate validation function employs separate memory within the controller. If the same function blocks are employed to execute the validation function, it is likely that those function blocks can be negatively affected by a random hardware failure in the controller's memory, resulting in a CCF. See Section A.1.8 on controller internal error.

A.1.2.3 Coping with a CCF Caused by a Predictable Failed Sensor State

The CCF limitation method listed above or a comparable alternative may be implemented using the last good signal validation output value (i.e., when there is no comparison deviation), or a predetermined default signal validation output value, that is then propagated through each SSC's control algorithm. The resulting effects on the controller's outputs are dependent on the control algorithms. The CCF *coping analysis* is limited to demonstrating that operators will be notified of this condition through alarms, and that they can manage the condition until the failed component(s) can be restored, without creating a transient. Since operators would be monitoring the condition, they would be expected to detect an unacceptable trend and reduce the likelihood of the occurrence of a plant transient. With a failed sensor or input module, operators can still control the affected plant components manually, unless the input supports an equipment protection interlock that blocks component repositioning.

A.1.3 Shared Output Module

A random failure of a shared output module can produce any of the following conditions:

Condition 1	Fail as-is
Condition 2	Fail Low (i.e., out of range low)
Condition 3	Fail High (i.e., out of range high)
Condition 4	Output signal drift (high or low)
Condition 5	Output signal oscillation

Failure effects are predictable for single SSCs. As more SSCs are affected, the failure effects become more difficult to predict. In most cases, Condition 1 is not self-announcing; to assure detectability, and thereby reduce the likelihood of random hardware failures from accumulating over time to become CCFs, outputs are periodically tested/cycled to force state changes.

Figure A-4 illustrates an example of a shared output module failure that leads to a CCF.

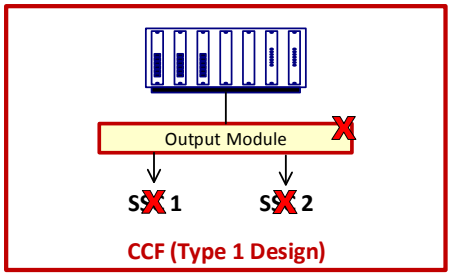
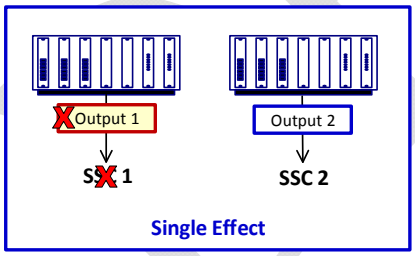
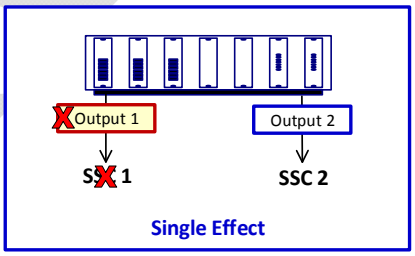


Figure A-4
CCF Caused by a Shared Output Module

A.1.3.1 Measures Intended to Reduce the Likelihood of a CCF of Multiple Controlled SSCs Caused by a Random Failure of a Shared Output Module to Level 2

To reduce the likelihood of a CCF of multiple controlled SSCs, caused by a random failure of a shared output module, applying one of the measures from Table A-6 (or comparable measures) is recommended.

Table A-6
Measures Intended to Reduce the Likelihood of a CCF Caused by a Random Failure of a Shared Output Module to Level 2

Preventive Measures	
P1	**Provide a separate output module for each SSC, with no shared resources.** An output module may provide an analog signal, a conventional binary signal (e.g., contact or voltage state change to distinguish logical 1/0 states), or data communications (e.g., a fieldbus signal) to the CPE. The figure on the left shows that a random failure of an output module in a Type 2 design (i.e., one controller for each SSC) results in spurious actuation of a single SSC or loss of a single SSC. Likewise, the figure on the right shows that a random failure of an output module in a Type 1 design (i.e., shared controller) has the same result, but the shared controller may still be a source of CCF.   Caution: This measure is only effective if there are no shared resources between these output modules, such as a shared power supply. If there are shared resources between output modules then those resources are examined for their potential to cause failure of multiple output modules, and the appropriate preventive measure(s) applied.

A.1.3.2 Limiting a CCF Caused by a Random Failure of a Shared Output Module

The generic measure of limiting a CCF by limiting the number of SSCs that share a resource is applicable here.

A.1.3.3 Coping with a CCF Caused by a Failure of a Shared Output Module

An output module failure can result in a de-energized output state. This condition may be covered by plant transient analyses, even if the output module controls multiple plant components. An example is an output module controlling two main feedwater regulating valves. If both valves fail closed the result is a loss of all main feedwater, which is analyzed for most (maybe all) plants.

However, an output module failure can also result in an erroneous high or low output state. An erroneous low output state is likely to be bounded by the de-energized output state. But an erroneous high output state may be unanalyzed. In the main feedwater example above, erroneous opening of two main feedwater regulating valves will cause excess feedwater flow which can lead to an overcooling condition. If the plant's safety analysis explicitly defines the cause of the analyzed transient as a single feedwater regulating valve failure, then this CCF may not be bounded.

Alternately, the safety analysis may define the transient based on an excess feedwater flow rate or other overcooling parameters; for safety analysis of this type, the excess feedwater flow rate or resulting overcooling temperature from the CCF may be bounded by the current excess feedwater flow transient described in the plant's safety analysis. If the CCF is bounded by an analysis currently in the safety analysis, then no additional analysis is needed.

A.1.4 Random Hardware Failure in a Shared Control Signal

This section address designs that would provide a conventional binary or analog control signal originating in one controller that is interfaced to multiple control SSCs within that controller or to SSCs controlled by another controller (e.g., signal validation output, Tave/Tref calculation).

A random erroneous control signal can be caused by an internal controller error or an input/output failure, and can produce any of the following conditions:

Condition 1	Control signal fail as-is
Condition 2	Control signal fail low (i.e., out of range low)
Condition 3	Control signal fail high (i.e., out of range high)
Condition 4	Control signal drift (high or low)
Condition 5	Control signal oscillation

All SSCs that use the same failed control signal respond erroneously. Control signals that remain in the same state for extended time durations, can fail in a non-announcing as-is mode (Condition 1). To provide assurance that this failure is detectable, and thereby reduce the likelihood of random hardware failures from accumulating over time to become CCFs, control signals are periodically tested/cycled to force state changes.

Figure A-5 illustrate two examples of a shared control signal that leads to a CCF. In the Type 1 design on the left, the control signal and both SSCs are implemented in one controller, whereas a Type 2 design is shown on the right.

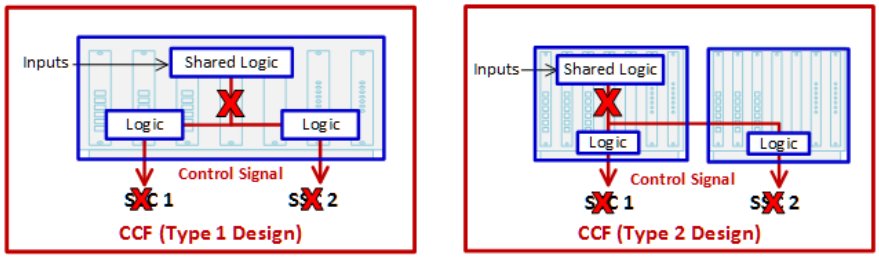


Figure A-5
CCF Caused by a Random Hardware Failure in a Shared Control Signal

A.1.4.1 Measures Intended to Reduce the Likelihood of a CCF of Multiple Controlled SSCs caused by a Random Failure of a Shared Control Signal to Level 2

To reduce the likelihood of a CCF of multiple controlled SSCs caused by a random failure of a shared control signal, applying one of the measures from Table A-7 (or comparable measures) is recommended.

Table A-7
Measures Intended to Reduce the Likelihood of a CCF caused by a Random Failure of a Shared Control Signal to Level 2

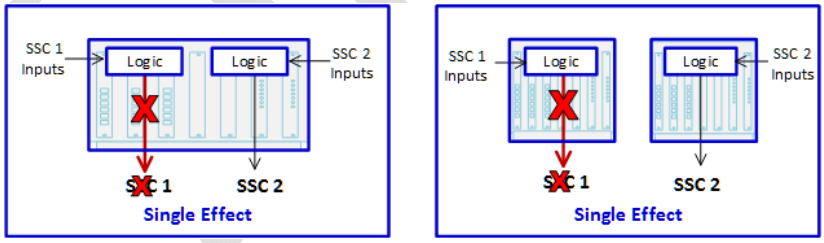
Preventive Measures	
P1	**Provide a dedicated control signal for each SSC, with each control signal provided with its own input sensor(s).** This preventive measure eliminates sharing of any control signals. The figure on the left shows two SSCs in the same controller (a Type 1 design), but each SSC uses its own calculated control signal and associated inputs, so that a random hardware failure (e.g., memory error, I/O processing error, sensor failure) that affects a control signal can only affect one SSC. Likewise, a Type 2 design in the figure on the right yields the same result. The figure on the left shows separate logic for each SSC. However, each separate logic function employs separate memory within the controller. If the same function blocks are employed to execute the logic functions, it is likely that those function blocks can be negatively affected by a random hardware failure in the controller's memory, resulting in a CCF. See Section A.1.8 on controller internal error. 

Table A-7
Measures Intended to Reduce the Likelihood of a CCF caused by a Random Failure of a Shared Control Signal to Level 2

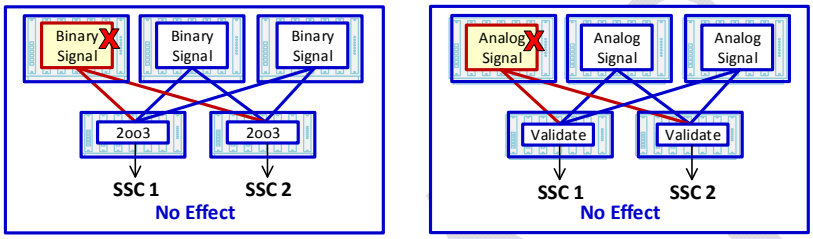
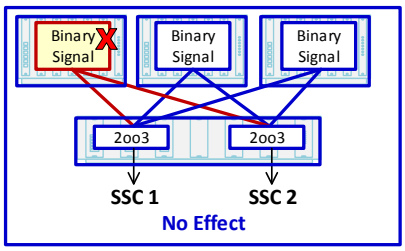
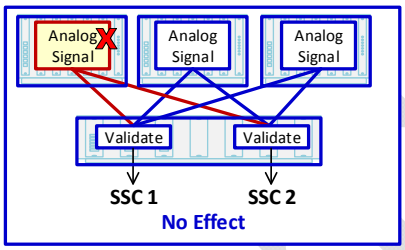
Preventive Measures	
P2	**Calculate the shared control signal in three separate controllers.** The redundant signals are then interfaced to each of the SSCs, with each SSC providing its own 2oo3 voting logic for conventional binary signals, or signal validation (e.g., median select, average of non-deviating control signals) for analog control signals. The figure on the left shows a shared conventional binary control signal being calculated three times, in three separate controllers, then interfaced to a separate two-out-of-three (2oo3) voter for each SSC in a Type 2 design. Likewise, the figure on the right shows a shared analog control signal being calculated three times in three separate controllers, then interfaced with a separate validation feature for each SSC, again in a Type 2 design. In both cases, a random failure of a shared control signal (caused by an internal error in a single controller) results in no effect.  The composed conventional binary and analog control signals originating from three separate controllers in the figures above, could originate from a single controller (i.e., a Type 1 design). However, for that configuration each separate logic function employs separate memory within the controller, and If the same function blocks are employed to execute the logic functions, it is likely that those function blocks can be negatively affected by a random hardware failure in the controller's memory, resulting in a CCF. See Section A.1.8 on controller internal error.

Table A-7 (continued)
Measures Intended to Reduce the Likelihood of a CCF caused by a Random Failure of a Shared Control Signal to Level 2

Preventive Measures	
	The figures below show the same design, except the voters are implemented in a Type 1 design.   If the control signal source is a non-safety controller sending a signal to a safety controller, then the safety controller also complies with guidance for inter-division independence, including communication independence and command prioritization with unalterable program memory (e.g., IEEE 7-4.3.2 in the U.S.). Caution: The Type 1 design figures above show separate 2oo3/validation functions. However, each separate 2oo3/validation function employs separate memory within the controller. If the same function blocks are employed to execute the 2oo3/validation function, it is likely that those function blocks can be negatively affected by a random hardware failure in the controller's memory, resulting in a CCF. See Section A.1.8 on controller internal error.

A.1.4.2 Limiting a CCF Caused by a Random Failure of a Shared Control Signal

To limit the effects of a CCF caused by a shared control signal failure, one of the measures listed in Table A-8 may be helpful.

Table A-8
Measures for Limiting a CCF Caused by a Random Failure of a Shared Control Signal

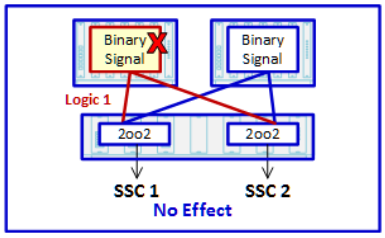
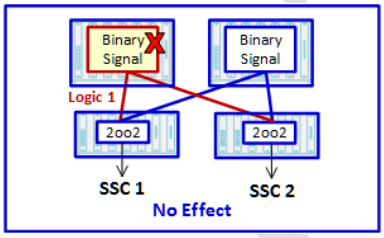
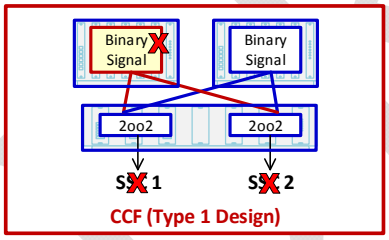
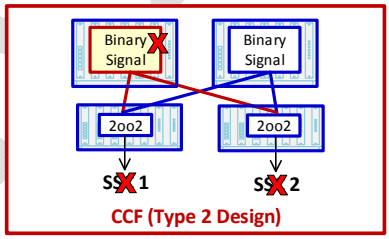
Limiting Measures	
L1	**Calculate conventional binary control signals in two separate controllers, with dedicated voting logic for each SSC, and interface the redundant signals with the dedicated logic.** The voting logic is separate for each SSC to avoid a CCF caused by a failure in the voting output. This design measure prevents a failure mode for only one conventional binary state (0 or 1) of a controller that originates the signals. Therefore, a CCF coping analysis is needed to demonstrate the acceptability of one controller that a) fails to generate a correct signal for the 2oo2 state, or b) erroneously removes the correct signal after the 2oo2 state has been achieved. This limiting measure actually prevents an *unacceptable* CCF (i.e., when the affected SSCs remain in or go to *unacceptable* states). Assuming a logic 1 represents an unacceptable state, the figures below show that there is no CCF if only one controller generates an erroneous logic 1.   On the other hand, an *acceptable* CCF will result if the affected SSCs remain in or go to *acceptable* states. The figure on the left shows an erroneous conventional binary control signal in one controller that is shared with two SSCs, each provided with its own 2oo2 voter implemented in a Type 1 design (both voters and their associated SSCs in one controller). The figure on the right shows an erroneous conventional binary control signal in one controller that is shared with two SSCs, each provided with its own 2oo2 voter implemented in a Type 2 design (a separate controller for each voter and associated SSC). In both cases, the result is a CCF if one controller fails to generate a signal for the desired 2oo2 state, or erroneously removes the correct signal after the desired 2oo2 state has been achieved.   The composed conventional binary control signals originating from two separate controllers in the figures above, could originate from a single controller (i.e., a Type 1 design for the source of the conventional binary signal). However, for a Type 1 design configuration, each separate conventional binary logic function employs separate memory within the controller. If the same function blocks are employed to execute the logic functions, it is likely that those function blocks can be negatively affected by a random hardware failure in the controller's memory, resulting in a CCF. See Section A.1.8 on controller internal error. If the control signal source is a non-safety controller sending a signal to a safety controller, then the safety controller also complies with guidance for inter-division independence, including communication independence and command prioritization with unalterable program memory (e.g., IEEE 7-4.3.2 in the U.S.).

Table A-8 (continued)
Measures for Limiting a CCF Caused by a Random Failure of a Shared Control Signal

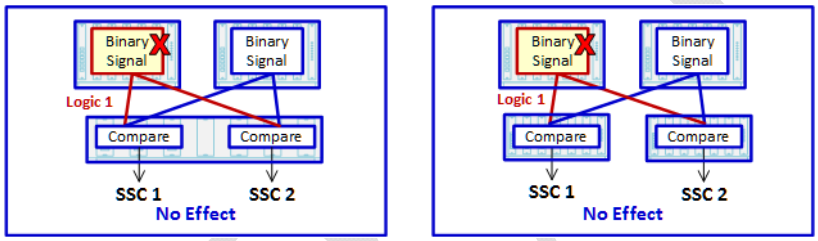
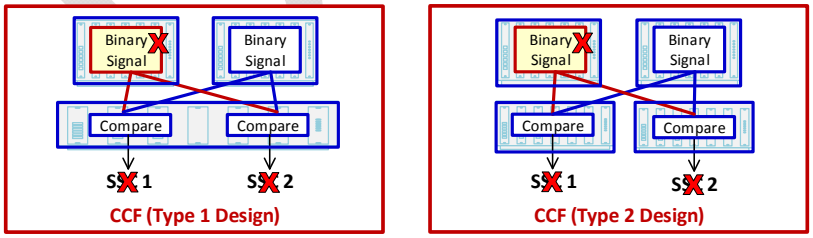
Limiting Measures	
	Caution: In the Type 1 design figures above, each separate 2oo2 function employs separate memory within the shared controller. If the same function blocks are employed to execute the 2oo2 function, it is likely that those function blocks can be negatively affected by a failure in the controller's memory, resulting in a CCF. See Section A.1.8 on controller internal error.
L2	**Calculate conventional binary control signals in two separate controllers with dedicated compare logic for each SSC, and interface the redundant signals with the compare logic.** The compare logic is separate for each SSC to avoid a CCF caused by a failure in the compare logic output. The output of the compare logic changes state only when both signals agree, otherwise the previous state is retained. Therefore, a CCF coping analysis is needed to demonstrate the acceptability of erroneously retaining the previous state, caused by a failure in one of the originating controllers. This limiting measure actually prevents an *unacceptable* CCF (i.e., when the affected SSCs remain in or go to *unacceptable* states). Assuming a logic 1 represents an unacceptable state, the figures below show that there is no CCF if only one controller generates an erroneous logic 1.  On the other hand, an *acceptable* CCF will result if the affected SSCs remain in or go to *acceptable* states. The figure on the left shows an erroneous conventional binary control signal in one controller that is shared with two SSCs, each provided with its own compare function implemented in a Type 1 design (both comparators and their associated SSCs in one controller). The figure on the right shows an erroneous conventional binary control signal in one controller that is shared with two SSCs, each provided with its own comparator implemented in a Type 2 design (a separate controller for each voter and associated SSC). In both cases, the result is a CCF that is erroneously retaining the previous state, caused by a controller failure, when a state change is actually required. 

Table A-8 (continued)
Measures for Limiting a CCF Caused by a Random Failure of a Shared Control Signal

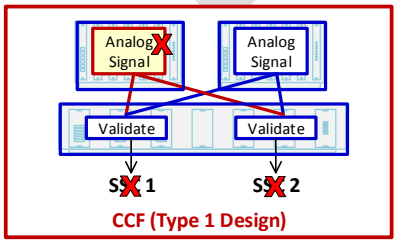
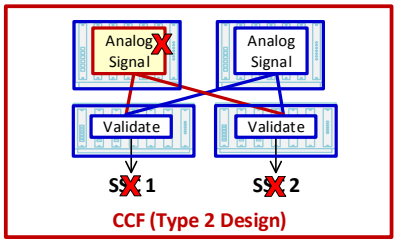
Limiting Measures	
	The composed conventional binary control signals originating from two separate controllers in the figures above, could originate from a single controller (i.e., a Type 1 design for the source of the conventional binary signal). However, for that configuration each separate logic function employs separate memory within the controller. If the same function blocks are employed to execute the logic functions, it is likely that those function blocks can be negatively affected by a random hardware failure in the controller's memory, resulting in a CCF. See Section A.1.8 on controller internal error. If the control signal source is a non-safety controller sending a signal to a safety controller, then the safety controller also complies with guidance for inter-division independence, including communication independence and command prioritization with unalterable program memory (e.g., IEEE 7-4.3.2 in the U.S.). Caution: The Type 1 design figures above show separate compare functions. However, each separate compare function employs separate memory within the controller. If the same function blocks are employed to execute the compare function, it is likely that those function blocks can be negatively affected by a random hardware failure in the controller's memory, resulting in a CCF. See Section A.1.8 on controller internal error.
L3	**Calculate analog control signals in two separate controllers with dedicated validation for each SSC, and separately interface the redundant signals with the dedicated validation for each SSC.** Signal validation is the average of both signals when they are within their specified range and within deviation limits. When signals deviate outside these limits, force the signal validation output to a predetermined state (e.g., hold last good value, fail-high, fail-low). Signal validation is separate for each SSC to avoid a CCF caused by a failure in the signal validation output. These outputs are then propagated through each separate SSC control logic. The figure on the left shows an erroneous analog control signal in one controller that is shared with two SSCs, each provided with its own signal validation SSC implemented in a Type 1 design (both signal validation and their associated SSCs in one controller). The figure on the right shows an erroneous analog control signal in one controller that is shared with two SSCs, each provided with its own validator implemented in a Type 2 design (a separate controller for each validator and associated SSC). In both cases, the result is a CCF because both SSCs are forced to a failed state. But since the failure state is predetermined, the CCF analysis is more manageable. In addition, a control signal failure that results in an unanalyzed CCF can be prevented. For example, if an erroneous high control signal can send two valves open, which is unanalyzed, the validator can be configured to alarm and hold the last good value, when the two control signals deviate. This prevents the CCF that results in unanalyzed erroneous opening of the valves; instead the CCF results in an analyzed condition that can be managed by plant operators through manual control.  

Table A-8 (continued)
Measures for Limiting a CCF Caused by a Random Failure of a Shared Control Signal

Limiting Measures	
	The composed analog control signals originating from two separate controllers in the figures above, could originate from a single controller (i.e., a Type 1 design for the source of the analog signal). However, for that configuration each separate function that produces the analog control signal employs separate memory within the controller. If the same function blocks are employed to execute the control functions, it is likely that those function blocks can be negatively affected by a random hardware failure in the controller's memory, resulting in a CCF. See Section A.1.8 on controller internal error. If the control signal source is a non-safety controller sending a signal to a safety controller, then the safety controller also complies with guidance for inter-division independence, including communication independence and command prioritization with unalterable program memory (e.g., IEEE 7-4.3.2 in the U.S.). Caution: The Type 1 design figures above also show separate validate functions. However, each separate validate function employs separate memory within the controller. If the same function blocks are employed to execute the validate function, it is likely that those function blocks can be negatively affected by a random hardware failure in the controller's memory, resulting in a CCF. See Section A.1.8 on controller internal error.

A.1.4.3 Coping with a CCF Caused by a Failure of a Shared Control Signal with a Predictable State

Limiting Measure L1

L1 is applied when an erroneous signal for one control signal state is unacceptable (e.g., spurious opening of multiple vent valves); L1 prevents that erroneous control action caused by a random hardware failure. However, L1 cannot ensure the control action is correctly generated when required. Therefore, the CCF *coping analysis* would evaluate the plant state(s) for which the correct control action is expected, to provide assurance that concurrent failure of that action for all affected SSCs is acceptable. To credit operator action in the CCF *coping analysis* for L1, the logic would also need to generate a signal mismatch alarm; signal mismatch alarms are discussed for L2 and L3.

Limiting Measure L2

L2 is applied when an erroneous signal for both control signal states is unacceptable (e.g., spurious closing of multiple isolation valves when they should be open, spurious opening of multiple isolation valves when they should be closed); L2 prevents those erroneous control actions caused by a random hardware failure. However, L2 cannot ensure the control actions are correctly generated when required. Therefore, the CCF *coping analysis* would evaluate the plant state(s) for which the correct control actions are expected, to provide assurance that concurrent failures of either action for all affected SSCs is acceptable.

For example, if there is a spurious close signal, normally open isolation valves will not spuriously close because L2 will detect a signal mismatch; and when the valves need to close, they will close because L2 will detect a signal match. However, when the valves need to reopen, they will not, because the original spurious close signal will cause a mismatch.

The compare logic can alarm a mismatch so that operators can take manual actions. Manual actions are possible because the failure effects the controller originating the signal, not the controller that receives the signal and actually controls the SSC, unless the input supports an equipment protection interlock that blocks component repositioning. The CCF *coping analysis* would demonstrate the operator's ability to recognize the undesirable condition, and take the appropriate actions, using HFE analysis methods (e.g., in the U.S., NUREG-0800 Appendix 18-A provides a method for crediting manual operator actions for mitigating transients with a concurrent CCF in the plant safety system).

Limiting Measure L3

If L3 is applied (signal validation), the signal validation output can be the last good signal validation output value (i.e., when there was no unacceptable signal deviation), or a predetermined default value, that is then propagated through the SSC's control algorithm. The resulting effect on the controller's outputs are dependent on the control algorithm. The CCF *coping analysis* is limited to demonstrating that operators will be notified of this condition through a signal deviation alarm, and that they can manage the condition until the failed component(s) can be restored, without creating a transient. Since the alarms prompt operators to monitor the condition, they would be expected to detect an unacceptable trend and reduce the likelihood of the occurrence of a plant transient. With a failed control signal input, operators can still control the affected plant components manually, unless the input supports an equipment protection interlock that blocks component repositioning.

A.1.5 Random Hardware Failure in a Shared Network or Data Link

This section applies to designs that would provide a shared data network or a shared data link that interconnect two or more controllers. A random failure of a shared network or data link can produce any of the following conditions:

Condition 1 Loss of all data
Condition 2 Data storm (or broadcast storm)
Condition 3 Erroneous Data

For all communication interfaces described below, if the communication is inter-divisional (between non-safety and safety, or two safety divisions), then the safety controller(s) also complies with guidance for inter-division independence, including communication independence and command prioritization with unalterable program memory (e.g. IEEE 7-4.3.2 in the U.S.).

A.1.5.1 Shared Network Condition 1 (Loss of All Data)

For Condition 1, all SSCs that rely on the digital communication interface for control input signals lose those control signals. Loss of the control signals may occur caused by complete data communication interface failure, a frozen data bit, or persistent communication errors that cause recurring rejection of data messages. Figure A-6 illustrates two examples of a shared network or datalink that could lead to a CCF of two SSCs that rely on a digital communication interface for input signals.

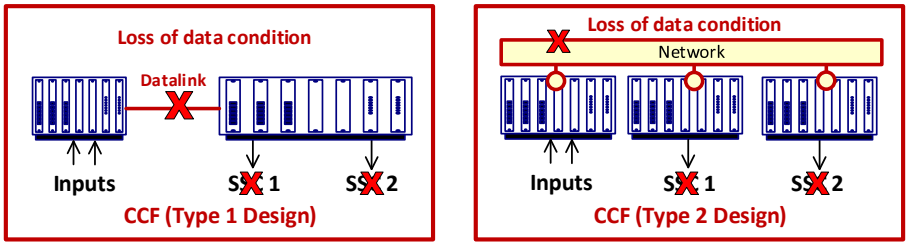


Figure A-6
CCF Caused by Condition 1 (Loss of All Data)

Measures Intended to Reduce the Likelihood of a CCF Caused by Shared Network Condition 1 (Loss of All Data) to Level 2

To reduce the likelihood of a CCF of multiple controlled SSCs caused by Condition 1, applying one of the measures from Table A-9 (or comparable measures) is recommended.

Table A-9
Measures Intended to Reduce the Likelihood of a CCF caused by Loss of Data on a Shared Network or Datalink to Level 2

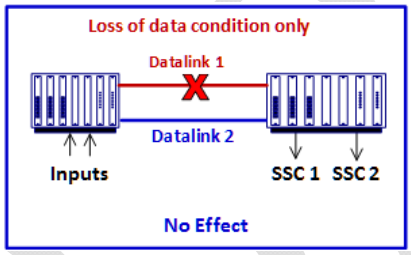
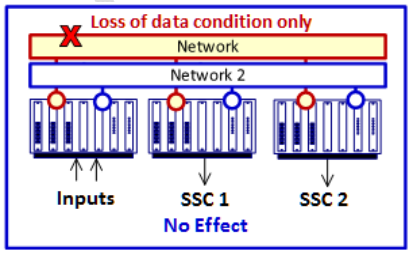
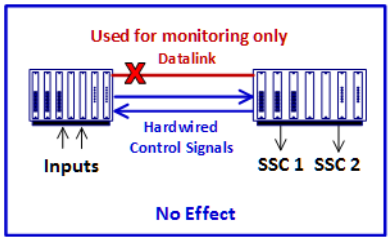
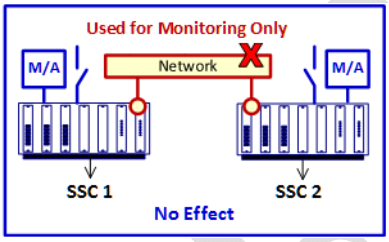
Preventive Measures	
P1	**Provide redundant data communication interfaces for control signals.** Design the data communications so that there is no active component failure that can cause loss of data on both interfaces. Provide a documented failure modes and effects analysis for all active data communication components. For example, the figures below show two methods for providing redundant data communication interfaces, and an FMEA shows that a random failure of any active data communication component does not result in loss of the data communication functions.   <u>Caution:</u> Communication interfaces whose data remains in the same state for extended time durations, can fail in a non-announcing as-is mode (i.e., frozen data bits). To provide assurance that this failure is detectable, and thereby reduce the likelihood of single communication interface failures from accumulating over time to become a redundant communication interface failure, the data is periodically tested/cycled to force data bit state changes; testing may be manual or automatic. The typical self-diagnostics provided with data communication interfaces, such as CRC and other data validity checks, are not sufficient to detect frozen data bits. In addition, for many applications it is not adequate (i.e., too late) to detect frozen bits when there is a demand for their state change.

Table A-9 (continued)
Measures Intended to Reduce the Likelihood of a CCF caused by Loss of Data on a Shared Network or Datalink to Level 2

Preventive Measures	
P2	**Provide hardwired control signals**. Data communications may be used for other purposes, but not for control signals. For example, the figure on the left shows a shared datalink, but the control signals necessary for any SSC are hardwired (in this case, between controllers); the network is used only for monitoring. Likewise, the figure on the right shows a shared network, but operator control signals are hardwired for each SSC (in this case, dedicated switches and/or manual/auto (M/A) stations for each SSC). In both cases, a random failure of the digital communication interface that creates a loss of data condition results in no effect on any control functions.   Caution: 1. Hardwired control signal schemes should be assessed for their reliability. With continuous self-testing and redundancy, the expected network reliability is typically better than hardwired reliability. 2. When hardwiring control signals using I/O modules, if a single I/O module is used for multiple signals, or multiple CPE, a failure of that I/O module can cause a CCF (see Tables A-4 and A-6 for preventive measures associated with input processing and output modules, respectively).

Limiting a CCF Caused by Shared Network Condition 1 (Loss of All Data)

If no preventive measures listed in Table A-9 are implemented, or if one is only partially implemented, then one of the limiting measures listed in Table A-10 may be helpful.

Table A-10
Measures for Limiting a CCF Caused by Loss of Data on a Shared Network or Datalink

Limiting Measures	
L1	**Define controller reaction to loss of control signal data in the application program.** One method is to set a failed control signal input to low, high, or the last good value prior to the loss of data. Also, demonstrate that the failed communication interface is detectable, or that undetected frozen data is acceptable.

Coping with a CCF Caused by Shared Network Condition 1 (Loss of All Data)

For limiting measure L1, the last good control signal value, or a predetermined default value, is propagated through each SSC's control algorithm. The resulting effects on the controller's outputs are dependent on the control algorithms. The CCF *coping analysis* is limited to demonstrating that operators will be notified of this condition through an interface communication failure alarm, and that they can manage the condition until the failed component(s) can be restored, without creating a transient.

For a failed communication interface that results in loss of automatic control signals, since operators are monitoring the condition, they can detect an unacceptable trend and can reduce the likelihood of the occurrence of a plant transient. With a failed control signal input, operators can still control the affected plant components manually, unless the input supports an equipment protection interlock that blocks component repositioning.

For a failed communication interface that results in loss of the operator's ability to take manual control actions or make auto/manual mode changes or automatic mode setpoint changes, the CCF *coping analysis* must demonstrate that the affected SSCs will operate successfully for the expected plant modes with no operator input. Alternately, the CCF *coping analysis* demonstrates that operators can manage the CCF with other plant components.

For a failed communication interface that is undetectable (e.g., frozen data bits), the CCF *coping analysis* demonstrates that the current state of the affected SSCs is acceptable for all plant modes.

A.1.5.2 Shared Network Condition 2 (Data Storm)

For Condition 2, data can be lost (as in Condition 1), or data can be unpredictably delayed. In addition, a controller can get overloaded in trying to keep up with the data overload. The result is unpredictable erroneous controller behavior, even if the controller does not rely on the data communications interface for control signals. Figure A-7 illustrates examples of a data storm on a shared network communication interface that leads to a CCF.

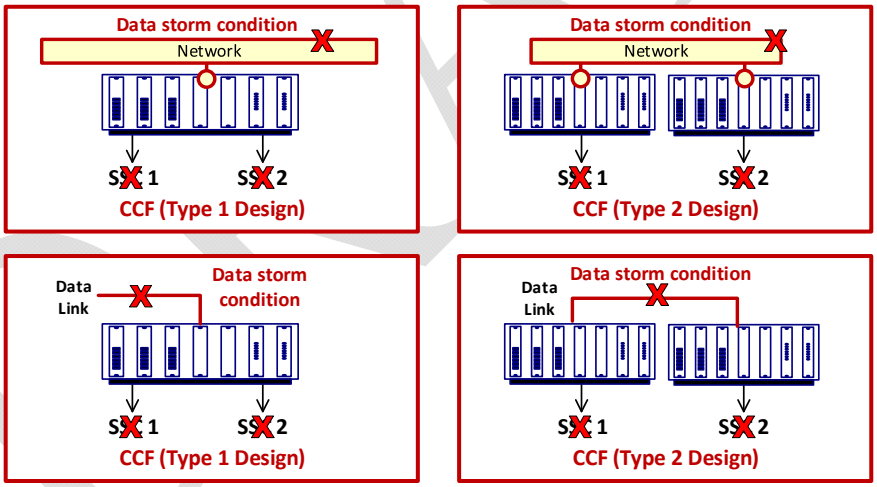


Figure A-7
CCF Caused by Condition 2 (Data Storm)

Measures Intended to Reduce the Likelihood of a CCF Caused by Shared Network Condition 2 (Data Storm) on a Communication Interface to Level 2

To reduce the likelihood of a CCF of multiple controlled SSCs caused by Condition 2, applying one of the measures from Table A-11 (or comparable measures) is recommended.

Table A-11
Measures Intended to Reduce the Likelihood of a CCF caused by a Data Storm on a Shared Network Interface to Level 2

Preventive Measures	
P1	**Provide separate and redundant transmit and receive data communication processors with multiple measures:** 1. Each transmit and receive interface has its own communications processor that functions with its own deterministic cycle independently and asynchronously from the function processor of each controller. Separate transmit communication processors provide assurance that if the function processor initiates a data storm, the data storm is not propagated by both of the redundant transmit communication processors, thereby avoiding a loss of all communication data. Separate receive communication processors to provide assurance that a data storm on either receive interface, may cause erratic operation of one receive communication processor, but the data storm will not propagate to negatively affect the deterministic operation of the function processor or the other redundant communication interface. Transmit and receive communication processors can be combined for the same communication interface, but they are independent from the function processor and from the second redundant communication interface. To facilitate independent asynchronous operation of all processors, the communication processors (both send and receive) and function processors exchange data via shared memory with memory arbitration circuits that provide assurance of deterministic function processing. In the U.S., refer to IEEE 7-4.3.2 for additional detail for the items listed above, regarding communication independence between function processors and communication processors.

Table A-11 (continued)
Measures Intended to Reduce the Likelihood of a CCF caused by a Data Storm on a Shared Network Interface to Level 2

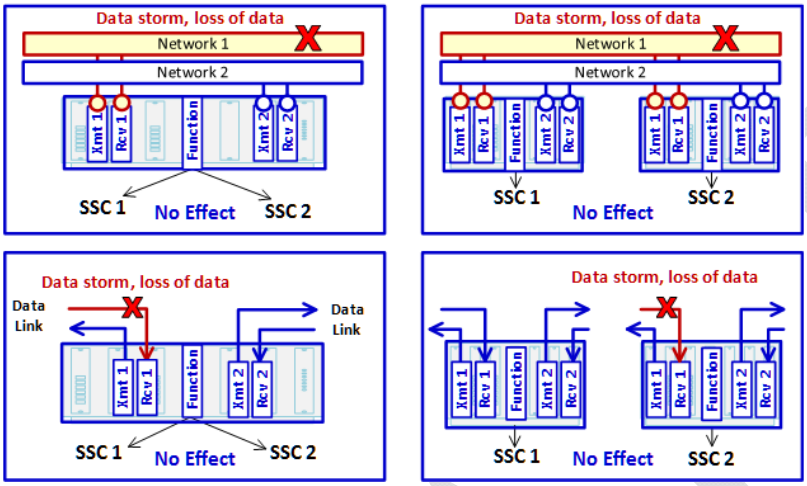
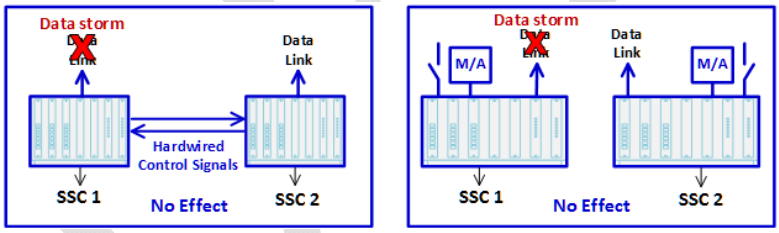
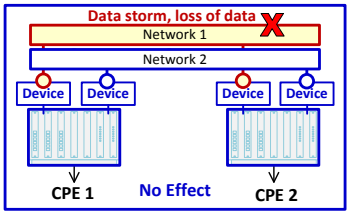
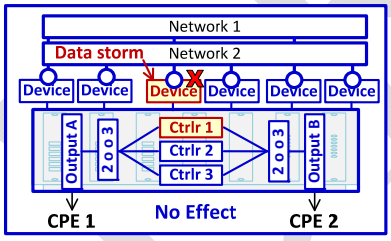
Preventive Measures	
	The figures below show examples of this preventive measure, one in a Type 1 design (two SSCs on one controller) and one in a Type 2 design (each SSC on a separate controller). 
P2	**Provide a data link with unidirectional communication for monitoring data, and hardwire all control signals.** The unidirectional method is broadcast only, with no bidirectional communication handshaking. The figures below show two examples of this preventive measure, one with control signals hardwired between controllers, and one with switches and M/A stations dedicated to each controller. Note that this design also results in no loss of data from each controller to other controllers.  <u>Caution:</u> Hardwiring control signals alone is not a preventive measure for this failure, because even if the communication interface is used only for monitoring data, with data communication that requires bidirectional handshaking, a data storm can still cause a function processor overload that can result in erroneous control function execution. Since this method does not permit data communication handshaking, it provides a broadcast data link; a shared network cannot be used.

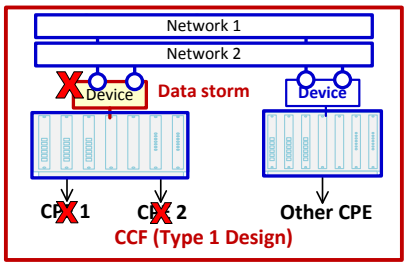
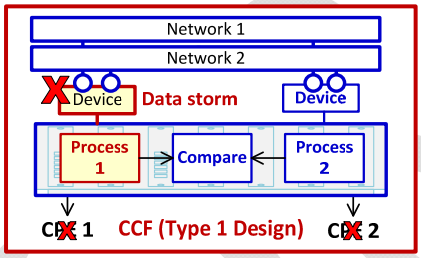
Table A-11 (continued)
Measures Intended to Reduce the Likelihood of a CCF caused by a Data Storm on a Shared Network Interface to Level 2

Preventive Measures	
P3	**Provide redundant network interfaces and a dedicated throttling device for each SSC.** A design evaluation and documented test results provide evidence that the throttling device prevents a data storm originating from a network device or from a controller on the network from propagating through the network to other controllers. The figure below shows an example of this preventive measure in a Type 2 design (each SSC on a separate controller).  Caution: 1. The throttling device itself can be the source of a data storm that overwhelms its connected controller. Therefore, this defensive measure prevents the CCF for a Type 2 design. 2. Note that this preventive measure does not reduce the likelihood of a CCF for a controller with a Type 1 design (multiple SSCs on one controller), because there is no shared memory between the function processor and the throttling device, forcing the function processor to still perform communication handshaking. Therefore, a data storm from the throttling device would negatively affect all SSCs controlled by its single connected controller. To make use of a preventive measure intended to reduce the likelihood of a CCF for a controller controlling multiple SSCs (Type 1 design), provide a controller with triplex redundancy with a separate throttling device for each redundancy. The triplex 2oo3 output voting will block erroneous signals from any single redundancy negatively affected by the data storm from its own throttling device. The figure below illustrates this concept. 

Limiting a CCF Caused by Shared Network Condition 2 (Data Storm)

If no preventive measures provided above are implemented, or if one is only partially implemented, one of the limiting measures listed in Table A-12 may be helpful.

Table A-12
Measures for Limiting a CCF Caused by a Data Storm on a Shared Network Interface

Limiting Measures	
L1	**Provide redundant network interfaces and a dedicated throttling device for each controller.** For a Type 1 design this measure prevents all controller failures caused by a data storm originating on the network. But a data storm originating in a throttling device could negatively affect the one controller to which that throttling device is connected. For a Type 1 design (multiple SSCs on one controller), all SSCs controlled by that controller would be negatively affected, as in the figure below. Note, that since the controller is negatively affected by a data storm from the throttling device, there is no benefit in providing redundant throttling device s for this configuration. 
L2	**Same as A11-P3 but for a controller that controls multiple SSCs**. Use a separate throttling device for each communication interface on each controller of a duplex configuration with an output compare function. This provides assurance that a data storm from a throttling device will not propagate to affect both controllers of the duplex configuration. But since there is no shared memory between the function processor and the throttling device, the function processor must still perform communication handshaking. Therefore, a data storm created by the throttling device can still affect the connected controller, but the potential control anomaly for multiple SSCs is limited to a controller shutdown (i.e., not spurious control actions) by the output compare function. 

Coping with a CCF Caused by Shared Network Condition 2 (Data Storm)

If a controller does not protect itself against a data storm, the erroneous control function response is not predictable. Limiting measure L1 can limit the data storm to affecting a single controller, but it cannot eliminate the effect on multiple SSCs on that controller (i.e., a Type 1 design).

The CCF *coping analysis* would need to demonstrate that operators would recognize the erroneous control function operation, and that they can manage the condition to reduce the likelihood of a plant transient caused by the data storm. Since alarms from the affected controller cannot be credited for this condition, operators may not be able to detect an unacceptable trend or reduce the likelihood of a plant transient.

It is noted that when a controller does not protect itself against a data storm both automatic and manual control are negatively affected for the controlled components (there are exceptions with unique designs). In addition, the alarms and indications generated by the controller are negatively affected. Therefore, this CCF analysis demonstrates coping with other plant instrumentation and components, not the ones monitored or controlled by the affected controller.

Since the failure can occur at any time, the analysis evaluates stable as well as transient plant conditions, including startup, shutdown and accidents. One acceptable coping method to reduce the likelihood of an unanalyzed condition may be for the operator to manually trip the plant or manually initiate a controlled shutdown, if an undesirable trend can be detected.

Limiting measure L2 simplifies the *coping analysis* by ensuring a data storm forces the SSCs to a predictable state.

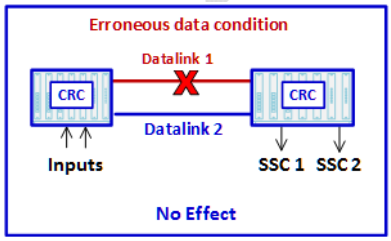
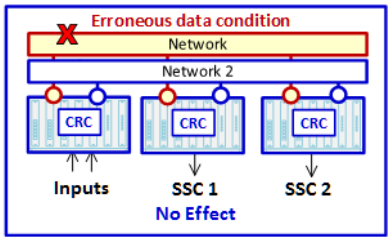
A.1.5.3 Shared Network Condition 3 (Erroneous Data)

Condition 3 pertains to erroneous data generated by the communication interface itself (e.g., communication interface modules, throttling devices, media converters), not by a controller that uses the communication interface. Erroneous data generated by a controller that uses the communication interface is addressed in Section A.1.8 on controller internal error. Erroneous data generated by the communication interface itself is detected and a CCF prevented as described below.

Measures Intended to Reduce the Likelihood of a CCF Caused by Shared Network Condition 3 (Erroneous Data) to Level 2

To reduce the likelihood of a CCF of multiple controlled SSCs caused by Condition 3, applying one of the measures from Table A-13 (or comparable measures) is recommended.

Table A-13
Measures Intended to Reduce the Likelihood of a CCF Caused by Erroneous Data on a Shared Network or Datalink to Level 2

Preventive Measures	
P1	**Same as A9-P1 for loss of data, plus the controller provides a data validity frame (e.g., CRC) to each data message when the message is created**. This is different than the validity frame that may be created by the network communication interface itself, because that interface could be the source of the erroneous data, and therefore would create a corresponding correct validity frame for the erroneous data that it creates (e.g., a correct CRC, but for erroneous data). The data validity frame created by the transmitting controller is checked by the receiving controller to reject erroneous data. Since the failure affects only one of the two redundant communication interfaces, erroneous data is prevented from being received by the receiving controller, and valid data is transmitted via the second communication interface. For example, the figures below show a data message with a CRC frame originating in one controller, which is received by one or more additional controllers provided with the same CRC algorithm. If a random hardware failure in the data link or network causes an erroneous data message, the receiving controller(s) will reject it and process the good data from the redundant data link or network.  
P2	**Same as A9-P2 for loss of data.** Data communications may be used for other purposes, but not for control signals.

Limiting a CCF Caused by Shared Network Condition 3 (Erroneous Data)

To limit the effects of a CCF caused by Condition 3, one of the limiting measures listed in Table A-14 may be helpful.

Table A-14
Measures for Limiting a CCF Caused by Erroneous Data on a Shared Network Interface

Limiting Measures	
L1	**Provide a non-redundant communication interface for each controller, with the data validity measures described for A13-P1**. Since this defensive measure does not include a redundant communication interface to provide assurance that valid data is received, provide a watch dog timer that checks that valid data is received within a predetermined time out; this can be after successive multiple invalid data rejections. In addition, provide a predetermined failure state for the data when the watch dog time out occurs (e.g., last good value, fail-high, fail-low) and a CCF coping analysis for that condition for all affected SSCs. The watchdog timer has no reliance on the messages from the other network nodes.

Coping with a CCF Caused by Erroneous Data on a Shared Network

Limiting measure L1 simplifies the *coping analysis* by ensuring erroneous data forces the SSCs to a predictable state, such that the resulting effects on the plant can be analyzed.

A.1.6 Random Hardware Failure in a Shared Operator Workstation

This section applies to any operator workstation with soft controls, including workstations that can send soft control commands to controllers within the same division (safety or non-safety) as well as workstations that can send control commands to multiple safety and/or non-safety divisions. A random failure of a shared operator workstation can lead to:

Condition 1 Loss of view or manual control capability for multiple SSCs
Condition 2 Erroneous control commands or bypass commands for multiple SSCs

A.1.6.1 Shared Operator Workstation Condition 1 (Loss of View or Manual Control)

Loss of view or manual control capability (Condition 1) includes the inability to:

- change manual/auto modes
- adjust automatic control setpoints
- make manual adjustments to controller outputs
- change component states (e.g., open/close a valve, start/stop a pump)

Figure A-8 illustrates examples of CCFs caused by Condition 1. In this case, the controllers are still functioning, but when an operator attempts manual action of SSC in response to a plant condition, the workstation does not generate any commands to the controller.

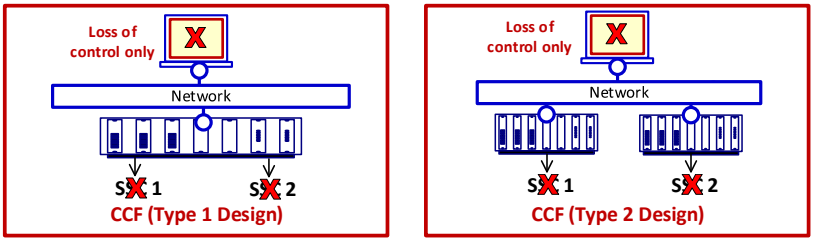


Figure A-8
Loss of Control Caused by a Random Failure of a Shared Operator Workstation

Measures Intended to Reduce the Likelihood of a CCF caused by Loss of Control from a random Failure of a Shared Operator Workstation to Level 2

To reduce the likelihood of a CCF of multiple controlled SSCs caused by a loss of control from a random failure of a shared operator workstations, applying one of the measures from Table A-15 (or comparable measures) is recommended.

Table A-15
Measures Intended to Reduce the Likelihood of a CCF caused by Loss of Control from a Random Failure of a Shared Operator Workstation to Level 2

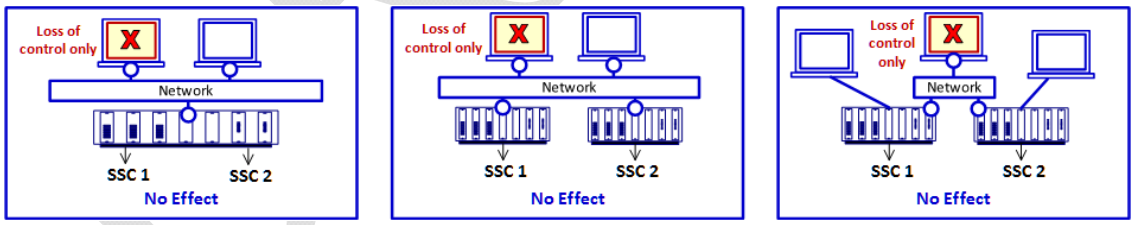
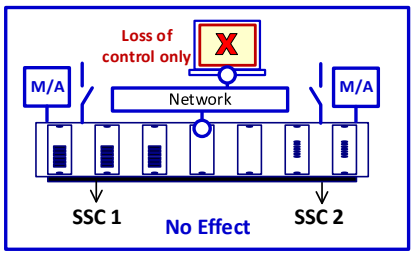
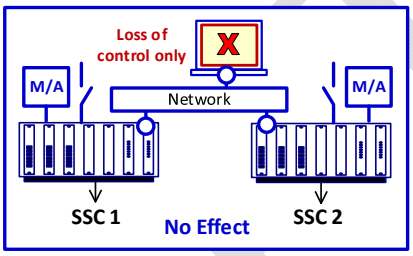
Preventive Measures	
P1	**Provide the same soft control capability from multiple operator workstations.** For safety divisions, backup operator workstations are Class 1E in the U.S. (or equivalent), including equipment qualification, compliance to safety critical life cycle processes, and residing in each separate safety division for compliance to the single failure criterion. For non-safety functions with multiple workstations this measure assumes that multiple workstations are not also susceptible to a single failure, such as a shared power source (see Section A.1 for guidance on measures intended to reduce the likelihood of CCFs due to shared resources to Level 2)The figures below illustrate this preventive measure; the left and middle figures illustrate an implementation in a non-safety system, the figure on the right illustrates an implementation in a safety system (with a separate backup HSI for each division):  <u>Caution:</u> 1. For non-safety systems, multiple workstations may be susceptible to a random hardware failure, such as a shared power source (see Section A.1 for guidance on measures intended to reduce the likelihood of CCFs caused by random hardware failures in shared resources to Level 2). Soft control interfaces that normally remain in the same state for extended time durations, can fail in a non-announcing as-is mode. To provide assurance that such a failure is detectable, and thereby reduce the likelihood of single failures from accumulating over time such that they generate CCFs, the soft control interface is periodically tested/cycled to force state changes. The typical self-diagnostics provided with operator workstations are not sufficient to detect frozen or unresponsive soft control targets.

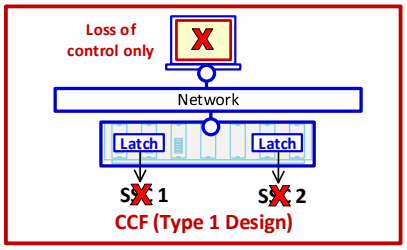
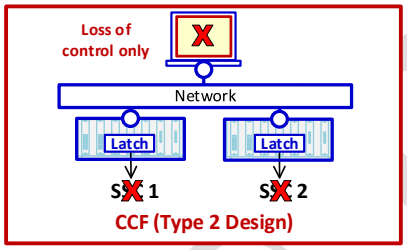
Table A-15 (continued)
Measures Intended to Reduce the Likelihood of a CCF caused by Loss of Control from a Random Failure of a Shared Operator Workstation to Level 2

Preventive Measures	
P2	**Duplicate the soft control capability of the operator workstation on conventional control stations for each SSC.** Conventional control stations include Auto/Manual devices and/or hand switches. For safety divisions the backup HSI is Class 1E in the U.S. (or equivalent), including equipment qualification, compliance to safety critical life cycle processes, and residing in each separate safety division for compliance to the single failure criterion. This measure assumes that multiple workstations are not also susceptible to a single failure, such as a shared power source (see Section A.1 for guidance on measures intended to reduce the likelihood of CCFs due to shared resources to Level 2). The figures below illustrate this preventive measure:   Caution: 1. For non-safety systems, multiple workstations may be susceptible to a random hardware failure, such as a shared power source (see Section A.1 for guidance on measures intended to reduce the likelihood of CCFs caused by random hardware failures in shared resources to Level 2). 2. Soft control interfaces that normally remain in the same state for extended time durations, can fail in a non-announcing as-is mode. To provide assurance that such a random hardware failure is detectable, and thereby reduce the likelihood of random hardware failures accumulating over time so that multiple separate random hardware failures become CCFs, the soft control interface is periodically tested/cycled to force state changes. The ability to force state changes should be carefully evaluated to provide assurance that there are no adverse effects on any SSC. The typical self-diagnostics provided with operator workstations are not sufficient to detect frozen or unresponsive soft control targets

Limiting a CCF Caused by a Loss of Control from a Random Failure of a Shared Operator Workstation

If none of the preventive measures provided above are implemented, or if one is only partially implemented, then one of the limiting measures listed in Table A-16 may be helpful.

Table A-16
Measures for Limiting a CCF Caused by Loss of Control from a Random Failure of a Shared Operator Workstation

Limiting Measures	
L1	**Provide assurance that that all signals from the workstation are momentary and latched in the controller (i.e., there are no latched signals in the operator workstation), such that failure of the operator workstation has no impact on the current state of the controllers.**   Provide a CCF coping analysis to demonstrate that the current state of the controllers will not cause an unacceptable CCF for a broad sampling of plant modes and transient conditions, and that the state of the affected SSCs does not require changes by the operator for accident mitigation or safe shutdown. Caution: Many safety components in auxiliary systems such as HVAC and CCW require no manual control for accident mitigation and safe shutdown; regardless, demonstrating that manual control of safety components is not needed (and therefore, safety HSI is not needed) may be contrary to regulatory guidance which states that backup safety HSI should be provided for all safety plant components (e.g., IEEE7-4.3.2 in the U.S.).

A.1.6.2 Shared Operator Workstation Condition 2 (Erroneous Commands)

Erroneous control commands or bypass commands can cause spurious operation of multiple SSCs, such as:

- spuriously changing manual/auto modes
- spuriously changing automatic control setpoints
- spuriously changing controller analog outputs (e.g., 4-20 mADC signals)
- spuriously blocking automatic safety functions
- spuriously changing component states (e.g., open/close a valve, start/stop a pump)

Figure A-9 illustrates examples of CCFs caused by Condition 2 (erroneous control command or erroneous bypass command).

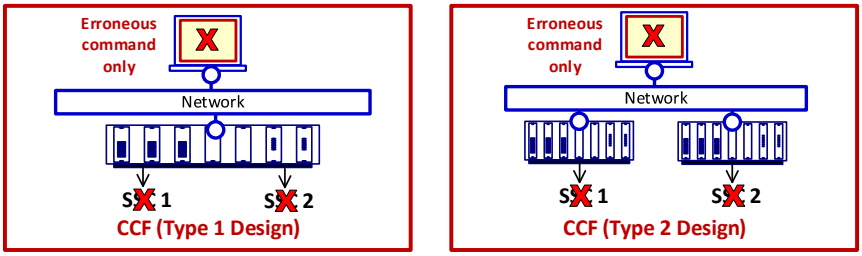


Figure A-9
Erroneous Commands Caused by a Random Failure of a Shared Operator Workstation

Measures Intended to Reduce the Likelihood of a CCF caused by Erroneous Commands from a Random Failure of a Shared Operator Workstation to Level 2

An erroneous command is one that is counter to the command expected by the operator (e.g., the operator selects an "open" command, but the workstation issues an erroneous "close" command)

To reduce the likelihood of a CCF caused by erroneous commands from a random failure of a shared operator workstation, applying one of the measures from Table A-17 (or comparable measures) is recommended.

Table A-17
Measures Intended to Reduce the Likelihood of a CCF caused by Erroneous Commands from a Random Failure of a Shared Operator Workstation to Level 2

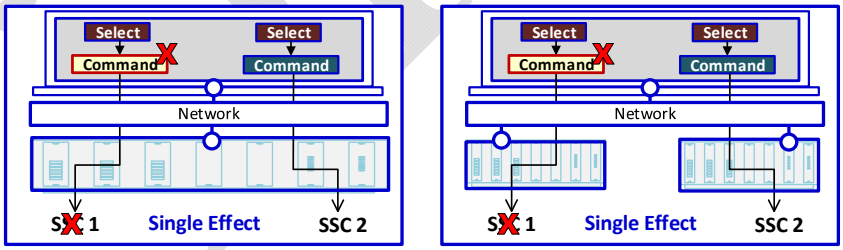
Preventive Measures	
P1	**Provide two distinct operator actions to issue control commands to provide assurance that that one or more erroneous commands to multiple SSCs are not issued from any shared workstation, and provide multiple additional measures.** An example of two distinct operator actions could be a component/SSC *selection* followed by an open/close *command;* both actions are required to generate a control command message. Provide the following additional measures: 1. The workstation is tested for durability to the same environmental qualification levels (e.g., temperature) as safety equipment to minimize the potential for spurious signals 2. Each SSC has its own selection and command controls  Although this measure prevents a CCF, it credits features of the workstation that are also the potential source of the CCF. Therefore, a coping analysis should determine the acceptability of a CCF in the event of multiple spurious commands. Since this P measure prevents the CCF, this coping analysis is an optional defense-in-depth measure that employs "best estimate" methods; refer to Section 3.4 for guidance on conducting this coping analysis.

Table A-17 (continued)
Measures Intended to Reduce the Likelihood of a CCF caused by Erroneous Commands from a Random Failure of a Shared Operator Workstation to Level 2

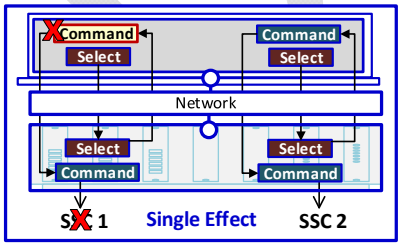
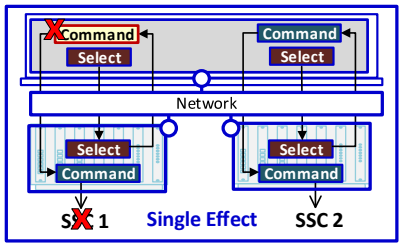
Preventive Measures	
	If this method is applied to a non-safety workstation that can send control commands to a safety controller, then the safety controller provides assurance that its own data communication independence (reference IEEE 7-4.3.2 in the U.S.), including all of the following additional measures: 3. Unalterable program memory (hardware protected) that is changeable only by removal from the controller. 4. Priority logic to ensure the safety function determines when mode/bypass changes are permitted (e.g., interlocks between divisions that allow only one division to have a maintenance bypass for the same safety function at any one time, interlocks that determine when operating bypasses can be accepted and are automatically removed) 5. Priority logic to ensure safety function commands (e.g., ESF actuation and interlocks) block non-safety commands that are opposite to the safety function commands (e.g., open vs. close, start vs. stop).
P2	**Provide three-way messaging between workstations and controllers to provide assurance that one or more erroneous commands to multiple SSCs are not issued from any shared workstation, and provide multiple additional measures.** 1. Three-way messaging consists of: a. the controller receives two distinct messages from the operator workstation for each control command (e.g., component selection followed by open/close command) b. the operator workstation cannot generate the second message (command) until it receives acknowledgement of the first message (select) from the controller c. the controller will not generate the acknowledgment or accept the second message unless it has distinctly received the first message by itself (i.e., without the second message) 2. Each SSC has its own selection and command controls 3. the workstation is tested to the same environmental qualification levels as safety equipment to minimize the potential for spurious signals This measure prevents a CCF through features of the workstation and diverse features of the controller; therefore, a CCF coping analysis is not applicable, as it is for P1. The following figures illustrate this preventive measure:  

Table A-17 (continued)
Measures Intended to Reduce the Likelihood of a CCF caused by Erroneous Commands from a Random Failure of a Shared Operator Workstation to Level 2

Preventive Measures	
	If this method is applied to a non-safety workstation that can send control commands to a safety controller, then the safety controller provides assurance that its own data communication independence (reference IEEE 7-4.3.2 in the U.S.), including all of the following additional measures: 4. Unalterable program memory (hardware protected) that is changeable only by removal from the controller. 5. Priority logic to ensure the safety function determines when mode/bypass changes are permitted (e.g., interlocks between divisions that allow only one division to have a maintenance bypass for the same safety function at any one time, interlocks that determine when operating bypasses can be accepted and are automatically removed) 6. Priority logic to ensure safety function commands (e.g., ESF actuation and interlocks) block non-safety commands that are opposite to the safety function commands (e.g., open vs. close, start vs. stop).

The preventive measures provided in Table A-17 were developed with the intent to reduce the likelihood of multiple erroneous commands to multiple SSCs to Level 2. However, they cannot reach Level 2 for single or multiple erroneous commands (e.g., successive commands) to an SSC, because after the SSC is selected, the workstation can send one or more erroneous commands, regardless of the command that may have been initiated by the operator. For example, after selecting a specific valve for control, the operator touches the OPEN soft control, but the workstation erroneously sends CLOSE. Or, after selecting a specific valve for control, the operator initiates nothing (i.e., he or she is still thinking), but the workstation sends an erroneous command to the selected SSC.

It is noted that these methods can be credited for measures intended to reduce the likelihood of multiple spurious commands to multiple SSCs to Level 2; they are not credited with reaching Level 2 for a single spurious command. Therefore, if multiple SSCs are normally controlled by a single command (e.g., system level actuation command), then a CCF coping analysis might be used to demonstrate the acceptability of spurious command.

Limiting a CCF Caused by Erroneous Command from a Random Failure of a Shared Operator Workstation

If none of the preventive measures provided above are implemented, or if one is only partially implemented, then one of the limiting measures listed in Table A-18 may be helpful.

The limiting measures provided in Table A-18 are intended to reduce the likelihood of multiple erroneous commands to multiple SSCs to Level 2. However, they do not reach Level 2 for a single or multiple erroneous commands (e.g., successive commands) to a group of SSCs, because after the SSC group is selected or enabled, the workstation can send one or more erroneous commands, regardless of the command that may have been initiated by the operator. For example, after selecting a specific group of valves for control, the operator touches the OPEN soft control, but the workstation erroneously sends CLOSE. Or, after selecting a specific group of valves for control, the operator initiates nothing (i.e., he or she is still thinking), but the workstation sends an erroneous command to the selected group of valves.

Table A-18
Measures for Limiting a CCF Caused by Erroneous Commands from a Random Failure of a Shared Operator Workstation

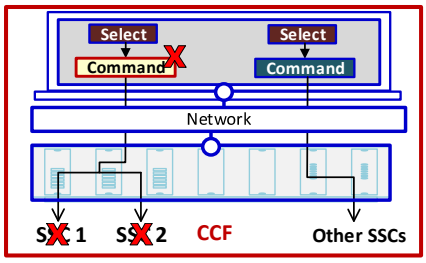
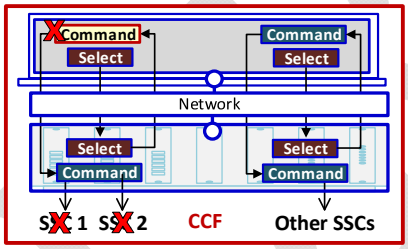
Limiting Measures	
L1	**Provide the same measures as A17-P1, but for a selection that enables multiple SSCs, such as for system or subsystem level controls.** Examples of system or subsystem level controls include boration initiation, condensate system initiation, movement of a control rod group, etc. For this case one or more erroneous commands cannot be prevented to the SSCs that are enabled by the selection. However, the CCF is limited to the multiple SSCs within the selection group. The following figures illustrate this limiting measure:  As for P1, an optional CCF coping analysis is recommended for erroneous commands to multiple groups of SSCs
L2	**Provide the same measures as A17-P2, but for a selection that enables multiple SSCs, such as for system or subsystem level controls.** Examples of system or subsystem level controls include boration initiation, condensate flow, movement of a control rod group, etc. For this case one or more erroneous commands cannot be prevented to the SSCs that are enabled by the selection. However, the CCF is limited to the multiple SSCs within the selection group. The following figure illustrates this limiting measure: 

Table A-18 (continued)
Measures for Limiting a CCF Caused by Erroneous Commands from a Random Failure of a Shared Operator Workstation

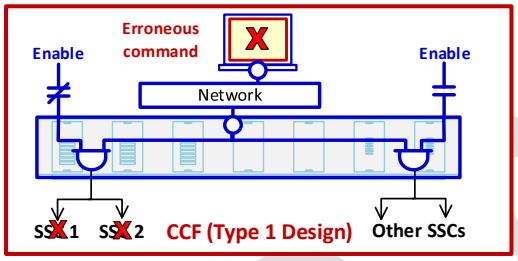
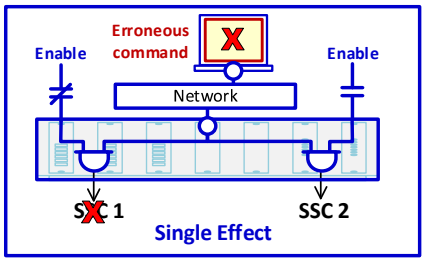
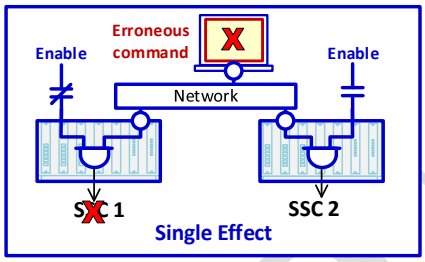
Limiting Measures	
L3	**Supplement the workstation with conventional "enable switches" that interface directly to the controllers to enable them to receive commands from the workstation, such that the controllers will ignore any workstation commands (valid or erroneous) unless an enable switch has been activated.** Provide a dedicated set of enable switches for each workstation The segmentation of SSCs into functional groups affected by any one "enable switch" limits the CCF. A dedicated set of enable switches for each workstation prevents any single switch from becoming a source of CCF for the affected SSCs. For example, there could be separate "enable switches" for reactor coolant system controls, steam generator controls, turbine controls, safety division A controls, safety division B controls, etc. When there is no "enable switch" activated, no SSCs are affected by any workstation commands (valid or erroneous). When an "enable switch" is activated the potential SSCs that could be affected by erroneous commands are limited to those within the "enable switch" segment. "Enable switches" are interlocked or administratively controlled so that only one "enable switch" is active at a time. The figures below illustrate this limiting measure:  Caution: This measure prevents multiple erroneous commands to multiple groups of SSCs. It cannot reduce the likelihood of a single or multiple erroneous commands to a group of SSCs, because after the "enable switch" is activated, the workstation can send one or more erroneous commands, regardless of the command that may have been initiated by the operator. For example, after enabling a specific group of SSCs for control, the operator touches the OPEN soft control for one SSC, but the workstation erroneously sends CLOSE to that SSC or sends OPEN to the wrong SSC. Or, after enabling a specific group of SSCs for control, the operator initiates nothing (i.e., he or she is still thinking), but the workstation erroneously sends one or more erroneous commands to one or more SSCs within the group.

Table A-18 (continued)
Measures for Limiting a CCF Caused by Erroneous Commands from a Random Failure of a Shared Operator Workstation

Limiting Measures	
	  If this method is applied to a non-safety workstation that can send control commands to a safety controller, then the safety controller ensures its own data communication independence (reference IEEE 7-4.3.2 in the U.S.), including unalterable program memory (hardware protected) that is changeable only by removal from the controller. When this L measure is applied, the enable switch is part of the safety system. Therefore, the enable switch logic, which is enabled for only one safety division at a time, is credited as the priority logic that will block erroneous signals from the non-safety operator workstation.

A.1.6.3 Coping with a CCF Caused by a Random Failure of a Shared Operator Workstation

Loss of Control Capability for Multiple SSCs

Although an operator workstation failure will not affect the automatic control algorithms or the current state of manually controlled plant components, a failure will typically affect an operator's ability to monitor the control functions, change the state of the algorithms (e.g., setpoint changes, mode changes) and manually change the state of the controlled plant components (e.g., valve open to close). Therefore, the CCF *coping analysis* demonstrates that operators can manage this condition, and avoid a plant transient, with other instrumentation and other plant components that are not affected by the operator workstation failure. Since the failure can occur at any time, the analysis evaluates stable as well as transient plant conditions, including startup, shutdown and accidents. One coping method to reduce the likelihood of an unanalyzed condition may be to trip the plant or initiate a controlled shutdown, if an undesirable trend can be detected.

Multiple Erroneous Commands that Affect Multiple SSCs

The *coping analysis* for multiple SSCs is challenging, because the failure state of those SSCs is not predictable; some valves may open others may close, some pumps may start others may stop. This challenge increases as more and more SSCs are impacted. Therefore, limiting the number of effected SSCs is important for L1, because without any preventive measures within the workstation, and to be consistent with the traditional nuclear plant design basis paradigm, the *coping analysis* would employ *design basis* methods for the enabled set of SSCs.

For many plants the PRA logic models may provide a basis for selecting the combinations of SSC malfunctions to be considered in a coping analysis. An examination of the accident sequence cut sets for any that have failure modes of the SSCs that are impacted can be performed. Any combinations of affected SSC failure modes that do not exist in the cut sets need

not be considered in the coping analysis. Any combinations of affected SSC failure modes that also appear in combination with failure modes of multiple unaffected components are not likely to be risk significant as this is an indication that additional random failures need to occur before core cooling is jeopardized or significant releases would occur. For combinations that appear in accident sequence cut sets and result in unacceptable results, limiting the CCF to fewer components may be a clear solution. But, examination of the cut sets from the PRA can help to identify other SSCs or actions that may be credited for mitigation.

A.1.7 Random Hardware Failure in a Shared Engineering/Maintenance Workstation

This section applies to any engineering/maintenance workstation, including workstations that interface with multiple divisions.

A random hardware failure in a shared engineering/maintenance workstation can lead to:

Condition 1	Loss of mode/bypass change or program alteration capability for multiple SSCs
Condition 2	Erroneous control, mode/bypass change or program alteration commands for multiple SSCs

A.1.7.1 Shared Engineering/Maintenance Workstation Condition 1 (Loss of Control)

Typically, these workstations are not required for plant operation. A review should be performed to confirm that the workstation provides only non-critical functions. Therefore, for most applications there is no need to reduce the likelihood of or limit this CCF. If an engineering workstation is required for operations, then it is an operator workstation as well. Refer to the measures intended for reducing the likelihood of, or limiting the effects of a CCF caused by Condition 1 (Loss of Control) in an operator workstation) provided in Section A.1.6. If needed to support plant operation and the review identifies only a limited time duration for which loss of the engineering/maintenance workstation is acceptable, and no P or L measures are provided, then the analysis should demonstrate that a failed workstation can be restored within that time duration.

If no preventive measures are implemented for a workstation needed to support plant operation, or if one is only partially implemented, then refer to the measures for limiting a CCF caused by Condition 1 (Loss of Control) in an operator workstation provided in Section A1.6.2.

A.1.7.2 Shared Engineering/Maintenance Workstation Condition 2 (Erroneous Commands)

Erroneous commands (Condition 2) includes:

- Erroneous control command
- Erroneous mode/bypass change
- Erroneous program alteration

Figure A-10 illustrates examples of CCFs caused by Condition 2.

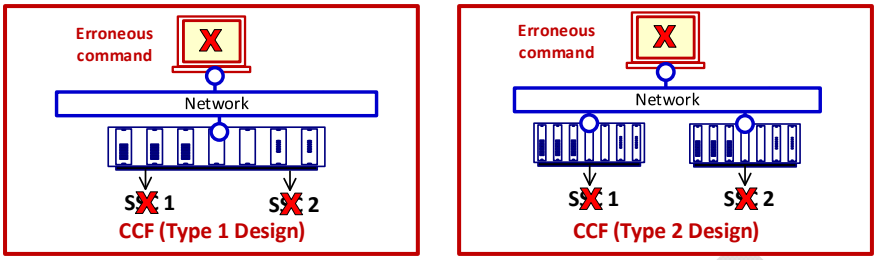


Figure A-10
Erroneous Commands Caused by a Random Failure of a Shared Engineering/Maintenance Workstation

Measures Intended to Reduce the Likelihood of a CCF caused by an Erroneous Command from a Random Failure of a Shared Engineering/Maintenance Workstation to Level 2

To reduce the likelihood of a CCF of multiple SSCs caused by an erroneous command from a random failure of a shared engineering/maintenance workstation, applying one of the measures from Table A-19 (or comparable measures) is recommended.

Table A-19
Measures Intended to Reduce the Likelihood of a CCF caused by an Erroneous Command from a Random Failure of a Shared Engineering/Maintenance Workstation to Level 2

Preventive Measures	
P1	**Provide assurance that a controller cannot receive any erroneous commands or data requests from a shared engineering / maintenance workstation while the controller is in operation by providing the following measures**: 1. The controller cannot receive any data (including data requests) from the engineering workstation during normal operation 2. For non-safety engineering workstations interfacing to safety controllers, the safety controllers provide communication independence and functional independence (reference IEEE 7-4.3.2 in the U.S.). This is ensured through a hardware interlock within each controller that normally prevents the controller from receiving commands of any type. This could be implemented with a hardware switch that controls the write port of the receive data memory or a physical disconnect of the interfacing data communication cable. Even if a non-safety engineering workstation has no ability to initiate control commands, change modes/bypasses or alter programs, a safety controller protects itself against a failure in the engineering workstation that generates these erroneous signals. Therefore, control, mode/bypass change or program alteration can only be affected when the controller's hardware switch is enabled or the data communication cable is physically connected. 3. Documented administrative controls to provide assurance that that the controller is taken out of service before the interlock described above is enabled. The figures on the left show a design that uses a hardware switch that controls the write port of the receive data memory, and the figures on the right show a design that involves a physical disconnect of the interfacing data communication cable.

Table A-19 (continued)
Measures Intended to Reduce the Likelihood of a CCF caused by an Erroneous Command from a Random Failure of a Shared Engineering/Maintenance Workstation to Level 2

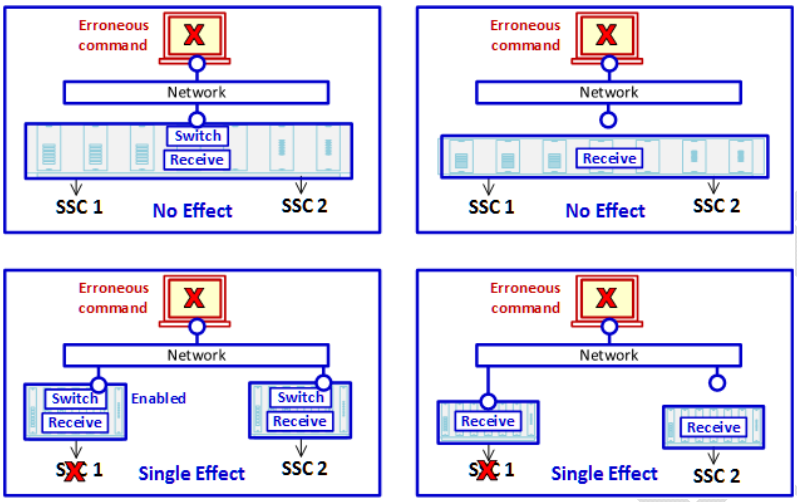
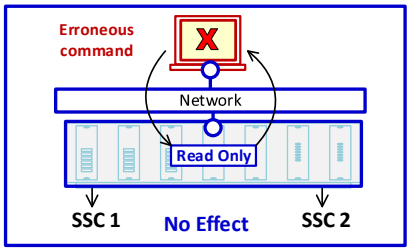
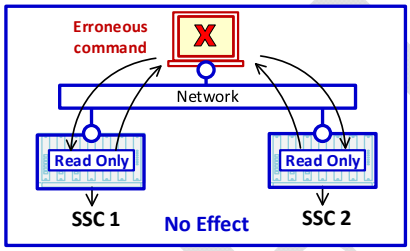
Preventive Measures	
P1	 For non-safety engineering workstations interfaced to safety controllers, this preventive measure can be further enhanced by providing separate engineering workstations for each division. But this is not necessary, because only one controller (from any safety division) is connected to the engineering workstation at any one time. Caution: This measure does not reduce the likelihood of a CCF for a Type 1 design (single controller controlling multiple SSCs), because when that controller is taken out of service to enable receipt of engineering workstation data, the out of service condition affects all SSCs controlled by the same controller. To reduce the likelihood of a CCF for a Type 1 design, provide a controller with duplex or triplex redundancy, configure each controller as if it were a separate controller, per the descriptions above, and include administrative controls to take only one controller out of service at a time during on-line operation.

Table A-19 (continued)
Measures Intended to Reduce the Likelihood of a CCF caused by an Erroneous Command from a Random Failure of a Shared Engineering/Maintenance Workstation to Level 2

Preventive Measures	
P2	**Provide assurance that a controller can only receive data requests from an engineering workstation during normal operation (e.g., commands to read specific error logs or data values), but does not normally allow control, mode/bypass change or program alteration command**s. The controller limits the data requests it will respond to, to provide assurance that the deterministic processing within the controller cannot be negatively affected by an overload of data requests. The following figures illustrate this measure:   For non-safety engineering workstations interfacing to safety controllers, other types of commands are permitted by using additional defensive measures: a) Provide a dedicated non-safety engineering workstation for each division. b) Provide a hardware interlock within the controller to reduce the likelihood of program memory alteration (e.g., a switch that disables the memory write enable port), or physically disconnect the data communication cable. c) Ensure the program memory is alterable only by removing the memory from the controller (reference IEEE 7-4.3.2). d) Provide priority logic to ensure the safety function determines when mode/bypass changes are permitted (e.g., interlocks between divisions that allow only one division to have a maintenance bypass for the same safety function at any one time). <u>Caution:</u> This measure does not reduce the likelihood of a CCF for a Type 1 design (single controller controlling multiple SSCs), because when that controller is taken out of service to enable receipt of engineering workstation data, the out of service condition affects all SSCs controlled by the same controller. To reduce the likelihood of a CCF for a Type 1 design, provide a controller with duplex or triplex redundancy, configure each controller as if it were a separate controller, per the descriptions above, and include administrative controls to take only one controller out of service at a time during on-line operation.

Limiting a CCF Caused by an Erroneous Command from a Random Failure of a Shared Engineering/Maintenance Workstation

There are no identified measures for limiting a CCF caused by an erroneous command from a random failure of a shared engineering/maintenance workstation beyond the generic limiting measure that would limit the number of SSCs affected.

A.1.7.3 Coping with a CCF Caused by a Random Failure of a Shared Engineering/Maintenance Workstation

Loss of Change Capability

Engineering/maintenance workstations are typically not credited for any plant operation functions. Therefore, documenting this is sufficient; an analysis is not required. But there may be some situations where the engineering/maintenance workstation is credited. For example, during startup or shutdown the workstation may be credited to enable or disable protective functions that are not appropriate for alternate plant modes (e.g., preventing ECCS actuation during depressurization). Similarly, engineering/maintenance workstations may be credited for entering calibration constants (e.g., for excore neutron monitoring). The CCF *coping analysis* would address the inability to utilize the engineering/maintenance workstation functions. One acceptable coping method may be to hold the plant in the current mode that does not require the engineering/workstation until the workstation functionality can be restored. The analysis should demonstrate that a failed workstation can be restored within the available time duration.

Erroneous Command

No limiting method is offered for this failure, because the potential combinations of erroneous commands is essentially unlimited, making the CCF *coping analysis* unmanageable.

A.1.8 Random Hardware Failure in a Shared Controller

This section applies to a random hardware failure of any controller that is shared by multiple SSCs, thus it is limited to a Type 1 design. This section is not applicable to a Type 2 design because there is no shared controller in a Type 2 design (i.e., a CCF is inherently prevented). A component failure within a shared controller can result in erroneous operation of multiple SSCs, and it can be caused by any of the following internal failure mechanisms:

- Application program memory failure
- Operating system memory failure
- CPU processing failure
- Internal data communication failure

Controller self-diagnostics are typically insufficient to detect program memory errors because program memory typically requires multiple cycles to completely test, and can take 10 minutes or more. This is applicable to each controller in any configuration (i.e., single, duplex or triplex). Therefore, between test cycles, a memory failure can result in erroneous operation. This is applicable to any controller configuration (i.e., single, duplex or triplex).

Figure A-11 illustrates an example of a CCF caused by a random failure within a shared controller.

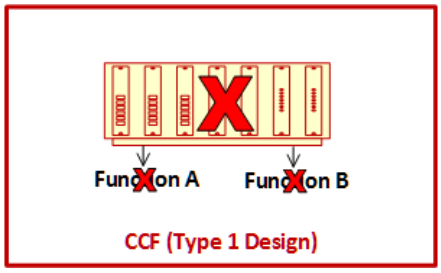
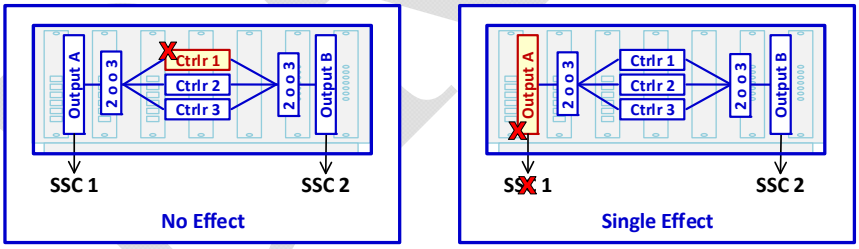


Figure A-11
Component Failure within a Shared Controller

A.1.8.1 Measures Intended to Reduce the Likelihood of a CCF caused by a Component Failure within a Shared Controller to Level 2

To reduce the likelihood of a CCF caused by a random failure within a shared controller, applying one of the measures from Table A-20 (or comparable measures) is recommended.

Table A-20
Measures Intended to Reduce the Likelihood of a CCF caused by a Component Failure in a Shared Controller to Level 2

Preventive Measures	
P1	**Provide a Triple Modular Redundant (TMR) controller configuration, where three separate controller outputs are 2oo3 voted to eliminate the erroneous output.** Distribute each SSC to a separate output module The figure on the left shows a random failure of one of three redundant controllers, resulting in no effect. The figure on the right shows a random failure of a single output module, resulting in a single effect. 

A.1.8.2 Limiting a CCF Caused by a Random Failure of a Shared Controller

If none of the preventive measures provided above are implemented, or if one is only partially implemented, then one of the limiting measures listed in Table A-21 may be helpful.

Table A-21
Measures for Limiting a CCF Caused by a Random Failure within a Shared Controller

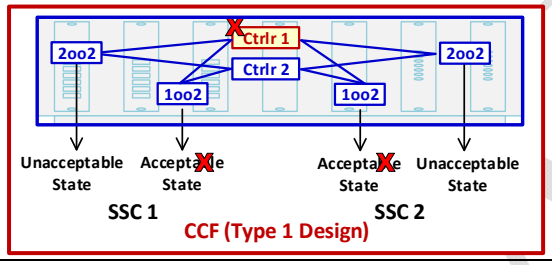
Limiting Measures	
L1	**Provide a duplex controller configuration with 2oo2 output voting for each SSC to provide assurance that that the controllers agree for selected output states where an erroneous output would cause unacceptable effects.** Both controllers are running in parallel. This measure limits the effects of a CCF caused by a failure within a controller to output states that can be analyzed and found acceptable. Voters only apply to SSCs that have an unacceptable output state. For most SSCs neither output state would be unacceptable (i.e., those that pose no threat to critical functions or have no potential to cause a plant transient); therefore, these SSCs don't need any 2oo2 voters. Voters are applied only to selected SSCs and only to the problem state associated with those SSCs. For example, spurious *closure* of multiple vent valves may be *acceptable*, but spurious *opening* of multiple vent valves may be *unacceptable*. Therefore, the close signal employs 1oo2 logic, and the open signal employs 2oo2 logic. For this example, the CCF coping analysis demonstrates the *acceptability* of multiple spurious valve *closures* and the *inability* to *open* the valves, in either case caused by a single controller internal failure; the CCF coping analysis does not need to consider spurious opening of multiple valves. The figure below illustrates this example: 
L2	**Provide a duplex controller configuration with an output compare function.** Controllers are in a hot-standby configuration, however both controllers continuously execute the control application, and the primary controller continuously compares its outputs to the standby controller to detect inconsistency for erroneous outputs that may cause undesired effects. When an unexpected inconsistency is detected, both controllers are forced to a predetermined shutdown mode equivalent to a watchdog timeout. This limitation method forces both controllers to an acceptable shutdown state for failures that are not detected quickly enough by normal self-diagnostics (e.g., a program memory failure in a byte applicable to a function block used by multiple application functions). This method has minimal impact on the reliability improvement normally achieved through a standby controller configuration, because most failures in the primary controller are self-detected prior to generating an erroneous output. Therefore, the primary controller will take itself out of service, causing the standby controller to take over prior to the compare function shutting down both controllers. Provide assurance that the hot standby interface between the controllers is not a source of a single component failure that can cause a failure of both controllers. The following figure illustrates this measure:

Table A-21 (continued)
Measures for Limiting a CCF Caused by a Random Failure within a Shared Controller

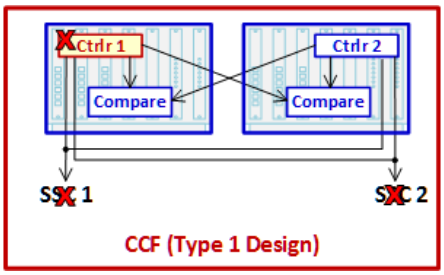
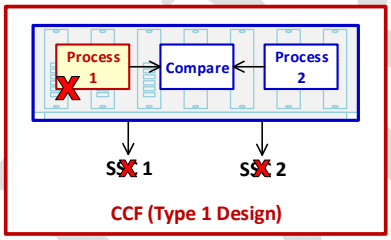
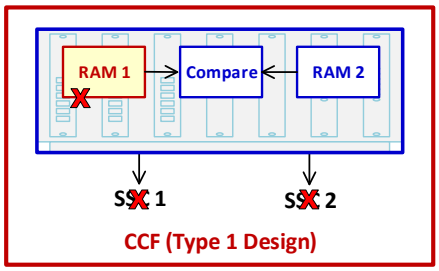
Limiting Measures	
	 An analysis should be performed to demonstrate the acceptability of controller shutdown and that the erroneous outputs that may occur for a short duration (typically milliseconds) prior to controller shutdown are acceptable.
L3	**Provide a single controller with an output compare function, configured with redundant and diverse internal processing.** Diverse processes perform the same functional algorithm using different internal function blocks. When an unexpected inconsistency is detected, the controller is forced to a predetermined shutdown mode equivalent to watchdog timeout. For CPU, compare function, and internal data communication failures, provide periodic instructions with comparison to known expected results. This limitation method forces a controller to an acceptable shutdown state for failures that are not detected quickly enough by normal self-diagnostics (e.g., a program memory failure in a byte applicable to a function block used by multiple application functions). Therefore, perform a failure modes and effects analysis to demonstrate that: 1. there are no function block failures that can cause the same erroneous output from both diverse processes, and 2. other failures that could negatively affect both diverse processes are detected by controller self-diagnostics and also cause a controller shutdown.  <u>Caution:</u> 1. A analysis may be needed to demonstrate the acceptability of controller shutdown and that the erroneous outputs that may occur for a short duration prior to controller shutdown, if any, are acceptable. 2. This limiting measure forces a controller to an acceptable shutdown state for failures that are not detected quickly enough by normal self-diagnostics (e.g., a program memory failure in a byte applicable to a function block used by multiple application functions). Therefore, perform a failure modes and effects analysis to demonstrate that: a. there are no function block failures that can cause the same erroneous output from both diverse processes, and b. other failures that could negatively affect both diverse processes are detected by controller self-diagnostics and also cause a controller shutdown.

Table A-21 (continued)
Measures for Limiting a CCF Caused by a Random Failure within a Shared Controller

L4	**Provide dual internal memory (e.g., mirrored RAM) where read/write functions are duplicated and compared.** Unexpected comparison errors result in a predetermined shutdown mode equivalent to watchdog timeout; this prevents erroneous control caused by memory errors. For CPU, compare function, and internal data communication failures, provide periodic instructions with comparison to known expected results. The figure below shows a memory error on one side of a mirrored RAM configuration that shuts down the controller via the compare feature, resulting in a predetermined state for both SSCs. This example describes mirrored RAM, but if program execution is from non-volatile memory (e.g., EPROM), the same memory duplication and compare functionality would apply. 

A.1.8.3 Coping with a CCF Caused by a Random Failure within a Shared Controller

If none of the Preventive or Limiting measures described above are implemented, the effects of an I&C failure are very difficult to predict. In this case, the analysis considers the worst case combination of high/low outputs from the perspective of threats to critical safety functions, depending on the SSCs that are controlled. These threats may originate from safety controllers/SSCs or non-safety controllers/SSCs. Outputs include signals to plant components as well as signals to other controllers.

When conducting the CCF *coping analysis*, interlocks that reside outside the affected controller can be credited; these interlocks may lessen the undesirable effects of the controller failure. Interlocks that reside within the software functions of the controller cannot be credited, because the failure may affect functions that are downstream of the software interlock.

For any of the limiting measures described above that result in a shutdown state of the controllers, the *coping analysis* assesses the resulting states of the affected SSCs (e.g., open, close, on, off, etc.).

Any of the limiting measures described above that employ output voting or output comparison can be applied only to outputs where erroneous signals are unacceptable, it is not necessary to apply these measures to all outputs. The CCF *coping analysis* demonstrates the adequacy of the selected outputs.

A.1.9 Random Hardware Failure in a Shared Clock

This section applies to a Type 1 or Type 2 design where a common clock signal is shared by multiple SSCs. In this guideline, a clock means a system or component that automatically and periodically provides date and time data, or any type of time reference for the synchronization of multiple functions. A clock can be external to any controller and/or resident within any

controller. A random failure of a shared clock can lead to erroneous controller outputs. Clock failures include any of the following conditions:

Condition 1	Incorrect date or time
Condition 2	Missing date or time
Condition 3	Out of range date or time (e.g., January 0, February 29, March 32)
Condition 4	Delayed clock updates (routinely or sporadically)
Condition 5	Accelerated clock updates (routinely or sporadically)
Condition 6	Other clock signal communication interface anomalies (e.g., data storm or other communication errors)

Figure A-12 illustrates examples of CCFs caused by a random failure of a shared clock:

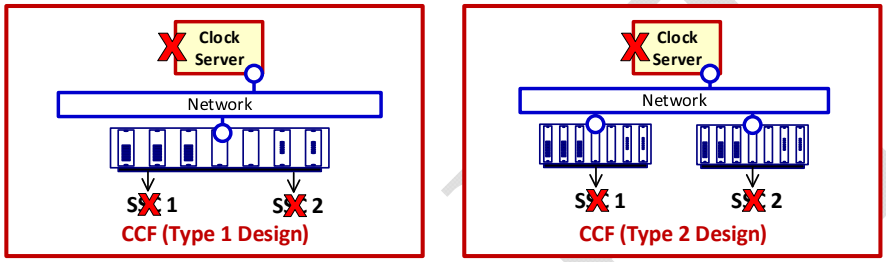


Figure A-12
Random Failure of a Shared Clock

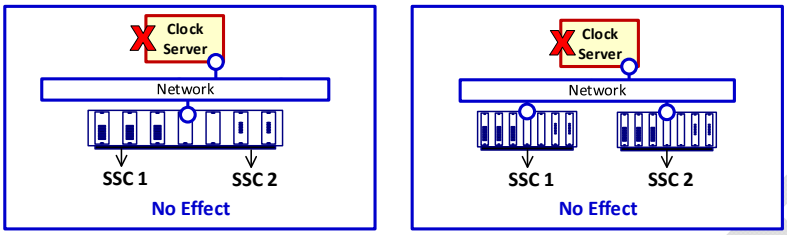
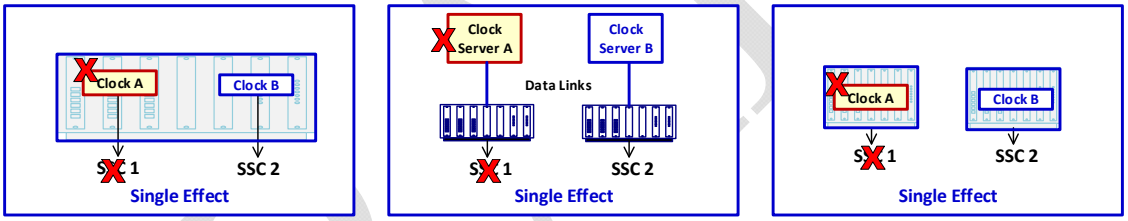
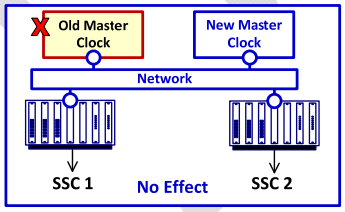
A.1.9.1 Measures Intended to Reduce the Likelihood of a CCF caused by a Random Failure of a Shared Clock to Level 2

To reduce the likelihood of a CCF of multiple controlled SSCs caused by a random failure of a shared clock, applying one of the measures from Table A-22 (or comparable measures) is recommended.

Table A-22
Measures Intended to Reduce the Likelihood of a CCF caused by a Random Failure of a Shared Clock to Level 2

Preventive Measures	
P1	**Do not use a shared clock for control and provide the following measures to provide assurance that a shared clock does not influence controller outputs:** a) No date or time functions are used to calculate or influence any controller outputs for SSC control. Therefore, time errors (Conditions 1-5 per Section A.1.9) have no adverse effect on SSCs. b) Analysis demonstrates that any internal features of the controller that use date or time functions (e.g., time stamping data that is stored in an event log) have no influence on control tasks or controller outputs. Therefore, time data errors (Conditions 1-5) have no adverse effect on SSCs. c) For Conditions 4 through 6, provide the following design features, and demonstrate via analysis or testing that clock communication interface anomalies (e.g., Conditions 4-6) do not affect controller operation: 1) Provide separate communication processors (for receiving the clock signal) in each controller with their own deterministic cycle that is independent and asynchronous from the function processor of each controller, so that erratic communication cycles, communication overload or error that causes erratic operation of the communication processor will not affect the deterministic operation of the function processor (i.e., the one that is programmed with application logic for the SSC). 2) To facilitate independent asynchronous operation, the communication processor and function processor within each controller exchange data via shared memory with memory arbitration circuits. In the U.S., refer to IEEE 7-4.3.2 for additional detail to provide assurance that communication independence between function processors and communication interfaces. 3) Analysis or testing demonstrate that clock communication interface anomalies do not affect controller operation. While 1) and 2) provide assurance of independence of each function processor from a common time reference communication interface, they still permit time synchronization for functions such as sequence of event (SOE) recording. For example, SOE time stamping can be synchronized in multiple controllers as follows: The clock server periodically deposits its time reference in the shared memory of each controller. Each function processor independently and asynchronously reads the time reference every control cycle. Each SSC processor identifies when there is a time reference change and then, based on its own known processor cycle time, establishes its own internal time stamping. For example, if an event occurs 10 SSC processor cycles after the last time reference change and the SSC processor has a cycle time of 50msec, then the SSC processor stamps the event with the clock server time reference plus 500msec. It is noted that with this method (and for any digital system), the SOE accuracy of digitally processed events can be no better than the cycle time of the SSC processor. The following figures illustrate this measure:

Table A-22 (continued)
Measures Intended to Reduce the Likelihood of a CCF caused by a Random Failure of a Shared Clock to Level 2

Preventive Measures	
	
P2	**Provide a separate unsynchronized clock for each SSC that requires date and/or time data, with each clock resident in the controller or separately interfaced to the controller** With this method the clock signals can be used for control, because there is a separate clock for each controller. For Type 2 designs each controller has its own internal clock or its own external clock, each with its own communication interface; a networked communication interface is not employed because the network can be a source of CCF. If this method is applied to a Type 1 design, each of the clocks is resident within the controller; a data communication interface is not used because a data storm on that interface could negatively affect multiple SSCs. The following figures illustrate this measure: 
P3	**Provide a "Best Master" clock arrangement that protects against erroneous clock updates.** Provide multiple clocks such that a "best master" clock can be automatically identified (per IEEE 1588), and in the event of erroneous data, another clock will automatically become the new "best master." This measure protects against Conditions 1 through 5 by automatically providing another master clock source in the event of a single failure in the prior master clock that produces erroneous date/time data.  Caution: 1. This measure does not protect against Condition 6 (other clock signal communication interface anomalies such as a data storm or other communication errors arising from a random hardware failure). See Tables A-9, A-11 and A-13 for preventive measures related to single failures in data communication interfaces. 2. An analysis demonstrates that the time it takes for a new "best master" clock to be identified and provide a signal does not adversely impact any CPE that needs the clock signal to function correctly.

A.1.9.2 Limiting a CCF Caused by a Random Failure of a Shared Clock

There are no identified measures for limiting the effects of a CCF caused by a random hardware failure of a shared clock beyond the generic measure of limiting the number of SSCs that share the clock.

A.1.9.3 Coping with a CCF Caused by a Random Failure of a Shared Clock

The CCF *coping analysis* examines the potential for erroneous clock signals and the effect of those erroneous signals on the SSC control algorithms.

A.2 CCF Caused by an Environmental Disturbance

This section provides guidance on measures intended to reduce the likelihood of a CCF of multiple controlled SSCs to Level 2, or limiting the effects of a CCF, caused by any of the following environmental disturbances on an individual basis:

- High temperature or humidity
- Electromagnetic interference (EMI)
- Seismic event
- Radiation
- Fire or smoke

Safety systems trains are designed with physical separation and may use qualified equipment for selected transient and accident conditions to meet the intent of reducing the likelihood of a CCF of multiple controlled SSCs to Level 2 for one or more of these sources. Non-safety systems are physically separated or tested to comparable levels if the measures described below are applied.

In considering the defensive measures available to reduce the likelihood of or limit the scope of digital I&C failures caused by environmental sources, it should be kept in mind that managing the event initiator for these challenges can be an effective way of influencing their likelihood. With one exception, challenges from these sources require failure of other systems in the plant as an initiator for these environmental challenges to occur. In that regard, the likelihood of the digital I&C failure begins with determining the likelihood of failure of the systems and equipment that result in the environmental challenge. If the likelihood of the environmental challenge is at or below Level 2, then the likelihood of an I&C failure of interest is also at or below Level 2.

The exception is seismic events. A seismic event is a natural phenomenon which challenges all SSCs in the plant concurrently and does not require failure of a system outside of the digital I&C system of interest.

In developing the preventive and limiting measures for each of the environmental challenges listed above, consideration is given to the likelihood of the challenge itself.

A.2.1 High Temperature or Humidity

High temperature or humidity is a result of loss of heating, ventilation and air conditioning (HVAC). High temperature or humidity is a result of loss of heating, ventilation and air conditioning (HVAC). In assessing the effects of high temperature and humidity on I&C, consideration should be given to the likelihood of loss of the HVAC. Single point vulnerabilities would preclude the conclusion that loss of HVAC is no more likely than CCFs that are not considered in the traditional conservative safety analysis. If loss of HVAC requires multiple failures, however, then the likelihood of high temperature and humidity resulting from the loss of HVAC is at or below Level 2. If multiple trains of HVAC are not independent or separated, then it may not be appropriate to consider loss of HVAC at likelihood Level 2, but only for events which could result in loss of all trains caused by the lack of independence or separation.

Figure A-13 illustrates a CCF in either a Type 1 design or a Type 2 design caused by high temperature or humidity. High temperature or humidity can cause one or more controllers to generate erroneous outputs.

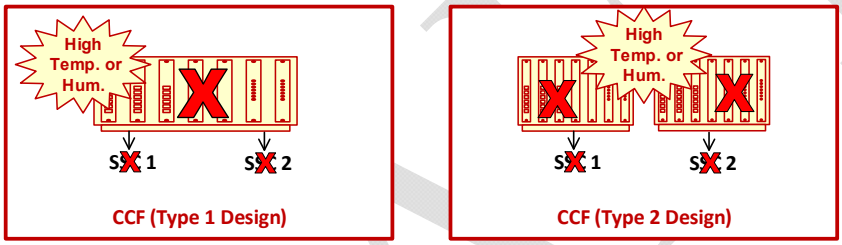


Figure A-13
CCFs Caused by High Temperature or Humidity

A.2.1.1 Measures Intended to Reduce the Likelihood of a CCF caused by High Temperature or Humidity to Level 2

To reduce the likelihood of a CCF caused by high temperature or humidity, applying one of the measures from Table A-23 (or comparable measures) is recommended.

Table A-23
Measures Intended to Reduce the Likelihood of a CCF Caused by High Temperature or Humidity to Level 2

Preventive Measures		
P1	**Demonstrate controller can operate without failure occurring with loss of the HVAC system for at an acceptable period for the design basis ambient temperature/humidity.** For design basis conditions consider seasonal changes (e.g., summer in Spain).	
	Safety Equipment For safety equipment provide equipment qualification in accordance with applicable standards (e.g., IEEE-323 in the U.S.)	Non-safety Equipment For non-safety equipment confirm manufacturer's specifications meet or exceed expected temperature and humidity levels, and confirm the methods used by the manufacturer to test their equipment to those specifications.
P2	**Provide redundant HVAC so that a single failure in the HVAC system does not result in complete loss of HVAC for any division (safety or non-safety).** Redundant HVAC is typical for the Main Control Room (MCR), but is not likely to be available or feasible in other parts of the plant.	
P3	**Accommodate HVAC failure with temporary HVAC within time to reduce the likelihood of the controller from exceeding its environmental specifications.** For heat rise time consider seasonal changes (e.g., summer in Spain). Confirm manufacturer's specifications and confirm the methods used by the manufacturer to test their equipment to those specifications. Temporary HVAC procedures are documented.	
P4	**Physically separate controllers so that an HVAC failure only affects one SSC** (i.e., only applicable to a Type 2 design). This method is typically applied to reduce the likelihood of HVAC failure from causing a CCF in multiple safety divisions; for safety divisions physical separation complies with applicable codes and standards (i.e., IEEE-384 in the U.S.).	

A.2.1.2 Limiting a CCF Caused by High Temperature or Humidity

To limit the effects of a CCF caused by high temperature or humidity, one of the limiting measures listed in Table A-24 may be helpful.

Table A-24
Measures for Limiting a CCF Caused by High Temperature or Humidity

Limiting Measures	
L1	**Force the controller to a predetermined shutdown state when the temperature reaches the maximum controller operating specification by monitoring the temperature at the controller location.** For example, some CPU chips have an over-temperature shutdown feature built-in, at the chip location. Caution: For I&C equipment located inside an enclosure, local heat rise (typically 15°F above ambient) should be accounted for when determining the suitability of a controller's maximum temperature specification.

A.2.2 Electro-Magnetic Interference (EMI)

An EMI disturbance can cause one or more controllers to generate erroneous outputs. Figure A-14 illustrates a CCF in either a Type 1 design or a Type 2 design caused by an EMI disturbance.

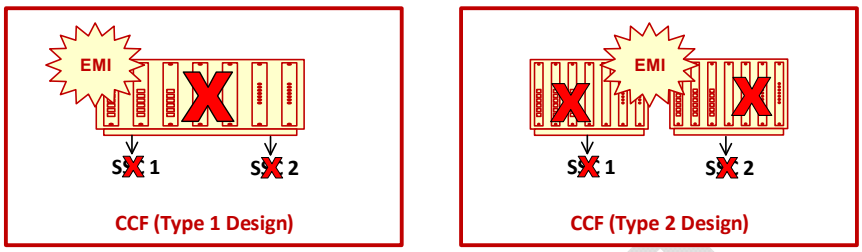


Figure A-14
CCFs Caused by an EMI Disturbance

A.2.2.1 Measures Intended to Reduce the Likelihood of a CCF caused by an EMI Disturbance to Level 2

To reduce the likelihood of a CCF caused by an EMI disturbance, applying one of the measures from Table A-25 (or comparable measures) is recommended.

Table A-25
Measures Intended to Reduce the Likelihood of a CCF caused by an EMI Disturbance to Level 2

Preventive Measures		
P1	**Demonstrate controller can operate without failure during design basis EMI conditions.**	
	Safety Divisions For safety divisions provide equipment qualification in accordance with applicable guides or standards (e.g., EPRI TR-102323 [Ref 9])	**Non-safety Division** For non-safety equipment confirm manufacturer's specifications meet or exceed design basis EMI levels and confirm the methods used by the manufacturer to test their equipment to those specifications.
P2	**Physically separate controllers with suitable EMI barriers so that design basis EMI affects only one SSC (i.e., only applicable to a Type 2 design).** Demonstrate controller can operate without failure during normal EMI conditions.	
	Safety Divisions For safety divisions provide equipment qualification in accordance with applicable guides and standards (e.g., RG 1.180 in the U.S.)	**Non-safety Division** For non-safety equipment confirm manufacturer's specifications meet or exceed design basis EMI levels and confirm the methods used by the manufacturer to test their equipment to those specifications.

A.2.2.2 Limiting a CCF Caused by an EMI Disturbance

To limit the effects of a CCF caused by EMI, one of the limiting measures listed in Table A-26 may be helpful.

Table A-26
Measures for Limiting a CCF Caused by an EMI Disturbance

Limiting Measures	
L1	**Demonstrate controller can operate without failure during normal EMI conditions.** Physically separate controllers so that design basis EMI affects a limited number of SSCs. This is the generic limiting measure (i.e., limit the number of affected SSCs), with an additional demonstration for normal EMI conditions. A coping analysis determines whether or not that erroneous operation of all controllers within the affected area is acceptable.

A.2.3 Seismic Event

A seismic event can cause one or more controllers to generate erroneous outputs caused by mechanical shock, vibration, or stress on internal components. Figure A-15 illustrates a CCF in either a Type 1 design or a Type 2 design caused by a seismic event.

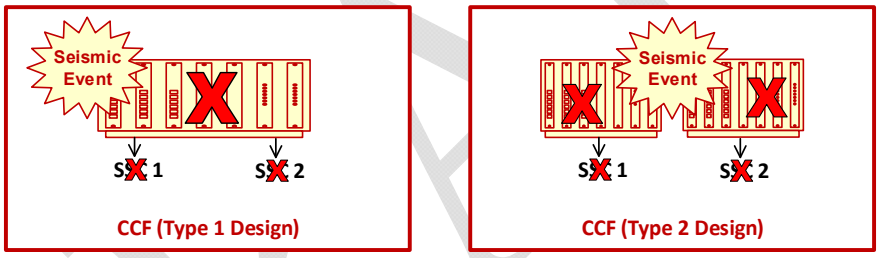


Figure A-15
CCFs Caused by a Seismic Event

A.2.3.1 Measures Intended to Reduce the Likelihood of a CCF caused by a Seismic Event to Level 2

A full range of ground motion should be considered when assessing I&C response to seismic events, from the operating base earthquake (OBE) to beyond the safe shutdown earthquake (SSE). Some I&C may not be necessary to consider beyond the OBE (such as those needed only to support plant operation). To identify the subset of I&C needed up to the SSE and for seismic events that exceed the SSE to be considered unlikely, safety analysis and PRA personnel should be consulted.

Regardless of the likelihood of any given level of ground motion, the following preventive and limiting measures address the scope of CCFs that might result from I&C failures caused by a seismic event

To reduce the likelihood of a CCF caused by a seismic event, applying one of the measures from Table A-27 (or comparable measures) is recommended. For non-safety systems, the potential for a CCF caused by the operating basis earthquake (OBE) is evaluated. For safety systems, and non-safety systems that can interfere with safe shutdown, the potential for a CCF caused by the safe shutdown earthquake (SSE) is evaluated.

Table A-27
Measures Intended to Reduce the Likelihood of a CCF caused by a Seismic Event to Level 2

Preventive Measures		
P1	**Demonstrate controller can operate without failure during design basis seismic conditions.**	
	Safety Divisions For safety divisions provide equipment qualification in accordance with applicable standards (e.g., IEEE-344 in the U.S.)	**Non-safety Division** For non-safety equipment confirm manufacturer's specifications meet or exceed design basis seismic conditions and confirm the methods used by the manufacturer to test their equipment to those specifications.
P2	**Perform a fragility analysis on the cabinets/mountings that support the digital I&C** and confirm a high confidence low probability of failure (HCLPF) even for beyond design basis ground motion. Also confirm low potential for systems interaction.	

A.2.2.3 Limiting a CCF Caused by a Seismic Event

If none of the preventive measures provided above are implemented, or if one is only partially implemented, then one of the limiting measures listed in Table A-28 may be helpful.

Table A-28
Measures for Limiting a CCF Caused by a Seismic Event

Limiting Measures	
L1	**Provide a seismic monitor to force controllers to a predetermined shutdown state.** For this method the seismic level at which the equipment can operate with no malfunction must is first established so that the setpoint for the seismic monitor can be established. This limiting method can be applied to systems that are not needed after a design basis seismic event. It cannot be applied to systems that are needed after a design basis seismic event (e.g., ESF systems, post-shutdown systems, etc.). If this method is applied to a reactor trip system, then the seismic monitoring/shutdown function is part of the reactor trip system (i.e., Class 1E in the U.S.). <u>Caution:</u> Margin in the seismic monitor setpoint should be carefully evaluated for the potential for spurious actuations that can adversely affect CPE.

A.2.4 Radiation

Essentially, there are two distinct radiological environments that can contribute to the dose of components in an I&C system; that associated with normal operation (including shutdown conditions and maintenance activities) and those that occur as a result of accident conditions. It is necessary to consider he accumulated dose from normal operation over the lifetime of the I&C when identifying possible failures resulting from radiation exposure. However, additional dose from accident conditions, such as TID or alternate source term, generally requires failure of multiple redundant trains of equipment (such as the ECCS) before sufficient fuel damage would occur that could lead to these source terms. Therefore, while the likelihood of radiation dose from normal operation does not reach Level 2, the source term considered for the design basis accident must reach Level 2 by definition.

Regardless of likelihood, the following preventive and limiting measures address the scope of CCFs that might result from I&C failures caused by radiation exposure.

Radiation can cause one or more controllers to generate erroneous outputs caused by an accumulated dose that results in degradation of radiation-sensitive materials. Figure A-16 illustrates a CCF in either a Type 1 design or a Type 2 design caused by prolonged radiation (i.e., accumulated dose) , such as that introduced by a harsh environment.

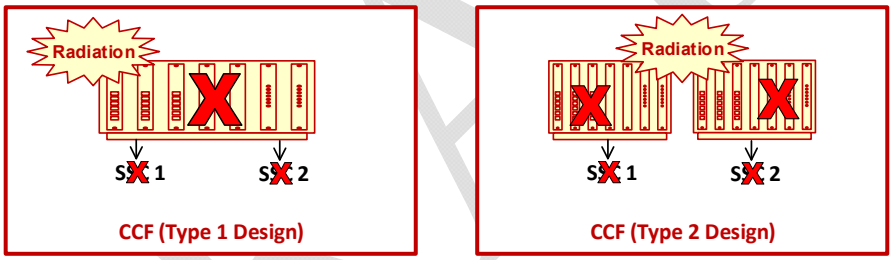


Figure A-16
CCFs Caused by Radiation

A.2.4.1 Measures Intended to Reduce the Likelihood of a CCF caused by Radiation to Level 2

To reduce the likelihood of a CCF caused by prolonged radiation, applying one of the measures from Table A-29 (or comparable measures) is recommended.

Table A-29
Measures Intended to Reduce the Likelihood of a CCF caused by Radiation to Level 2

Preventive Measures		
P1	**Locate equipment in an environment where the radiation exposure is negligible and unchanged during design basis events**.	
P2	D**emonstrate equipment can operate without failure up to and including design basis accumulated radiation dose (i.e., total integrated dose)**.	
	Safety Divisions For safety divisions provide equipment qualification in accordance with applicable standards (e.g., IEEE-323 in the U.S.)	**Non-safety Division** For non-safety equipment confirm manufacturer's specifications meet or exceed design basis radiation dose and confirm the methods used by the manufacturer to test their equipment to those specifications.
P3	**Provide a Type 2 design, and locate equipment in an environment where the radiation exposure is unchanged during design basis events**. This measure prevents concurrent failure of multiple controllers, but does not reduce the likelihood of failure of a controller caused by prolonged radiation exposure. Therefore, control a single SSC from each controller (i.e., a Type 2 design). Also, demonstrate that the failure of a controller is detectable, either through self-announcing or periodic testing, so that multiple failures of controllers do not accumulate to become a CCF. Provide plant procedures that direct failure investigation and correction, with the intention of replacing all controllers before the prolonged radiation exposure results in failure of multiple controllers.	

A.2.4.2 Limiting a CCF Caused by Radiation

If none of the preventive measures provided above are implemented, or if one is only partially implemented, then one of the limiting measures listed in Table A-30 may be helpful.

Table A-30
Measures for Limiting a CCF Caused by Radiation

Limiting Measures	
L1	**Provide a Type 1 design, and locate equipment in an environment where the radiation exposure is unchanged during design basis events.** This measure prevents concurrent failure of multiple controllers, but does not reduce the likelihood of failure of a controller caused by prolonged radiation exposure. This method is only applicable where the failure of the SSCs controlled by the affected controller is self-announcing or detectable through periodic testing. Provide plant procedures that direct failure investigation and correction, with the intention of replacing all controllers before the prolonged radiation exposure results in failure of multiple controllers, thereby preventing a more severe CCF. A coping analysis determines if erroneous operation of all SSCs for an affected controller is an acceptable CCF.

A.2.5 Fire or Smoke

Current fire protection programs in nuclear power plants are typically implemented with a defense-in-depth philosophy that is directed at preventing fires from occurring, detecting fires if they do occur, and suppressing them before significant damage results, all while ensuring that a train of equipment remains available to provide adequate core cooling even if a postulated fire were not to be suppressed. In this regard, before exposure of I&C to high temperatures from combustion or smoke, multiple failures must have occurred already (a fire with failure of suppression and detection). Given these multiple failures, the likelihood of exposure to heat and smoke from a fire is considered to be Level 2 for I&C needed in response to a fire.

Furthermore, when specific I&C is needed in response to a fire, it is unreasonable to expect that the I&C exposed to the fire itself survives. As a result, the I&C located within a fire zone in which a fire is assumed to occur is generally not considered to be necessary in response to that fire. It is the I&C supporting trains of equipment not involved in the fire that are needed in response to the fire and should be demonstrated to be functional in the presence of heat and smoke, if any, in the area in which that I&C is located.

Regardless of whether it is needed or whether or not the likelihood of the challenge is at or below Level 2, the following preventive and limiting measures address the scope of CCFs that might be considered resulting from digital I&C failures that may be exposed to high temperatures or smoke resulting from a fire.

Fire or smoke can cause one or more controllers to generate erroneous outputs caused by high temperature. High temperature can be caused directly by the heat from the fire or by smoke deposits on heat producing components that reduce the likelihood of heat conduction. High temperature can be caused by many factors, including heat that is conducted or radiated directly from the fire, and smoke deposits on air filters and heat sinks. Figure A-17 illustrates a CCF in either a Type 1 design or a Type 2 design caused by fire or smoke.

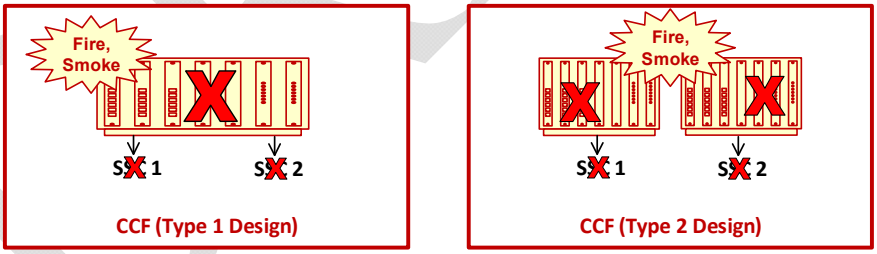


Figure A-17
CCFs Caused by Fire or Smoke

A.2.5.1 Measures Intended to Reduce the Likelihood of a CCF caused by Fire or Smoke to Level 2

To reduce the likelihood of a CCF caused by fire or smoke, applying one of the measures from Table A-31 (or comparable measures) is recommended.

Table A-31
Measures Intended to Reduce the Likelihood of a CCF caused by Fire or Smoke to Level 2

Preventive Measures	
P1	**Demonstrate equipment can operate without failure based on the design basis ambient temperature for the combustibles in the area.**
P2	**Provide a Type 2 design and physically separate controllers with suitable fire barriers so that a fire only affects one SSC.** This method is typically applied to reduce the likelihood of a fire from causing a CCF in multiple safety divisions; for safety divisions, physical separation complies with applicable codes and standards (i.e., IEEE-384 in the U.S.).

A.2.5.2 Limiting a CCF Caused by Fire or Smoke

If none of the preventive measures provided above are implemented, or if one is only partially implemented, then one of the limiting measures listed in Table A-32 may be helpful.

Table A-32
Design Measures for Limiting a CCF Caused by Fire or Smoke

Limiting Measures	
L1	**Physically separate controllers with suitable fire barriers so that a fire only affects a limited number of SSCs.** This method is typically applied to reduce the likelihood of a fire from causing a CCF in multiple safety divisions; for safety divisions provide physical separation in accordance with applicable guides and standards (e.g., IEEE-384 in the U.S.). This is the generic limiting measure with the addition of compliance with codes and standards applicable to safety systems. A coping analysis determines if erroneous operation of all controllers in the affected area is acceptable.
L2	**Monitor temperature at the controller location, and force the controller to a predetermined shutdown state when the temperature reaches the maximum controller operating specification.** For example, some CPU chips have an over-temperature shutdown feature built-in, at the chip location. Caution: For I&C equipment located inside an enclosure, local heat rise should be, and accounted for when determining the suitability of a controller's maximum temperature specification

A.2.6 Coping with a CCF Caused by an Environmental Disturbance

With the exception of seismic challenges, the environmental disturbances identified above are likely to be localized to some extent. In that regard, the generic limiting measure of limiting the number of SSCs that could be affected by an environmental disturbance would be applied to separate redundant divisions of the affected I&C systems such that they are not exposed to the same environmental conditions during selected transients or accidents.

PRA methods can assist in determining which divisions of I&C would benefit from being able to survive exposure to specific environmental challenges. A fault tree of the functions needed following a given transient is first developed (the fault tree likely already exists in the PRA). The fault tree is solved to produce the combinations of failures (cut sets) that must occur to fail the

modeled functions. The cut sets are examined to identify those in which combinations of SSC failure modes occur that could be caused by I&C misbehaviors as a result of the environmental challenges. For those cut sets made up of only SSC failure modes that could be caused by the environmental condition of interest, separation of the I&C for controlling at least one of the affected SSCs from the I&C that controls the remaining affected SSCs is sufficient to provide protection of the I&C from that environmental condition.

A.2.6.1 Shutdown State

For any limiting measure provided above, that results in a shutdown state in one or more controllers, the *coping analysis* assesses the resulting states of the affected SSCs (e.g., open, close, on, off, etc.).

A.2.6.2 Erroneous Operation

The *coping analysis* for multiple SSCs is challenging, because the failure state of those SSCs is not predictable; some valves may open, others may close; some pumps may start, others may stop. This challenge increases as more and more SSCs are impacted. Therefore, limiting the number of affected SSCs is important. As noted above, PRA methods can be used to help determine which controllers to separate.

Once these components are identified, the analysts can use expert judgment to identify the worst combinations of erroneous SSC operation, and thereby limit any detailed analysis to those combinations. Analysts will typically identify combinations that have the potential to exceed the boundaries of previously analyzed limiting faults, such as large break loss of coolant accident (LBLOCA) and main steam line break (MSLB).

For many plants the PRA will provide a sufficient basis to demonstrate these combinations will not lead to core damage or large radiation release. An examination of the accident sequence cut sets for any that have failure modes of the SSCs that are impacted can be performed. Any combinations of affected SSC failure modes that do not exist in the cut sets need not be considered in the coping analysis. Any combinations of affected SSC failure modes that also appear in combination with failure modes of multiple unaffected components are not likely to be risk significant as this is an indication that additional random failures need to occur before core cooling is jeopardized or significant releases would occur. For combinations that appear in accident sequence cut sets and result in unacceptable results, limiting the CCF to fewer components may be a clear solution. But, examination of the cut sets from the PRA can help to identify other SSCs or actions that may be credited for mitigation.

A.3 CCF Caused by a Design Defect

This section applies to any *design defect* in one or more controllers, either in a Type 1 Design shown in Figure A-1 (multiple SSCs on one controller) or in a Type 2 design shown in Figure A-1 (one SSC on each controller) as noted for each defensive measure. The following types of *design defect*s are addressed in this section:

- Operating system defect
- Application logic defect

- Embedded digital device defect
- Requirements error or omission
- Data communication defect

The measures listed in this section are a more detailed set of measures that are derived from industry experience and prior EPRI research [20].

A *design defect* cannot cause a CCF until it is activated. For a CCF to occur in a Type 1 design, the defect needs to be activated within a single controller. For a CCF to occur in a Type 2 design, the defect must be common among multiple controllers, and the defect must be activated concurrently in multiple controllers. For a Type 2 design, if the likelihood of concurrent triggers can be significantly reduced and an activated defect can be made self-announcing, thereby allowing the defect to be corrected in all controllers, then the likelihood of CCF is considered to be Level 2. Figure A-18 illustrates these principles (note that the middle figure shows separate but concurrent *activating conditions*):

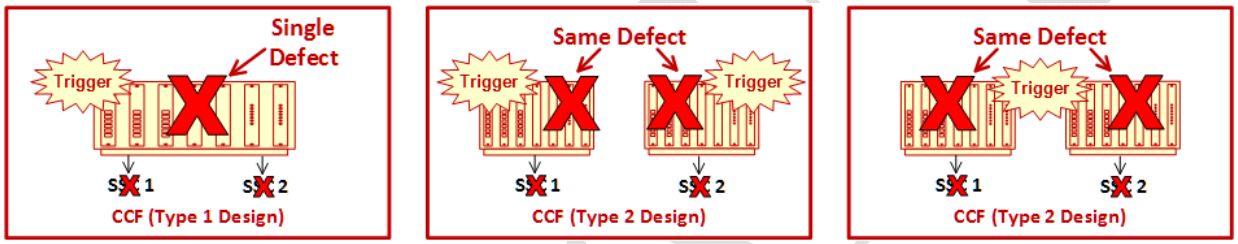


Figure A-18
CCF Caused by an Activated Design Defect

It is noted that duplex and triplex configurations provide no preventive or limiting measure for a *design defect* if the same defect resides in each controller.

Compared to the other I&C failure sources addressed in Sections A.1 (random hardware failure within the I&C), A.2 (environmental disturbance), and A.4 (operations and maintenance error), many of the preventive and limiting measures for SSC malfunctions caused by I&C design defects tend to be more qualitative and subjective, and depend more on specific attributes of the I&C system and the application. For example, what is judged to constitute adequate documentation of software quality may depend on the complexity of the I&C platform and the functional complexity of the application, as well as the safety or operational significance of the potential failure, all of which introduce subjective considerations. Consideration of operating history will involve some judgment regarding the relevance of the operating history to the nuclear plant application, as well as how much successful operating history is enough to be meaningful. Overall assessment of protection against failures caused by design defects will effectively be a subjective, graded approach, with the preventive and/or limiting measures applied accordingly, possibly including consideration of multiple preventive measures to support an overall assurance argument. Additional discussion of causes of CCFs involving design defects and preventive measures that can reduce their likelihood can be found in [20].

In this guide, the likelihood of a CCF caused by a design defect is considered to be at Level 2 if the potential defect and/or its triggering conditions have been adequately managed using preventive measures, for example if the target system has been subjected to robust requirements engineering methods (See also Section 5.2), and then developed and implemented under structured development and quality assurance processes that are joined with defensive design features. These criteria may be applied to safety or non-safety systems and are the underlying basis for some of the preventive and limiting measures described in this section.

A.3.1 Operating System Design Defect

A *design defect* in the operating system can cause one or more controllers to generate erroneous outputs or the outputs to freeze in their current state.

For the purpose of this guideline, an operating system (OS) is the portion of the software that "comes with the box" in the sense that it is generally not configurable by end users, and the OS alone does not perform any application-specific logic that would be designed for influencing or controlled any SSC (which is the subject of Section A.3.2). An OS can be a commercially available, multi-tasking, real-time package available from a third party, or it can be a single task, once-through firmware program designed by the equipment vendor and embedded in their digital product. The only software distinction made in this guideline is that between an OS and application, which often have different characteristics under the control of different entities.

A.3.1.1 Measures Intended to Reduce the Likelihood of a CCF Caused by a Design Defect in the Operating System to Level 2

To reduce the likelihood of a CCF caused by a *design defect* in the operating system, applying one of the measures from Table A-33 (or comparable measures) is recommended.

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

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

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.

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

<table>
<tr><th colspan="3">Preventive Measures</th></tr>
<tr><td></td><td>Safety Divisions
k) Employ a software development process that meets applicable standards and guides (e.g., RG 1.152 in the U.S.), or demonstrate quality equivalence (e.g., commercial grade dedication in the U.S.).
l) Provide defensive measures to reduce the likelihood of unintended software changes during development (e.g. in accordance with RG 1.152 in the U.S.).
m) Provide defensive measures for preventing unintended operating system changes, and detecting unintended operating system changes via periodic testing, when the system is installed.</td><td>Non-safety Division
n) Confirm configuration control, documented requirements and design, and traceability of verification and validation to the documented design requirements by personnel who were not engaged in the design.
o) Confirm good practice security methods during software development.
p) Provide defensive measures for preventing unintended operating system changes when the system is installed.</td></tr>
<tr><td>P2</td><td colspan="2">Same measures as A33-P1, except the low likelihood of a defect is demonstrated through the operating history of the OS in lieu of documented software quality by meeting the following conditions:
a) Substantial and successful operation in multiple different bounding applications of continuous operation without manual or automatic controller reset, or a controller error, including a crash or freeze.
b) The experience base bounds the target application as follows:
1) The software and hardware versions are the same as the target versions. This applies to all operating system software including software for all interfaces and HSIs. Hardware and software problems are reported and promptly and appropriately dispositioned. Hardware and software changes are controlled.
2) The quantity of application program memory is equal to or exceeds the target.
3) The library function blocks encompass all function blocks used in the target.
4) The quantity of modules for each type of I/O is equal to or exceeds the target.
5) The types of data communication interfaces, including interfaces for HSI, encompass the target, and the quantity of each interface type is equivalent to or exceeds the target.
6) The controller’s function processing, I/O processing and communication processing cycle times are equal to or are faster than the target application.</td></tr>
</table>

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

Preventive Measures	
P3	**Demonstrate that a defect will not be activated when the SSC is needed to perform its required function. .** Applicable only where the controlled SSC is normally in the state needed to perform its required function. Include all of the following defensive measures: a) Administrative controls are in place to provide assurance that the time the controlled SSC is not in the state needed to perform its required function is minimal. Therefore, manipulations are of a short duration and the SSC is returned to its required position after any manipulation. b) Administrative controls to provide assurance that any manipulations that put the controlled SSC in an alternate state (i.e., not the required state) occur for only one SSC at a time. This provides assurance that a defect activated by the manipulation will negatively affect only one SSC. c) Alarms or frequent administrative monitoring controls are in place to immediately identify an SSC that is not in its required state. If the SSC is not being intentionally manipulated this would self-announce an activated defect. d) Provide plant procedures that direct failure investigation and correction, with the intention of correcting the defect in all controllers before the defect is likely to be triggered in multiple controllers. e) The positioning features and alarm/monitoring features (defined above) do not rely on any common design features that could result in erroneous SSC positioning and failure to detect that erroneous positioning. f) The digital device has no external inputs or data communication that will change states when the SSC must be in its required position. This provides assurance that there are no potential defect triggers that could erroneously position the SSC away from its required position.
P4	**Employ a different operating system for each controller so that a failure caused by a design defect in one controller is less likely to affect multiple SSCs.** Applicable only where there are separate controllers controlling individual SSCs. If this preventive measure is applied to controllers in different divisions of a safety system for the same safety function, the impact on Technical Specification Completion Times (CT) and Bypass Times (BT) is assessed, because the safety function relies on internal diversity within the safety system to reduce the likelihood of a CCF, and that diversity is adversely affected when a division is taken out of service. On the other hand, if a diverse backup system is employed to cope with a safety system CCF, then the diversity is not adversely affected when a division of the safety system is taken out of service.

A.3.1.2 Limiting a CCF Caused by a Design Defect in the Operating System

If none of the preventive measures provided above are implemented, or if one is only partially implemented, then one of the limiting measures in Table A-34 may be helpful.

Table A-34
Measures for Limiting a CCF Caused by a Design Defect in the Operating System

<table>
<tr><th colspan="3">Limiting Measures</th></tr>
<tr><td>L1</td><td colspan="2">Reduce the likelihood of defects through documented software quality and a simple OS, and provide assurance that an activated defect forces the affected controller(s) to a predictable shutdown state. This measure is applicable to a Type 1 Design or a Type 2 Design with a) insufficient controller differences or b) an activated defect is not detectable (in either case, triggering of a defect in multiple controllers cannot be prevented.) See Section A.3.6 for guidance on coping with a CCF caused by an operating system defect.
a) Single task operating system (OS steps are invariant during plant operation (“blind” to plant transients), so plant transients cannot trigger design defects in the OS).
b) Static memory allocation.
c) Execution of all function blocks applicable to the application in a cyclical non-varying manner, regardless of the input states to each function block (i.e., no branching that would skip a function block).
d) Function processing that is completely independent and asynchronous of I/O processing and digital data communication processing (i.e., separate processors for function, communication and I/O with shared memory for data exchange).
e) Watchdog timers to detect scan overrun and underrun conditions, with forced shutdown condition on a watchdog timeout. Watchdog timers have no reliance on the function processor that is executing the software for which they are detecting scan overrun and underrun conditions.
f) Buffer overflow detection with forced shutdown.
g) Exception handlers for situations such as out of range inputs, calculated results (e.g., divide by zero), or not-a-number (NaN). Exception handlers provide predefined data defaults to reduce the likelihood of controller shutdown.
h) Provide a high quality software development process in accordance with the table below.</td></tr>
<tr><td></td><td>Safety Divisions
i) Employ a software development process that meets applicable standards and guides (e.g., RG 1.152 in the U.S.), or demonstrate quality equivalence (e.g., commercial grade dedication in the U.S.).
j) Provide defensive measures to reduce the likelihood of unintended software changes during development (e.g. in accordance with RG 1.152 in the U.S.).
k) Provide defensive measures for preventing unintended operating system changes, and detecting unintended operating system changes via periodic testing, when the system is installed.</td><td>Non-safety Division
l) Confirm configuration control, documented requirements and design, and traceability of verification and validation to the documented design requirements by personnel who were not engaged in the design.
m) Confirm good practice security methods during software development.
n) Provide defensive measures for preventing unintended operating system changes when the system is installed.</td></tr>
</table>

Table A-34 (continued)
Measures for Limiting a CCF Caused by a Design Defect in the Operating System

Limiting Measures	
L2	**Same as A34-L1, except low likelihood of a defect is demonstrated through operating history of the OS in lieu of documented software quality by also demonstrating that the operating history of the OS meets the same conditions listed under A33-P2**.
L3	**Provide all of the same measures as A33-P1, but limit the number of SSCs that share a controller**. When a common operating system is applied to all controllers, but each controller controls multiple SSCs, the defensive measures in P1 limit the CCF to the SSCs controlled by a single controller. This is different than the generic limiting measure (limit the number of SSCs that share a CCF source), because the application of the operating system with the *design defect* is not limited.
L4	**Provide all of the same measures as A33-P2, but limit the number of SSCs that share a controller**. When a common operating system is applied to all controllers, but each controller controls multiple SSCs, the defensive measures in P2 limit the CCF to the SSCs controlled by a single controller. This is different than the generic limiting measure (limit the number of SSCs that share a CCF source) because the application of the operating system with the *design defect* is not limited.
L5	**Provide all of the same measures as A33-P4, except that each controller controls multiple SSCs.** Therefore a design defect in one controller can result in spurious actuation of multiple SSCs in that controller.

A.3.2 Application Software Design Defect

A *design defect* in the application software can cause one or more controllers to generate erroneous outputs or the outputs to freeze in their current state. The term "application logic" in this guideline is intended to indicate software that is purposely designed for any given controlled SSC to meet its functional requirements. Application logic can be a binary executable, or it can be a data file that is used by a controller's operating system to create a unique instance that is tailored for specific SSCs. Application logic can be viewed by various tools in a variety of formats, including source code, function block diagrams, assembly language, etc.

A.3.2.1 Measures Intended to Reduce the Likelihood of a CCF Caused by a Design Defect in the Application Logic to Level 2

To reduce the likelihood of a CCF caused by a *design defect* in the application logic, applying one of the preventive measures in Table A-35 (or comparable measures) is recommended.

Table A-35
Measures Intended to Reduce the Likelihood of a CCF Caused by a Design Defect in the Application Logic to Level 2

<table>
<tr><th colspan="3">Preventive Measures</th></tr>
<tr><td>P1</td><td colspan="2">Provide distinct requirements and application logic for each controlled SSC (functional/ signal diversity). This measure is applicable to a Type 1 Design or a Type 2 Design. Application differences reduces the likelihood that the same defect will exist for multiple SSCs. This measure does not consider multiple different design defects.
a) Each SSC is specified with different functional requirements (refer to Section A.3.4 for measures related to requirements errors or omissions), including:
1) different control algorithms
2) different process inputs (via I/O modules and data communications) (signal diversity)
b) Provide a high quality software development process in accordance with the table below.</td></tr>
<tr><td></td><td>Safety Divisions
c) Employ a software development process that meets applicable standards and guides (e.g., RG 1.152 in the U.S.), or demonstrate quality equivalence (e.g., commercial grade dedication in the U.S.).
d) Provide defensive measures (e.g., secure development environment) to reduce the likelihood of unintended software changes during development (e.g. in accordance with RG 1.152 in the U.S.).
e) Provide defensive measures for preventing unintended operating system changes, and detecting unintended operating system changes via periodic testing, when the system is installed.</td><td>Non-safety Division
f) Confirm configuration control, documented requirements and design, and traceability of verification and validation to the documented design requirements by personnel who were not engaged in the design.
g) Confirm good practice security methods during software development.
h) Provide defensive measures for preventing unintended operating system changes when the system is installed.</td></tr>
<tr><td>P2</td><td colspan="2">Perform extensive testing, and provide high software quality. This preventive measure can be applied regardless of application logic differences, and it is applicable to Type 1 or Type 2 designs.
a) Perform extensive testing of the application software including all external and internal state combinations. If all state combinations cannot be achieved also provide an analysis to demonstrate that untested state combinations are irrelevant [Ref 35].
b) Requirements are complete and correct per Section A.3.4.1.
c) Provide a high quality software development process in accordance with the table below.</td></tr>
</table>

Table A-35 (continued)
Measures Intended to Reduce the Likelihood of a CCF Caused by a Design Defect in the Application Logic to Level 2

Preventive Measures		
	Safety Divisions d) Employ a software development process that meets applicable standards and guides (e.g., RG 1.152 in the U.S.), or demonstrate quality equivalence (e.g., commercial grade dedication in the U.S.). e) Provide defensive measures to reduce the likelihood of unintended software changes during development (e.g. in accordance with RG 1.152 in the U.S.). f) Provide defensive measures for preventing unintended operating system changes, and detecting unintended operating system changes via periodic testing, when the system is installed.	**Non-safety Division** g) Confirm configuration control, documented requirements and design, and traceability of verification and validation to the documented design requirements by personnel who were not engaged in the design. h) Confirm good practice security methods during software development. i) Provide defensive measures for preventing unintended operating system changes when the system is installed.
P3	**Same as A33-P3 for an operating system defect**.	
P4	**Employ some form(s) of diversity such that a failure caused by a design defect in a controller is unlikely to affect more than one SSC.** Applicable only where there are separate controllers controlling individual SSCs. If this preventive measure is applied to controllers in different divisions of a safety system for the same safety function, the impact on Technical Specification Completion Times (CT) and Bypass Times (BT) must be assessed, because the safety function relies on internal diversity within the safety system to reduce the likelihood of a CCF, and that diversity is adversely affected when a division is taken out of service. On the other hand, if a diverse backup system is employed to cope with a safety system CCF, then the diversity is not adversely affected when a division of the safety system is taken out of service.	

A.3.2.2 Limiting a CCF Caused by a Design Defect in the Application Logic

If none of the preventive measures provided above are implemented, or if one is only partially implemented, then one of the measures in Table A-36 may be helpful.

Table A-36
Measures for Limiting a CCF Caused by a Design Defect in the Application Logic

<table>
<tr><th colspan="3">Limiting Measures</th></tr>
<tr><td>L1</td><td colspan="2">Reduce likelihood of defects through documented software quality and detect activating conditions in order to force the affected controller(s) to a shutdown state. This measure is applicable to a Type 1 Design or a Type 2 Design where the same functional requirements are specified for multiple SSCs, and concurrent triggering of a defect cannot be prevented. See Section A.3.6 for guidance on coping with a CCF caused by a defect in the application logic.
a) Different algorithm implementations for the same control function, with output compare function. The output compare function forces the controller to a predetermined shutdown state when the controller outputs have unexpected differences (e.g., based on tolerance and timing).
b) Watchdog timer 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.
c) Provide a high quality software development process in accordance with the table below.</td></tr>
<tr><td></td><td>Safety Divisions
d) Employ a software development process that meets applicable standards and guides (e.g., RG 1.152 in the U.S.), or demonstrate quality equivalence (e.g., commercial grade dedication in the U.S.).
e) Provide defensive measures to reduce the likelihood of unintended software changes during development (e.g. in accordance with RG 1.152 in the U.S.).
f) Provide defensive measures for preventing unintended operating system changes, and detecting unintended operating system changes via periodic testing, when the system is installed.</td><td>Non-safety Division
g) Confirm configuration control, documented requirements and design, and traceability of verification and validation to the documented design requirements by personnel who were not engaged in the design.
h) Confirm good practice security methods during software development.
i) Provide defensive measures for preventing unintended operating system changes when the system is installed.</td></tr>
<tr><td>L2</td><td colspan="2">Provide all of the same measures as A35-P1, but limit the number of SSCs that share the same or similar application logic. Other defensive measures in P1 are applicable to reduce the likelihood of a defect and thereby allow the resulting CCF to be considered a beyond design basis event. Therefore, this is different than the generic limiting measure (limit the number of SSCs that share a CCF source) which puts no conditions on the likelihood of the source failure.</td></tr>
<tr><td>L3</td><td colspan="2">Provide all the same measures as A35-P4, except that each controller controls multiple SSCs. Therefore a design defect in one controller can result in spurious actuation of multiple SSCs in that controller.</td></tr>
</table>

A.3.3 Embedded Digital Devices

For the purposes of this guide, an embedded digital device is one that meets the following conditions:

1. Meets the definition of "digital"
2. Performs a single function
3. Has limited inputs
4. Has limited configurability via predefined parameters and parameter ranges
5. Has no application programming

An embedded single function device can exist at any layer of the control architecture. Therefore, it can negatively affect both Type 1 and Type 2 designs. Note that an embedded digital device may exist in plant components that are not necessarily identified as digital I&C equipment, such as:

- UPS
- Sensor
- Motor Starter
- Pneumatic valve positioner
- Relay

A.3.3.1 Measures Intended to Reduce the Likelihood of a CCF Caused by a Design Defect in an Embedded Digital Device to Level 2

To reduce the likelihood of a CCF caused by a design defect in an embedded digital device, applying one of the preventive measures in Table A-37 (or comparable measures) is recommended.

Table A-37
Measures Intended to Reduce the Likelihood of a CCF Caused by a Design Defect in an Embedded Digital Device to Level 2

Preventive Measures	
P1	**Perform extensive testing via the following measures:** a) Test the embedded digital device for all external and internal state combinations. If all state combinations cannot be achieved also provide an analysis to demonstrate that untested state combinations are irrelevant. (There are many possible internal state combinations in memory, data processing, etc. that have the potential to cause erroneous controller behavior. In addition, unused inputs, in combination with internal states, also have the potential to cause erroneous controller behavior if the unused input states are not what they are assumed to be.) b) Provide a secure operational environment per applicable guides and standards (e.g., RG 5.71 or NEI 08-09 in the U.S.). For safety systems, provide measures for detecting unintended software changes through periodic testing.
P2	**Provide assurance that a substantial and successful operating history bounds the target application by providing the following measures**: a) Substantial and successful operation without device reset for many different bounding applications. b) The experience base bounds the target application as follows: 1) The software and hardware versions are the same as the target versions. Hardware and software problems are reported and promptly and appropriately dispositioned. Hardware and software changes are controlled. 2) The configuration settings are the same as the target application. 3) The interfaces are the same as the target application. c) Provide a secure operational environment per applicable guides and standards (e.g., RG 5.71 or NEI 08-09 in the U.S.). For safety systems, provide measures for detecting unintended software changes through periodic testing. (This is to provide an active means for detecting unintended (not malicious) changes.)
P3	**Provide assurance that a defect will not be activated concurrently for multiple embedded devices**. This measure is applicable only were the controlled SSCs are in continuous modulation or frequently repositioned, so that an activated defect will immediately affect the controlled SSC, and is therefore self-announcing. Include all of the following additional measures: a) Provide assurance that inputs and outputs for each embedded device have different sources/destinations using the same type of I/O is acceptable. b) Provide an HFE evaluation to demonstrate that control room HSI allows operators to quickly detect the adverse control condition. c) Provide plant procedures that direct failure investigation and correction, with the intention of correcting the defect in all controllers before the defect is likely to be activated in multiple controllers. d) Provide a secure operational environment per applicable guides and standards (e.g., RG 5.71 or NEI 08-09 in the U.S.). For safety systems, provide measures for detecting unintended software changes through periodic testing.

Table A-37 (continued)
Measures Intended to Reduce the Likelihood of a CCF Caused by a Design Defect in an Embedded Digital Device to Level 2

Preventive Measures	
P4	**Same as A33-P3 for an operating system defec**t.
P5	**Employ diverse embedded digital devices for each SSC so that a design defect in one embedded digital device is unlikely to affect more than one SSC.** Applicable only where there are different embedded digital devices controlling individual SSCs. If this preventive measure is applied to embedded digital devices in different divisions of a safety system for the same safety function, the impact on Technical Specification Completion Times (CT) and Bypass Times (BT) must be assessed, because the safety function relies on internal diversity within the safety system to reduce the likelihood of a CCF, and that diversity is adversely affected when a division is taken out of service. On the other hand, if a diverse backup system is employed to cope with a safety system CCF, then the diversity is not adversely affected when a division of the safety system is taken out of service.

A.3.4 Requirements Error or Omission

An error or omission in the requirements used to develop the target application can result in a CCF, including erroneous outputs or frozen outputs in one or more controllers.

A.3.4.1 Measures Intended to Reduce the Likelihood of a CCF caused by a Requirements Error or Omission to Level 2

To reduce the likelihood of a CCF caused by a requirements error or omission, applying one of the measures from Table A-38 (or comparable measures) is recommended.

Table A-38
Measures Intended to Reduce the Likelihood of a CCF caused by a Requirements Error or Omission to Level 2

Preventive Measures	
P1	**Employ the same legacy I&C system requirements without any changes.** The basis for this measure is that the likelihood of a CCF caused by an error or omission in I&C legacy system requirements is already considered to be at Level 2 (i.e., a CCF due to an error or omission is likely to have been discovered and corrected in the life of the legacy system). This measure is not applicable if a digital system results in any differences in requirements from a legacy analog system being replaced (see A38-P2, below, for changed requirements). Provide all of the following measures: a) Documented legacy system requirements are captured in a requirements specification for the replacement system. b) Implied requirements for the legacy I&C system, such as functional and physical assumptions and constraints described in the plant safety analysis, are explicitly stated in a requirements specification for the replacement system. c) Independent verification demonstrates that the replacement system requirements are complete and unambiguous. A requirements traceability matrix is one method of ensuring requirements completeness.

Table A-38 (continued)
Measures Intended to Reduce the Likelihood of a CCF caused by a Requirements Error or Omission to Level 2

Preventive Measures	
P2	**If legacy requirements are changed, then systematically define, analyze and verify new requirements**. Provide the following measures: a) Requirements are explicitly stated in a requirements specification b) The requirements specification clearly differentiates legacy system requirements (that are unchanged) from changed requirements or new requirements c) Independent verification demonstrates that replacement system requirements are unambiguous and complete. A requirements traceability matrix is one method of ensuring requirements completeness. d) Hazard analysis demonstrates that hazards are identified, then prevented or mitigated through specific requirements or design constraints (including functional or physical constraints; reference EPRI 3002000509). Hazard analysis methods include FMEA, FTA, or other methods described in EPRI 3002000509.

A.3.5 Data Communications Design Defect

A *design defect* that is activated in a data communication network can result in one of the following conditions:

Condition 1 Loss of All Data
Condition 2 Data Storm
Condition 3 Erroneous Data

The measures for protecting against a CCF caused by an activated data communications design defect (described here) are differentiated from those that protect against a CCF caused by a single failure in the data communications (described in Section A.1), because a single failure adversely affects only one data communication interface, where as a design defect can adversely affect all data communication interfaces that share the same design; this includes redundancy communication interfaces and communication interfaces in different systems or segments. However, the measures are similar in some ways; for example, a loss of data condition can be caused by either failure source, and a hardwired backup in either case can be equally effective

A.3.5.1 Data Communications Design Defect Condition 1 (Loss of All Data)

Loss of all data can result in loss of manual control capability from operator workstations and/or loss of control signals between controllers for all controllers that share the same communication network or the same communication network design. All SSCs that rely on the digital communication interface for manual and/or automatic control input signals lose those control signals, as shown in Figure A-19.

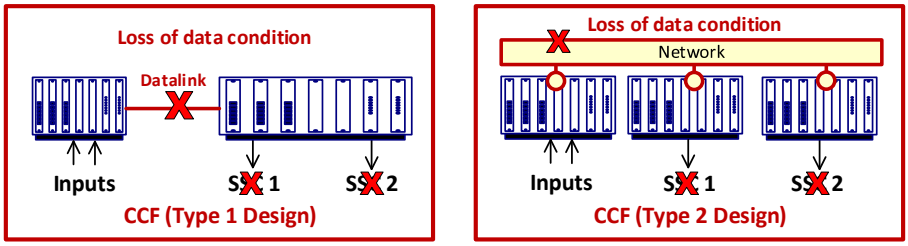


Figure A-19
CCF Caused by Data Communications Design Defect Condition 1 (Loss of All Data)

This failure would appear to be bounded by the loss of all data caused by a random hardware failure as described in Section A.1.5.1. However, a random hardware failure affects *one* communication interface of a redundant pair or *one* communication interface of multiple communication interfaces that share the same design. On the other hand, a *design defect* can affect *all* communication interfaces that share the same design, redundant or separate. Therefore, preventive and limiting measures for a *design defect* are not the same as those for a random hardware failure.

Measures Intended to Reduce the Likelihood of a CCF Caused by Data Communications Design Defect Condition 1 (Loss of All Data) to Level 2

To reduce the likelihood of a CCF caused by Condition 1 caused by an activated *design defect*, applying one of the measures from Table A-39 (or comparable measures) is recommended.

Table A-39
Measures Intended to Reduce the Likelihood of a CCF caused by Data Communications Design Defect Condition 1 (Loss of All Data) to Level 2

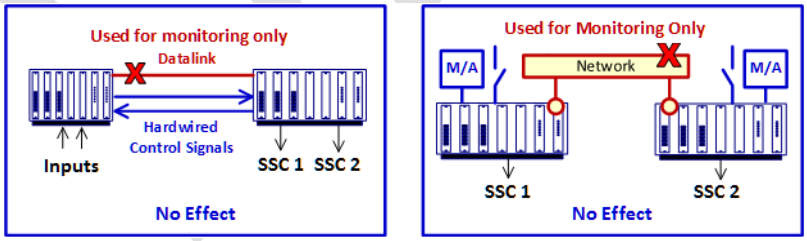
Preventive Measures	
P1	**Hardwire operator manual control signals and/or control signals between controllers.** Data communications may be used for other purposes, but not for control signals. For example, the figure on the left shows a shared datalink, but the control signals necessary for any SSC are hardwired (in this case, between controllers); the network is used only for monitoring. Likewise, the figure on the right shows a shared network, but operator control signals are hardwired for each SSC (in this case, dedicated switches and/or manual/auto (M/A) stations for each SSC).  Caution: Hardwired control signal schemes should be assessed for their reliability. In some cases, network reliability may be better than hardwired reliability.

Table A-39 (continued)
Measures Intended to Reduce the Likelihood of a CCF caused by Data Communications Design Defect Condition 1 (Loss of All Data) to Level 2

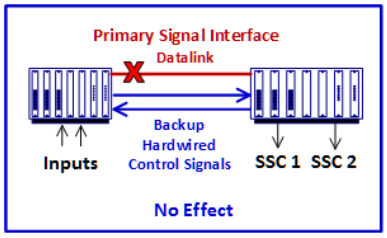
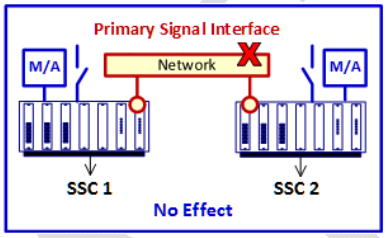
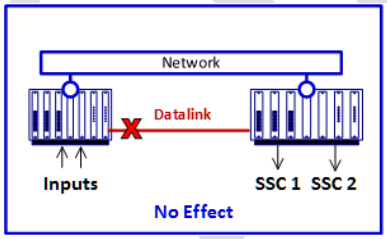
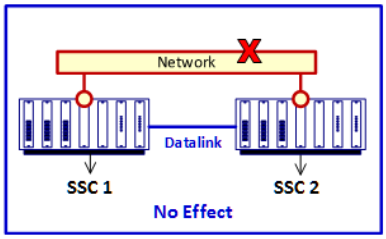
Preventive Measures	
P2	**Use the communication interface as the primary control interface, but provide backup hardwired interfaces for operator manual control signals and/or control signals between controllers**. Do not use digital data communication media for the backup. Note that manual transfer between control sources is not needed, because the assumed failure is loss of data from the network, not erroneous data. Therefore, duplicate signals can be combined using simple OR logic. For example, the figure on the left shows a shared datalink as the primary control signal interface, but hardwired backup control signals are also provided. Likewise, the figure on the right shows a shared network as the primary control signal interface, but backup operator control signals are hardwired for each SSC (in this case, dedicated switches and/or manual/auto (M/A) stations for each SSC).   Caution: Hardwired control signal schemes should be assessed for their reliability. In some cases, network reliability may be better than hardwired reliability.
P3	**Use the communication interface as the primary control interface, but provide a diverse backup digital communication interface for operator manual control signals and/or control signals between controllers**. For example, as shown in the figures below, if a network is the primary interface, a data link could be the backup. Note that manual transfer between control signal sources is not needed, because the failure assumed is loss of data from the primary interface, not erroneous data. Therefore, duplicate signals can be combined using simple OR logic.  

Table A-39 (continued)
Measures Intended to Reduce the Likelihood of a CCF caused by Data Communications Design Defect Condition 1 (Loss of All Data) to Level 2

<table>
<tr><th colspan="3">Preventive Measures</th></tr>
<tr><td>P4</td><td colspan="2">Reduce the likelihood of a communication interface design defect. Provide all of the following measures listed below to meet the intent of reducing the likelihood of a design defect in the communication interface to Level 2.
a) All data is updated using a fixed deterministic cycle, where all data is broadcast to all nodes, with each node broadcasting a fixed message length every cycle.
b) Messages from operator workstations are broadcast to all nodes using the same deterministic manner as above, including fixed length messages, but the data within each message varies depending on the operator control command from that workstation.
c) Where multiple nodes transmit data on the same communication interface (i.e., a network), all nodes transmit their data in a fixed sequence, repeated deterministically in every communication cycle.
d) Each node includes a watchdog timer to detect when a broadcast from a predecessor node on the same communication interface (i.e., network) has not occurred, thereby allowing the node to initiate its own data broadcast. The watchdog timer has no reliance on the messages from the predecessor nodes.
e) Provide transmit and receive communication processors with their own deterministic cycles that are independent and asynchronous from the function processor (SSC processor) of each controller, so that erratic operation of a function processor will not affect the deterministic operation of the network. Transmit and receive communication processors can be combined for the same communication interface, but they are independent from the function processor.
f) To facilitate independent asynchronous operation, the communication processors (both send and receive) and function processors exchange data via shared memory with memory arbitration circuits that provide assurance of deterministic communication processing.
g) All broadcast data is deposited in the shared memory, facilitating deterministic data communication; the function processor reads only the data pertinent to its applications.
h) Each node includes detection and rejection of corrupted data (e.g. CRC algorithm) before data is deposited in shared memory.
i) Data messages include indication of correctly refreshed (updated) data. Each node includes a watchdog timer to detect unexpected valid data update delay. The watchdog timer has no reliance on the messages from the predecessor nodes.
j) Provide a high quality software development process in accordance with the table below:</td></tr>
<tr><td></td><td>Safety Divisions
k) Employ a software development process that meets applicable standards and guides (e.g., RG 1.152 in the U.S.), or demonstrate quality equivalence (e.g., commercial grade dedication in the U.S.).
l) Provide defensive measures to reduce the likelihood of unintended software changes during development (e.g. in accordance with RG 1.152 in the U.S.).
m) Provide defensive measures for preventing unintended operating system changes, and detecting unintended operating system changes via periodic testing, when the system is installed.</td><td>Non-safety Division
n) Confirm configuration control, documented requirements and design, and traceability of verification and validation to the documented design requirements by personnel who were not engaged in the design.
o) Confirm good practice security methods during software development.
p) Provide defensive measures for preventing unintended operating system changes when the system is installed.</td></tr>
</table>

Table A-39 (continued)
Measures Intended to Reduce the Likelihood of a CCF caused by Data Communications Design Defect Condition 1 (Loss of All Data) to Level 2

Preventive Measures	
	Note that since this method prevents this failure through features of the network that are also the potential source of this failure, a CCF coping analysis is recommended, using "best estimate" methods, to demonstrate tolerance to a complete failure of a redundant communication interface. This analysis is limited to a single (albeit redundant) communication interface, not all separate communication interfaces that share the same design, because the likelihood of a defect being activated concurrently on all separate communication interfaces is very low. The CCF coping analysis for a communication interface demonstrates that this CCF is bounded by beyond design basis acceptance criteria, because the failure is caused by a *design defect*, not a random component failure. If the communication interface is used for both manual control from operator workstations and control signals between controllers, the CCF analysis assumes both have failed. The coping analysis may credit other unaffected SSCs. This recommendation is a defense-in-depth measure that does not negate the CCF likelihood of "Level 2" conclusion for this preventive measure. To facilitate a successful CCF coping analysis, the following additional defensive measures are recommended: q) All detected data anomalies result in a MCR alarm. A CCF coping analysis includes an HFE evaluation to demonstrate that the control room HSI allows operators to quickly detect the adverse control condition. r) All detected data anomalies result in transition to controller algorithms for failed communication inputs. Define reaction to communication interface failure in application programs of each controller, such as setting a failed input signal to low, high or last good value.

Limiting a CCF Caused by Data Communications Design Defect Condition 1 (Loss of All Data)

If none of the preventive measures provided above are implemented, or if one is only partially implemented, then one of the measures from Table A-40 may be helpful.

Table A-40
Measures for Limiting a CCF caused by Data Communications Design Defect Condition 2 (Loss of All Data)

Limiting Measures	
L1	**Use different communication interface configurations to limit the CCF to the SSCs that share a communication interface.** This measure is applicable where there are multiple communication interfaces of the same design and a failure of a communication interface is immediately detectable. Design measures reduce the likelihood of a defect. Communication interface configuration differences reduce the likelihood of the defect being activated concurrently in multiple communication interfaces. Other measures provide assurance that an activated defect is detectable and corrected before it is activated in multiple communication interfaces, thereby limiting the CCF to SSCs controlled by a single communication interface. A CCF coping analysis demonstrates that this CCF is bounded by beyond design basis acceptance criteria. If the communication interface is used for both manual control from operator workstations and control signals between controllers, the CCF analysis assumes both have failed. The coping analysis may credit other unaffected SSCs. Apply all of the following measures: a) Different quantities and configurations of data messages for different communication interfaces. b) Different communication interface cycle times. c) Different communication interface loading. d) Detection and rejection of corrupted data (e.g., CRC). e) Watchdog timers to detect unexpected delays in valid data update. Watchdog timers have no reliance on the communication processors that may be the source of data update delay. f) Continuous on-line frozen data detection. Communication interfaces whose data remains in the same state for extended time durations, can fail in a non-announcing as-is mode. To provide assurance that this failure is immediately detectable, and thereby reduce the likelihood of single communication interface failures from accumulating over time to become multiple communication interface failures, the data is frequently and automatically cycled to force state changes. The typical self-diagnostics provided with data communication interfaces, such as CRC and other data validity checks, are not sufficient to detect frozen data bits. g) All detected data anomalies result in a MCR alarm. Provide an HFE evaluation to demonstrate that control room HSI allows operators to quickly detect the adverse control condition. h) Provide plant procedures that direct failure investigation and correction, with the intention of correcting the defect in all communication interfaces before the defect is likely to be activated in multiple communication interfaces. i) All detected data anomalies result in transition to controller algorithms for failed communication inputs. Define reaction to communication interface failure in application programs of each controller, such as setting a failed input signal to low, high or last good value. j) Provide a high quality software development process in accordance with the table below.

Table A-40 (continued)
Measures for Limiting a CCF caused by Data Communications Design Defect Condition 2 (Loss of All Data)

Limiting Measures		
	Safety Divisions	**Non-safety Division**
	k) Employ a software development process that meets applicable standards and guides (e.g., RG 1.152 in the U.S.), or demonstrate quality equivalence (e.g., commercial grade dedication in the U.S.). l) Provide defensive measures to reduce the likelihood of unintended software changes during development (e.g. in accordance with RG 1.152 in the U.S.). m) Provide defensive measures for preventing unintended operating system changes, and detecting unintended operating system changes via periodic testing, when the system is installed.	n) Confirm configuration control, documented requirements and design, and traceability of verification and validation to the documented design requirements by personnel who were not engaged in the design. o) Confirm good practice security methods during software development. p) Provide defensive measures for preventing unintended operating system changes when the system is installed.

A.3.5.2 Data Communications Design Defect Condition 2 (Data Storm)

For Condition 2, data can be lost (as in Condition 1), or data can be unpredictably delayed. In addition, a controller can get overloaded in trying to keep up with the data overload. The result may be unpredictable erroneous controller behavior, even if the controller does not rely on the data communications interface for control signals. Figure A-20 illustrates the result.

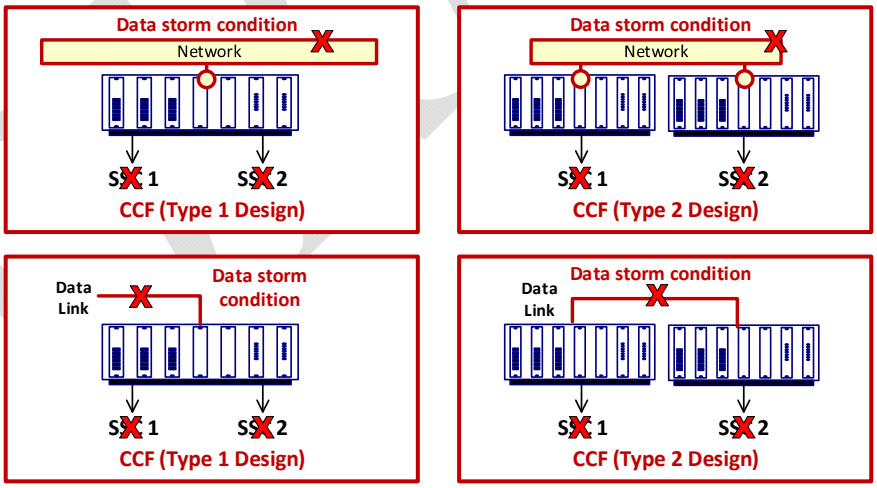


Figure A-20
CCF Caused by Data Communications Design Defect Condition 2 (Data Storm)

This failure would appear to be bounded by the data storm condition caused by a random hardware failure as described in Section A.1.5.2. However, a random hardware failure affects *one* communication interface of a redundant pair or *one* communication interface of multiple communication interfaces that share the same design. On the other hand, a *design defect* can negatively affect *all* communication interfaces that share the same design, redundant or separate.

Therefore, preventive and limiting measures for a *design defect* are not the same as those for a random hardware failure.

Measures Intended to Reduce the Likelihood of a CCF Caused by Data Communications Design Defect Condition 2 (Data Storm) to Level 2

To reduce the likelihood of a CCF caused by Condition 2 caused by an activated *design defect*, applying one of the measures from Table A-41 (or comparable measures) is recommended.

Table A-41
Measures Intended to Reduce the Likelihood of a CCF caused by Data Communications Design Defect Condition 2 (Data Storm) to Level 2

Preventive Measures	
P1	**Same as A11-P1 for data storm caused by a random hardware failure, plus A39-P1 or A39-P2 for loss of data caused by a design defect**. While a random hardware failure that causes a data storm can only affect a single communication interface, a data storm caused by an activated design defect has the potential to affect all communication interfaces that share the same design, which can result in a loss of all data from redundant communication interfaces and/or separate communication interfaces. Therefore, A11-P1 for a data storm (caused by a random hardware failure) allows controllers to continue functioning, but adding A39-P1 or A39-P2 for loss of data (caused by a design defect) allows controllers to continue transmitting and receiving control signals.
P2	**Same as A11-P2 for data storm caused by a random hardware failure, plus A39-P1 or A39-P2 for loss of data caused by a design defect**. While a random hardware failure that causes a data storm can only affect a single communication interface, a data storm caused by an activated design defect has the potential to affect all communication interfaces that share the same design, which can result in a loss of all data from redundant communication interfaces and/or separate communication interfaces. Therefore, A11-P2 for a data storm (caused by a random hardware failure) allows controllers to continue functioning, but adding A39-P1 or A39-P2 for loss of data (caused by a design defect) allows controllers to continue transmitting and receiving control signals.
P3	**Same as A39-P4 for loss of data caused by a design defect to reduce the likelihood of a communication interface design defect**.

Limiting a CCF Caused by Data Communications Design Defect Condition 2 (Data Storm)

If none of the preventive measures provided above are implemented, or if one is only partially implemented, then one of the measures from Table A-42 may be helpful.

Table A-42
Design Measures for Limiting a CCF Data Communications Design Defect Condition 2 (Data Storm)

Limiting Measures	
L1	**Same as A11-P1 for data storm caused by a random hardware failure, plus A40-L1 for loss of data caused by a design defect.** While a random hardware failure that causes a data storm can only affect a single communication interface, a data storm caused by an activated *design defect* has the potential to affect all communication interfaces that share the same design, which can result in a loss of all data from redundant communication interfaces and/or separate communication interfaces. Therefore, A11-P1 for a data storm (caused by a random hardware failure) allows controllers to continue functioning, but adding A40-L1 (for loss of data caused by a *design defect*) limits the effect to the SSCs that share a single communication interface.

A.3.5.3 Data Communications Design Defect Condition 3 (Erroneous Data)

Erroneous data caused by a *design defect* activated in the data network can result in unpredictable erroneous controller behavior. Figure A-21 illustrates the result.

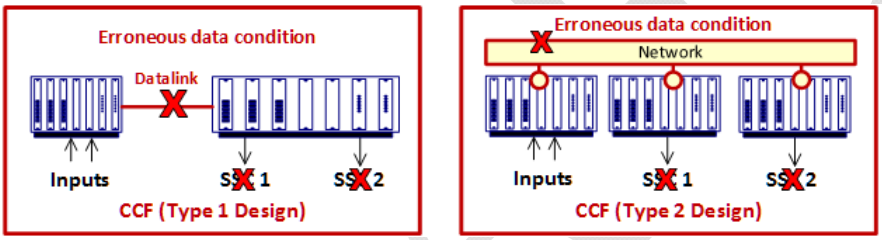


Figure A-21
CCF Caused by Data Communications Design Defect Condition 3 (Erroneous Data)

This failure would appear to be bounded by the erroneous data condition caused by a random hardware failure as described in Section A.1.5.3. However, a random hardware failure affects *one* communication interface of a redundant pair or *one* communication interface of multiple communication interfaces that share the same design. On the other hand, a *design defect* can negatively affect *all* communication interfaces that share the same design, redundant or separate. Therefore, preventive and limiting measures for a *design defect* are not the same as those for a random hardware failure.

Measures Intended to Reduce the Likelihood of a CCF Caused by Data Communications Design Defect Condition 3 (Erroneous Data) to Level 2

To reduce the likelihood of a CCF caused by data communications design defect Condition 3, applying one of the measures from Table A-43 (or comparable measures) is recommended.

Table A-43
Measures Intended to Reduce the Likelihood of a CCF caused by Data Communications Design Defect Condition 3 (Erroneous Data) to Level 2

Preventive Measures	
P1	**Same as A13-P1 for erroneous data caused by a random hardware failure, plus A41-P1 or A41-P2 for loss of data caused by a design defect**. While a random hardware failure that causes erroneous data can only affect a single communication interface, erroneous data caused by an activated *design defect* has the potential to affect all communication interfaces that share the same design. P1 rejects erroneous data, which gives the same result as loss of all data from redundant communication interfaces and/or separate communication interfaces. Therefore, A13-P1 (for erroneous data caused by a random hardware failure) allows controllers to continue functioning without any erroneous data, but adding A41-P1 or A41-P2 for loss of data (caused by a *design defect*) allows controllers to continue transmitting and receiving control signals.
P2	**Same as A13-P2 for erroneous data caused by a random hardware failure**. Data communications may be used for other purposes, but not for control signals.
P3	**Same as A39-P4 for loss of data to reduce the likelihood of a communication interface design defect**.

Limiting a CCF Caused by Data Communications Design Defect Condition 3 (Erroneous Data)

If none of the preventive measures provided above are implemented, or if one is only partially implemented, then one of the measures from Table A-44 may be helpful.

Table A-44
Measures for Limiting a CCF caused by Data Communications Design Defect Condition 3 (Erroneous Data)

Preventive Measures	
L1	**Same as A14-L1 for erroneous data caused by a random hardware failure, plus A41-P1 or A41-P2 for loss of data caused by a design defect**. While a random hardware failure that causes erroneous data can only affect a single communication interface, erroneous data caused by an activated *design defect* has the potential to affect all communication interfaces that share the same design. In this case, the watchdog timer, independent from the functions processor, invoked by A14-L1 results in an alarm, and A41-P1 or A41-P2 provide an alternate means for transmitting and receiving control signals.

A.3.6 Coping with a CCF Caused by a Design Defect

The effect of a design defect in a controller is bounded by the failures that can lead to an internal controller error as described in Section A.1.8, because a software design defect can only manifest itself in the context of its host hardware. For example, a design defect in a controller would have the same effect as a shared memory hardware error in that controller. Therefore, the limiting measures in this section are needed for a Type 1 controller design, only if the likelihood of an internal controller error failure has not been adequately reduced.

Diversity to promote the non-concurrent triggering of a design defect may include differences in software, cycle time, CPU load, I/O configuration, automated diagnostics, etc. The more differences that exist among the controllers, the easier it is to defend that activating conditions are likely to be non-concurrent. It is important to note that these differences alone are not sufficient to preclude consideration of all activating conditions. Therefore, non-concurrent

activating conditions are still considered for a defect that leads to a failure that is not self-announcing. Failures that are not self-announcing remain hidden and the result is a CCF.

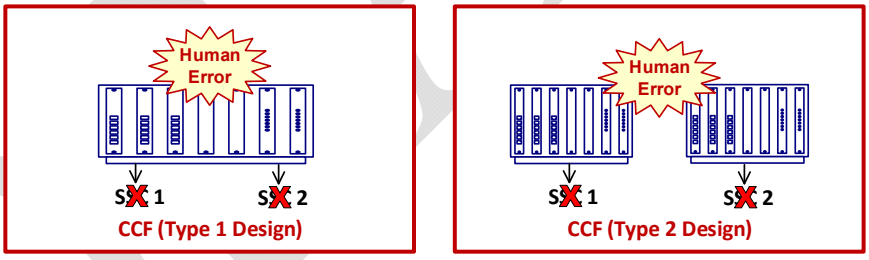
An activated design defect that leads to a CCF of safety SSCs (i.e., with a Level 1 likelihood) is likely to need diverse equipment to provide backup automatic or manual functions to achieve a successful coping analysis (i.e., to mitigate the CCF). The diverse backup equipment does not need to duplicate the functions of the failed controllers. Instead, the functionality of the diverse backup functions might be demonstrated by analysis, using best estimate or conservative methods. Best estimate methods are recommended (see Section 3.4), if the with the implemented design and quality measures are judged sufficient to provide assurance that that the likelihood of CCF is at Level 1. Preventive measures provided in this section note where design and quality requirements are applicable to safety systems or non-safety systems.

A.4 CCF Caused by an Operations or Maintenance Error

This section is applicable to in-service I&C systems that could be susceptible to a human error. Sources of human errors include operator errors or maintenance errors, which can result in any of the following conditions:

Condition 1	Mispositioning of multiple components
Condition 2	Failure to correctly position multiple components
Condition 3	Misconfiguring multiple controllers
Condition 4	Leaving multiple components bypassed or out-of-service
Condition 5	Taking the wrong components out-of-service

Figure A-22 illustrates some CCFs caused by human error.



1

Figure A-22
CCFs Caused by a Human Error

A.4.1 Measures Intended to Reduce the Likelihood of a CCF Caused by a Human Error to Level 2

To reduce the likelihood of a CCF caused by a human error, applying one of the preventive measures listed in Table A-45 (or comparable measures) is recommended.

Table A-45
Measures Intended to Reduce the Likelihood of a CCF caused by a Human Error to Level 2

Preventive Measures	
P1	**Provide multiple measures regarding human performance and human factors engineering (HFE):** a) Procedures for controlling human actions. Procedures meet applicable guides and standards. b) Training and qualification for people who interact with I&C equipment. Training and qualification programs meet applicable guides and standards. c) Design of HSI used by operators in accordance with applicable HFE guides and standards (e.g., NUREG 0700 and 0711 in the U.S., and EPRI [References 29-31]) d) Human performance methods that are commonly used in currently operating plants to reduce human errors, such as three-way communication, place keeping and self-checking. Human performance methods follow applicable guides and standards, and are reinforced through training. The components of this preventive measure are consistent with methods to reduce the likelihood of human performance errors in operating plants today. While it cannot be claimed that these methods eliminate all potential for human performance errors, these methods have proven highly effective in operating plants today. Therefore, these methods are credited to reach a CCF likelihood conclusion of “Level 2” for those plants. Digital systems do not introduce any human interaction complexity that would diminish that same conclusion for system replacements. The following design features reduce the likelihood of some very specific human errors that can lead to CCF: - Interlocks that reduce the likelihood of bypassing equipment protection (e.g., thermal overload bypass) and plant protection functions (e.g., operating bypass), when those functions are expected to be operational. - Interlocks that reduce the likelihood of concurrent bypassing of more than one like trip/actuation measurement channel, when those channels are expected to be operational. - Interlocks that reduce the likelihood of concurrent bypassing (e.g., pull-to-lock) of more than one redundant plant component, when these components are expected to be operational. - Interlocks that reduce the likelihood of adjusting setpoints, constants or tuning parameters outside ranges that are normally expected. For all items above, alarms (in lieu of interlocks) that warn of the abnormal configuration. Interlocks/alarms of this type can be credited when assessing the likelihood of CCF caused by human error. For interlocks/alarms that require signal interfaces between safety divisions, the inter-division communication (hardwired or digital) is designed in accordance with applicable criteria to ensure divisional independence (e.g., IEEE 384 and IEEE 7-4.3.2 in the U.S.).

APPENDIX B: LIKELIHOOD REDUCTION MEASURES

This Appendix provides some likelihood reduction measures that can be helpful to the designer engineer. As described in Section 3.4, the purpose of a likelihood reduction measure is to aid in the determination of whether a credible CCF can be analyzed using beyond design basis inputs, assumptions and acceptance criteria, because the CCF is still credible, but its likelihood is significantly less than the likelihood of a CCF caused by a single failure in the I&C. If a likelihood reduction measure is fully applied, then a credible CCF can be analyzed as a beyond design basis event (or, if practical, as a design basis event should the safety analyst choose to do so).

The fundamental criteria for a likelihood reduction measure are as follows:

1. The likelihood reduction measure significantly reduces the likelihood of the I&C failure at its source, and
2. the likelihood reduction measure significantly reduces the likelihood of a CCF caused by that I&C failure source.

B.1 Measures to Significantly Reduce the Likelihood of Specific, Credible Failure Modes Caused by a Single Random Hardware Failure

At a glance, a measure to reduce the likelihood of a CCF caused by a single random hardware failure in the I&C to be significantly less than a CCF caused by a single random hardware failure in the I&C amounts to circular reasoning. However, it may be possible to apply a likelihood reduction measure in a manner that makes certain failure modes in the I&C significantly less likely than other failure modes in the same I&C.

One failure mode that can be caused by a single random hardware failure in the I&C is an erroneous command, which is difficult to assess because it can be unpredictable and force designers and safety analysts to make assumptions about how it can affect controlled SSCs. Erroneous commands can be produced by controllers, operator workstations, or engineering workstations. If a preventive measure for an erroneous command (from Section A.4) is fully applied, then a CCF caused by an erroneous command is not credible and requires no further consideration. However, such preventive measures are not always provided in an I&C system, but certain defensive measures may still be available that can reduce the likelihood of an erroneous command to be significantly less than other failure modes (such as a "hard failure" to a shelf state).

An erroneous command produced by a single random hardware failure in the I&C can arise from a memory error, an address error, or some other internal error that may go undetected for some period of time if it is not immediately self-announcing.

> For example, an erroneous control system command that incorrectly latches a close signal to several valves that are already closed may not be self-announcing until plant conditions require those valves to open and they remain closed, or until an operator attempts to open them from a human system interface in the I&C system and they remain closed.

If the I&C system or component is provided with diagnostic features that can detect internal errors and force a preferred response such as an alarm and a preferred failure mode (e.g., fail as-is, or fail to a shelf state), then the following likelihood reduction measure may be applicable:

LR1 – Provide all the following measures to significantly reduce the likelihood of a CCF caused by an erroneous command due to a random internal error:

1. To reduce the likelihood of an erroneous command caused by a random internal error to be significantly less likely than other failure modes, and force a preferred failure mode such as fail as-is or fail to a shelf state, provide diagnostic features at the source of the internal errors that can produce an erroneous command. Diagnostic features meet the following conditions:

   a. The diagnostic features cover a wide range of internal error conditions that can produce an erroneous command.

   b. The diagnostic features run in the background and do not interfere with the specified functional and performance requirements of the I&C system or component.

   c. The diagnostic features provide timely detection and response to an internal error. Ideally, diagnostic features provide deterministic, real-time detection and response to internal errors, but in some cases, such as detection of memory errors, diagnosis may take many program cycles to check all memory bits, sometimes on the order of minutes which means the diagnostic feature cannot be used as a preventive measure because an erroneous command can be produced in response to a memory error during this diagnostic interval, but an assessment demonstrates that the likelihood of an internal error over the time interval in which it can be detected is significantly less than the likelihood of other random hardware failures in the same I&C system or component.

      For example, a 5 VDC power supply inside a controller can randomly fail and cause the controller to fail to a shelf state (i.e., a hard failure), such that the likelihood of the hard failure is consistent with those caused by other component failures. However, if LR1 is provided for internal errors such as a memory error, the likelihood of an erroneous command due to such an internal error can be shown to be significantly less than the likelihood of a hard failure in response to a failed power supply.

   d. Upon detection of an internal error, an alarm is raised and a preferred failure mode is forced.

      For example, in a duplex controller (i.e., primary and backup arrangement), the primary may be forced by a diagnostic feature to fail to the shelf state in response to a detected memory error, and

the backup automatically takes control in a bumpless manner. Depending on the nature of the memory error and the timing of the diagnostic feature that detects it, a CCF of multiple controlled SSCs may or may not result. In either case, an alarm is raised so that corrective actions can be taken to restore the failed primary controller.

2. To reduce the likelihood of a credible CCF caused by an erroneous command, the I&C systems or components are arranged with adequate segmentation so that the erroneous command does not propagate from one segment to another. This measure may also limit the number of controlled SSCs that are exposed to the erroneous command.

   For example, if an erroneous command produced by an operator workstation is only addressable to one controller, not many controllers, and the affected controller does not propagate the command to other controllers, then the erroneous command can only affect the SSCs controlled by that controller.

B.2 Measures to Significantly Reduce the Likelihood of a Credible CCF Caused by a Design Defect

A design defect is possible in an operating system, the application software, an embedded digital device, the requirements, or the data communications as these potential failure sources apply to a proposed I&C system or component. If a preventive measure is not fully applied to any of the applicable sources of a design defect, then a CCF caused by a design defect is credible.

However, there is no need to analyze a CCF caused by an activated design defect using design basis inputs, assumptions and acceptance criteria, if the following limiting reduction measure is fully applied, because it reduces the likelihood of this CCF to be significantly less than the likelihood of a CCF caused by a single failure (which is in the design basis):

LR2 – Provide all the following measures to significantly reduce the likelihood of a credible CCF caused by an activated design defect:

1. To reduce the likelihood of a design defect at its source, provide a structured design process that meets the following conditions:

   a. For safety systems, the structured design process follows applicable rules, guides and standards.

      For example, per 10 CFR 50.55, the protection systems in a facility may be required to follow IEEE Std. 603-1991. Section 5.3 of IEEE Std. 603-1991 states that "*safety system equipment shall be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program (ANSI/ASME NQAI-1989*."

Guidance on a structured design process for safety systems can be found in NRC Regulatory Guides 1.168 through 1.173.

b. For non-safety systems, the structured design process follows normal plant practice for assuring quality per Generic Letter 84-01. Normal plant practice for a system development lifecycle model typically include requirements, hardware and software design and/or configuration, testing, and configuration management activities.

2. To significantly reduce the likelihood of a CCF caused by an activated design defect, provide sufficient independence between controllers so that a defect activated in one controller does not propagate to other controllers. A "controller" may be an individual controller or a control segment made up of a controller and peripherals such as input modules, output modules, cabinet power supplies, etc.

   a. For safety systems, independence between divisions is ensured through compliance to the rules, guides and standards that provide reasonable assurance of independence.

      For example, Section 5.6 of IEEE Std. 603-1991, which the protection systems in some facilities may be required to follow per 10 CFR 50.55, provides independence criteria, including criteria for physical independence between divisions, isolation between safety systems and non-safety systems, etc.

   b. For non-safety systems, independence between controllers or control segments follows good engineering practice for providing sufficient functional, signal, and physical independence.

      For example, a main steam turbine control system segment and a main turbine bypass valve control segment are sufficiently independent if there are no functional or signal dependencies between the segments, and each segment is provided with its own physical enclosure (e.g., cabinet).

APPENDIX C: CCF SUSCEPTIBILITY ANALYSIS WORKSHEET

This Appendix provides a CCF susceptibility analysis worksheet template via Table C-1, which can be used to document each step of the analysis using the following instructions:

Step 1: Determine the applicability of each I&C failure source in the proposed I&C system or component design using the guidance in Section 4.2.2.1. For each I&C failure source, check "yes" or "no" under the "Applicable?" column in Table C-1 and provide a technical basis for each answer. For example, if a proposed I&C system or component design will not be provided with data communications capability, then that would be the basis for checking "no" for data communications.

If an I&C failure source is identified in the proposed I&C system or component design that is not listed in Table C-1, then add it to the worksheet for the appropriate category (where it says "other") and provide a technical basis for inclusion.

Step 2: For each applicable I&C failure source (that is, where "yes" is checked under the "Applicable?" column), determine whether a CCF of multiple controlled SSCs is credible or not, using the guidance in Section 4.2.2.2. For each I&C failure source, check "yes" or "no" under the "CCF Credible" column in Table C-1. A "no" answer for any applicable failure source means a preventive measure is fully applied (either a complete preventive measure from this Appendix or an alternate measure with justification).

If a specific preventive measure from Appendix A is fully applied, then it should be noted by the associated Table number and P number in the technical basis column (such as A2-P1 for shared power supply if it is fully applied within the proposed I&C system or component design). Provide notes or references to notes or other documents as needed that describe and/or demonstrate how the preventive measure is fully applied.

If a specific preventive measure from Appendix A is not fully applied, or a new preventive measure is provided in the proposed I&C system or component design, then it is an alternate preventive measure that requires justification. Provide references to notes or other documents as needed that describe and/or demonstrate how the alternate preventive measure is used to conclude that a CCF for that I&C failure source is not credible.

Step 3: For each credible CCF (that is, where "yes" is checked under the "CCF Credible?" column), determine if the CCF malfunction result is limited to a specific set of SSCs and/or preferred SSC malfunction states using the guidance in Section 4.2.2.3. For each credible CCF, check "yes" or "no" under the "CCF Limited?" column in Table C-1. A "yes" answer for any credible CCF means a limiting measure is fully applied.

If a specific limiting measure from Appendix A is fully applied, then it should be noted as such with the Table and L number in the technical basis column (such as A2-L1 for shared power supply if it is fully applied to the proposed I&C system or component design). Provide notes or references to notes or other documents as needed that describe and/or demonstrate how the limiting measure is fully applied.

If a specific limiting measure from Appendix A is not fully applied, or a new limiting measure is provided in the proposed I&C system or component design, then it is an alternate limiting measure that requires justification. Provide references to notes or other documents as needed that describe and/or demonstrate how the alternate limiting measure is used to conclude that the CCF is limited to a specific set of SSCs and/or preferred SSC malfunction states.

Step 4: For each credible CCF, determine if the CCF malfunction result can be analyzed using design basis inputs, assumptions and acceptance criteria, or beyond design basis inputs, assumptions and acceptance criteria (that is, if a likelihood reduction measure is fully applied for each credible CCF) using the guidance in Section 4.2.2.4. For each credible CCF, check "yes" or "no" under the "CCF Likelihood Reduced?" column in Table C-1. A "yes" answer for any credible CCF means a likelihood reduction measure is fully applied.

If a specific likelihood reduction measure from Appendix B is fully applied, then it should be noted as such. Provide notes or references to notes or other documents as needed that describe and/or demonstrate how the likelihood reduction measure is fully applied.

If a specific likelihood reduction measure from Appendix B is not fully applied, or a new likelihood reduction measure is provided in the proposed I&C system or component design, then it is an alternate likelihood reduction measure that requires justification. Provide references to notes or other documents as needed that describe and/or demonstrate how the alternate likelihood reduction measure is used to conclude that the CCF malfunction result can be analyzed using beyond design basis inputs, assumptions and acceptance criteria.

Step 5: For each credible CCF, determine the SSC malfunction, which can be driven by any limiting measures applied in Step 3. SSC malfunction states can be characterized by the functional and performance characteristics of each affected SSC, such as fully open, fully closed, running, stopped, energized, deenergized, etc.

For the resulting SSC malfunctions, list the affected SSCs and their states in the "SSC Malfunction(s)" column in Table C-1, or provide references that list the affected SSCs and their states. In addition, the method of analysis (design basis or beyond design basis) should be identified, using the results from Step 4, in the "Design Basis or Beyond Design Basis?" column.

Table C-1: Suggested CCF Susceptibility Analysis Worksheet Template

I&C Failure Source		Applicable?			CCF Credible?			CCF Limited?			CCF Likelihood Reduced?			CCF Malfunction Result	
Cat.	Type	Yes	No	Basis	Yes	No	Basis	Yes	No	Basis	Yes	No	Basis	SSC Malfunction(s)	Design Basis or Beyond Design Basis?
Single Random Hardware Failure	Power Supply														
	Sensor														
	Output Module														
	Control Signal														
	Data Communications														
	Operator Workstation														
	Eng./Maint. Workstation														
	Controller														
	Clock														
	Other?														
Environmental Disturbance	High Temperature or Humidity														
	EMI														
	Seismic														
	Radiation														
	Other?														
Design Defect	Operating System														
	Application Software														
	Embedded Digital Device														
	Requirements Error/Omission														
	Data Communications														
	Other?														
Other?															

APPENDIX D: EXAMPLES

To be developed.

[BLANK PAGE]