Recommended Input for New RIS on CCF

The following questions, which are commonly asked by industry engineers, should be clearly answered in this RIS.

1. Why does the credibility of a CCF need to be considered?

   When a CCF is credible, the component level, system level and/or plant level effect of that CCF must be assessed to determine if the CCF results in a plant level end result that is bounded by previous plant analysis or a new unbounded condition exists that requires new analysis. The plant level end result refers to the effect on the margins to the critical safety limits threatened by the CCF (e.g., DNBR, pressure boundary analytical limits).

2. For which digital devices does the credibility of a CCF need to be considered?

   Digital devices offer the potential for increased design complexity compared to their analog predecessors, including control (and potential failure) of multiple plant components which were traditionally controlled by separate analog devices (i.e., a CCF). This design complexity was very difficult to achieve, hence typically not attempted when analog technology was employed; therefore, only very specific CCFs were considered in the original design basis of most operating plants (e.g., loss of all feedwater, ATWS, SBO).

   Digital systems typically integrate functions and/or controlled plant components that were separately implemented in analog systems. This integration occurs either (1) directly in the same digital device, (2) indirectly through interconnection of multiple digital devices using digital data communication interfaces and/or common video display units (VDU), or (3) indirectly through the use of common digital designs in independent digital devices. This integration introduces new sources of CCF that if not prevented can adversely affect more plant components (i.e., a CCF) than their analog predecessor, which can result in unanalyzed plant transients.

   When any digital technology is employed (e.g., software, FPGA, CPLD), the potential for a failure that affects multiple plant components (i.e., a CCF) should be considered for all plant components that (1) can cause a plant transient, or (2) are credited for mitigating plant transients either directly or as an auxiliary safety support function. This potential should be assessed through a documented CCF susceptibility analysis, which is a systematic evaluation of credible CCF sources (i.e., a single random hardware failure, environmental conditions and a design defect) and the defensive measures included in the design to prevent a CCF from those sources.

Plant components controlled by an embedded digital device (EDD) have potential CCF vulnerabilities just like plant components controlled by any other digital device. Therefore, a documented CCF susceptibility analysis is needed. Depending on the simplicity of the EDD, that analysis may be able to credit the testing conducted for the EDD and supporting analysis, to reach a conclusion that a CCF is not credible; this is discussed in Item 3b below.

3. What criteria are considered when determining the credibility of a CCF?

   Because a credible CCF can put the plant in an unanalyzed condition that may be unsafe, only deterministic criteria should be used in determining if a CCF is credible or not. Deterministic criteria should be used, because these criteria do not require subjective judgements for such an important issue essential to plant safety. Deterministic criteria are design attributes such as (1) separate communication processors and function processors, as described in ISG-04, to ensure a function processor is not adversely affected by a digital communication data storm, or (2) testability or internal diversity, for prevention of a CCF due to a design defect.

   Additional examples of deterministic criteria that can be used to reach a CCF not credible conclusion are as follows:

   a. A design defect in a digital device can affect multiple plant components controlled by a single digital device or controlled by multiple independent digital devices, when that same design is shared among those digital devices. Despite the presence of common design elements (e.g., operating system, function blocks) within multiple independent digital devices, internal diversity within the configuration of those common design elements (e.g., different cycle times, different application software, different I/O and communication interfaces, different operating modes) can be credited in reaching a conclusion that a CCF of those independent digital devices (and the multiple plant components that they control) is not credible, if a triggered malfunction in one digital device is self-announcing; therefore, the design defect is correctable before it can be triggered in the second digital device (i.e., to become a CCF of both digital devices).

b. The simplicity alone of a digital device can be credited in reaching a conclusion that a CCF due to a design defect is not credible, only if all external and internal state combinations are tested, or an analysis is provided that demonstrates that untested state combinations are irrelevant; this deterministic criterion is typically relevant to single purpose EDDs with very few external inputs and very limited configurability.

4. Why is it important to assess the likelihood of a credible CCF?

Anticipated Operational Occurrences (AOO) are plant accidents that are expected to occur one or more times during the life of the plant. These were historically defined based on the component/system level malfunction results of single random hardware failures in plant components, or the I&C and electrical systems that control those components. Due to this relatively high frequency expectation, AOOs are within the plant’s design basis and are analyzed using conservative methods and acceptance criteria.

Therefore, when a credible CCF can be caused by a single random hardware failure, the malfunction result of that CCF must be considered an AOO and must be assessed using conservative design basis analysis methods and acceptance criteria. In essence, the CCF is a design basis AOO.

Conservative analysis methods require consideration of worst case plant conditions, use of only safety systems for event mitigation, worst case performance of those mitigating systems, and acceptance criteria with significant margin to critical safety limits. Conservative acceptance criteria mean that for a design basis CCF in a control system, the CCF malfunction result must be bounded by the plant level end result of current anticipated operational occurrences (AOO). Conservative acceptance criteria for a design basis CCF in an auxiliary safety support system, means that the CCF malfunction cannot result in an adverse component/system level effect on the auxiliary safety support system that is not previously analyzed in the FSAR; this is typically limited to single safety division.

On the other hand, when a credible CCF is significantly less likely than a CCF due to a random hardware failure, the CCF can be considered beyond design basis. Therefore, the malfunction result of that CCF can be assessed using best estimate analysis methods and acceptance criteria.

Best estimate methods allow the use of nominal plant conditions, use of high quality non-safety systems for event mitigation, nominal performance of those mitigating systems, and acceptance criteria that does not exceed critical safety limits. Best estimate acceptance criteria mean that for a beyond design basis CCF in a control system, the CCF malfunction result must be bounded by the plant level end result of current AOOs or postulated accidents (PA). Best estimate acceptance criteria for a beyond design basis CCF in an auxiliary safety support system, means that the CCF malfunction cannot result in an adverse effect on the safety systems supported by that auxiliary system. For mitigating a beyond design basis CCF, the analysis can credit safety systems, control systems in continuous operation, or other non-safety systems that are normally in standby but have augmented quality.

In both cases (within or beyond design basis), the analysis can only credit systems that currently exist in the plant, because these have had prior regulatory review. A bounded plant level end result refers to maintaining the margin to critical safety functions, such as DNBR and pressure boundary analytical limits, for the corresponding current accident analysis (AOO or PA).

5. Why is it acceptable to use best estimate methods when assessing a CCF that is concluded to be beyond design basis (i.e. significantly less likely than a CCF due to a random hardware failure)?

   The precedence for using best estimate analysis methods and acceptance criteria for beyond design basis events was established for the analysis of Anticipated Transients Without Scram (ATWS) and Station Blackout (SBO) events. Both of these are beyond design basis events. Best estimate analysis methods and acceptance criteria were employed for the original analyses of these events in the plant’s FSAR; therefore, these same methods would be applicable to any upgrades to the ATWS or SBO mitigating systems.

   This use of best estimate analysis methods and acceptance criteria is also supported by the SRM to SECY 93-087 and BTP 7-19, which establish this beyond design basis methodology for a CCF due to a design defect in safety systems. While the SRM to SECY 93-087 and BTP 7-19 were originally written to address the complexity of digital systems in new plants, that same complexity concern is applicable to the digital systems being applied to digital upgrades in operating plants today. This is also consistent with the SRM to SECY-15-0106 which states "the same requirements should apply to operating and new reactors."

6. What criteria are considered when determining the likelihood of a credible CCF?

   The conclusion in the SRM to SECY 93-087 that a CCF due to a design defect in a safety system is beyond design basis is based on (1) the low likelihood of a design defect due to a robust design process in safety systems, and (2) the inability of a triggered defect in one division to propagate to multiple safety divisions to actually cause a CCF, due to the independence of those safety divisions. Item 1 is a qualitative assessment; Item 2 is a deterministic assessment.

   Therefore, using the technical basis from the SRM to SECY 93-087, for any credible CCF, the likelihood of that CCF can be assessed using a combination of (1) qualitative measures to assess the effectiveness of the design process in reducing the likelihood of the CCF source, and (2) deterministic measures to assess the effectiveness of the segmentation/independence in preventing propagation of a triggered CCF source to multiple digital devices or multiple plant components. When both of these attributes exist, a credible CCF can be considered significantly less likely than a CCF due to a single random hardware failure; hence, the CCF can be considered beyond design basis. Therefore, the malfunction result of that CCF can be assessed using best estimate analysis methods and acceptance criteria, as explained in Item 4 above.

   The beyond design basis conclusion of the SRM to SECY 93-087 is clearly applicable to a digital design defect in safety systems, because they have a robust design process and divisional independence, both governed by regulatory guidance and criterion. However, the same technical basis can also be applied to non-safety control systems. A CCF due to a design defect in a non-safety control system can be considered beyond design basis, if the control system exhibits (1) comparable design process attributes to reduce the likelihood of a design defect (qualitative), and (2) comparable design attributes to prevent the propagation of a triggered defect (deterministic).

However, due to their lower safety significance compared to safety systems, for non-safety control systems a graded approach can be applied when assessing these qualitative and deterministic attributes. For example, when assessing the likelihood of a CCF due to a design defect within a distributed control system: (1) Control systems that can initiate plant transients are expected to adhere to high quality commercial design life cycle standards that include well documented requirements, design and testing; they are not expected to adhere to the same regulated design life cycle criteria as safety systems. (2) Segmentation of control functions into different digital controllers is an acceptable means to limit the effect and prevent propagation of a triggered defect; divisional independence is not required as it is for safety systems.

It is important to note that while the SRM to SECY 93-087 establishes the precedence for using these two attributes (one qualitative and one deterministic) to conclude that the likelihood of a CCF has been significantly reduced (i.e., beyond design basis), based on the SRM to SECY 93-087 they are not sufficient attributes to consider a CCF due to a design defect not credible. Therefore, for this example the effect of a CCF due to a design defect in multiple distributed digital controllers would be analyzed using best estimate methods. To reach the conclusion that a CCF due to this design defect is not credible and thereby requires no further CCF malfunction result analysis, additional deterministic attributes would be required, as described in Item 3a, above.

7. When analyzing a credible CCF, what failure modes need to be considered for digital devices?

   The documented CCF susceptibility analysis described in Item 2 above, should assess the effects of a credible CCF at the component and/or system level. Where the component and/or system level effect is different than previously analyzed in the plant’s FSAR, a documented CCF malfunction result analysis should assess the effects of the CCF at the plant level to determine if the plant level end result is bounded by previously analyzed plant accidents.

Digital devices have the same failure modes as analog devices (i.e., failure to perform the intended control function, and spurious or erroneous control of the intended function). However, due to the integration of controlled components either (1) directly in the same digital device, (2) indirectly through interconnection of multiple digital devices using digital data communication interfaces and/or common video display units (VDU), or (3) indirectly through the use of common digital designs in independent digital devices, those failure modes have the potential to adversely affect more plant components (i.e., a CCF) than their analog predecessor. In addition, digital devices have the additional failure mode of data storms, where valid or erroneous data can be generated at an abnormally high rate that has the potential to adversely affect all connected digital devices.

NUREG 6303 provides guidance for decomposing complex digital systems into hardware/software blocks. A CCF susceptibility analysis considers the failure of only one block at a time (e.g., a single hardware component, a software function block). However, it must be recognized that the effect of that single hardware/software block failure can result in erroneous signals that propagate through the system to affect multiple functions or multiple plant components concurrently. This failed signal propagation is unlikely to result in all controlled plant components failing in the worst possible way, but it could certainly result in multiple plant components failing in different ways, depending on how the output of the failed block is used in the system.

Therefore, when conducting a CCF susceptibility analysis, if a CCF is concluded to be credible, the output(s) of a failed digital block should be assumed to fail as-is, high and low, and in a data storm mode. However, the propagation and adverse effect of these output failures can be restricted with the use of deterministic limiting measures such as a watch dog timer, or redundancy with output voting, which can detect an erroneous operation and force a single specific failure output state that is more easily analyzed.

8. Response to 50.59 Questions

There are three 50.59 questions that are particularly relevant to digital upgrades:

Question 2: Result in more than a minimal increase in the likelihood of occurrence of a malfunction…?

This question pertains to all malfunctions, not just malfunctions that result in a CCF. This requires a comparison of the analog and digital systems, to assess single point vulnerabilities and the qualitative reliability of the analog vs. digital components; reliability calculations can be used, but are not required. A CCF would be pertinent to this assessment only if the CCF is concluded to be credible and within the design basis (i.e., as likely as a single random hardware failure); a beyond design basis CCF is sufficiently unlikely to have no bearing on this assessment.

Question 5: Create the possibility of an accident of a different type…?

The transients analyzed in the UFSAR typically include events that challenge only a single critical safety function, such as reactivity control, pressure control, volume control, **OR** heat removal. Digital designs that maintain clear segregation between the controls for these critical safety functions do not create the possibility for an accident of a different type.

However, when these control functions are integrated, either directly or indirectly, and there is a credible CCF that is within the design basis and can adversely affect multiple critical safety functions, then there is the possibility of an accident of a different type.

When these control functions are integrated, either directly or indirectly, and there is a credible CCF that is beyond the design basis and can adversely affect multiple critical safety functions, then a CCF malfunction result analysis is conducted to determine if the plant level end result is bounded by the plant level end result determined for other AOOs or PAs previously analyzed in the FSAR. As stated in Item 1 above, plant level end result refers to the effect on the margins to the critical safety limits threatened by the CCF. As stated in Item 4 above, for a credible CCF that is beyond design basis, the CCF malfunction result analysis uses best estimate methods with best estimate acceptance criteria.

Question 6: Create a possibility for a malfunction … with a different result…?

This question can clearly be answered favorably for a CCF that does not result in a different component level or system level malfunction, as determined through the documented CCF susceptibility analysis. Where there is a different component/system level malfunction, a CCF malfunction result analysis is conducted to determine if the plant level end result is bounded by the plant level end result determined for other accidents previously analyzed in the FSAR. As stated in Item 1 above, plant level end result refers to the effect on the margins to the critical safety limits threatened by the CCF.

As stated in Item 4 above, for a credible CCF that is within the design basis, the CCF malfunction result analysis uses conservative design basis methods with conservative acceptance criteria. For a credible CCF that is beyond design basis, the CCF malfunction result analysis uses best estimate methods with best estimate acceptance criteria.

9. What is the impact of new NRC/Industry guidance?

   Current regulatory guidance establishes the basis for determining the credibility of a CCF, and the likelihood of a CCF that is concluded to be credible. Some examples:

   a. The deterministic guidance for communication independence in ISG-04 is appropriate to consider when determining if a CCF is credible due to a single random hardware failure or design defect in a data communication interface, including a failure/defect that results in a data storm.
   b. The software life cycle guidance in Regulatory Guides 1.68 through 1.73 is appropriate to consider when qualitatively assessing the likelihood of a design defect in a safety system that could lead to a CCF.
   c. Adherence to the guidance in RG 1.152 Rev. 3 for a secure development and operational environment (SDOE) is sufficient to reach a conclusion that an unwanted design change is not credible; therefore, a design defect due that could lead to a CCF due to an unwanted design change is also not credible.

While control systems are not expected to adhere to these same regulatory guidance documents, a graded approach can be taken to determine if a control system has comparable (not equivalent) attributes that can be credited to meet the same intent as these more prescriptive criteria that are applied to safety systems. For example, a graded approach can be taken to determine if a control system has comparable (not equivalent) security attributes that can be credited to meet the same intent as the more prescriptive SDOE criteria in RG 1.152.

10. What digital upgrades would screen out for a 50.59 evaluation?

    Due to the complexity of digital designs and the potential for new susceptibilities to CCF, the Staff would not expect any analog to digital upgrades in control systems that can cause plant transients, safety systems or auxiliary safety support systems to screen out. An analog to digital upgrade needs a CCF susceptibility analysis, and for any sources of CCF determined to be credible, that upgrade also needs a CCF malfunction results analysis. Digital to digital upgrades also need these analyses, if they were not previously conducted or if the new digital design requires changes to previous analyses.

11. Does the analysis of a CCF require a new method of evaluation?

    The use of digital technology does not require a new method of evaluation. The CCF susceptibility analysis (Item 2 above) and CCF malfunction result analysis (Item 7 above) are extensions of previously employed failure modes and effects analysis (FMEA) and plant transient and accident analysis (TAA). The best estimate methods and acceptance criteria that can be employed for a credible CCF that is determined to have low likelihood (Item 4 above) are the same as methods employed for other beyond design basis events, such as ATWS and SBO. All analyses that support 50.59 evaluations must be documented and maintained.

12. Is a D3 analysis required?

    The SRM to SECY 93-087 requires a D3 analysis, which consists of (1) an assessment to determine the vulnerability of the I&C systems to CCF; this is referred to as the CCF susceptibility analysis in Item 2, and (2) a plant level analysis to demonstrate adequate plant diversity, for each CCF vulnerability; adequate diversity is demonstrated for each credible CCF by the CCF malfunction result analysis described in Item 6. If there is no credible CCF (i.e., no CCF vulnerability) then a CCF malfunction result analysis is not required.

The SRM does not distinguish CCF in safety vs. non-safety systems; this distinction arose through BTP 7-19 which limited consideration of CCF to safety systems only. The staff now recognizes that CCF in non-safety control systems that can cause plant transients is of equal concern, due to the potential that a CCF in those systems can result in unanalyzed transients. Therefore, these systems are included in the guidance of Item 2 above.

The SRM states that a CCF is beyond design basis, hence permits the use of best estimate methods when conducting the CCF malfunction results analysis. The Staff clarifies that the credibility of CCF should be determined based on an assessment of deterministic attributes (Item 3 above) and the likelihood of any credible CCF should be determined based on an assessment of both qualitative and deterministic attributes, as described in Item 6. When the appropriate attributes exist to conclude that the likelihood of a credible CCF is significantly less than the likelihood of a CCF due to a random hardware failure, the CCF can be considered beyond design basis and best estimate methods and acceptance criteria can be used.