NEI 20-07

Guidance for Addressing CCF in High Safety Significant Safety-related DI&C Systems

July 1, 2021

NUCLEAR ENERGY INSTITUTE

Addressing HSSSR Systematic CCF

- BTP 7-19, Rev. 8 allows for “NRC-approved alternative methods, including defensive measures, in the design of a system or component—that may eliminate a potential CCF from further consideration.”
- BTP 7-19, Section 3.1.3: “Licensees may propose technical approaches to address CCF that this BTP does not describe…The NRC’s approval of an alternative method should include a supporting technical basis and acceptance criteria for its use.”
- The approach described in this presentation is intended to fall under these statements in BTP 7-19

Addressing HSSSR Systematic CCF

- Two step process
  - Step 1
    - Perform a systematic hazards analysis based on STPA that creates a model of the system control structure and identifies unsafe control actions
    - Establish a Risk Reduction Objective (RRO)
  - Step 2
    - Develop STPA loss scenarios based on Step 1
    - Identify and allocate systematic control methods to eliminate or mitigate loss scenarios
    - Score control methods to achieve a sufficient effectiveness commensurate with the RRO

Step 1: Hazard Analysis & Establishing Risk Reduction Objective (RRO)

Addressing HSSSR Systematic CCF – Step 1

- Hazard Analysis
  - IEC 61508-1 requires a determination of hazards of the Equipment Under Control (EUC) and the EUC control system, and "consideration shall be given to the elimination or reduction of the hazards." NEI 20-07 uses the first 3 parts of the STPA hazard analysis method in this first step of the process.
    - Identify losses
    - Identify system hazards that contribute to losses
    - Create control system model (control structure) and identify unsafe control actions (UCAs)

Addressing HSSSR Systematic CCF – Step 1

- Unsafe control actions
  - The STPA handbook explains that for each control action linked to a hazard, four cases need to be analyzed:
    - Not providing the control action causes the hazard
    - Providing the control action causes the hazard
    - Providing the control action too late or out of order causes the hazard
    - Providing the control action too long or stopped too soon

Addressing HSSSR Systematic CCF – Step 1

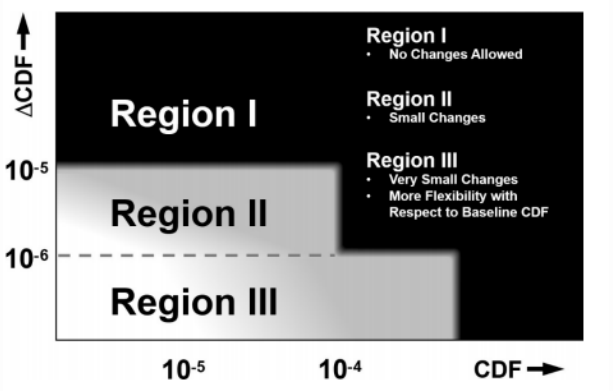


Figure 4. Acceptance guidelines* for core damage frequency

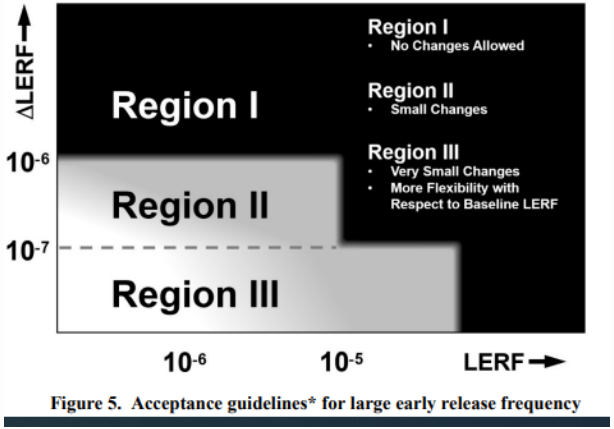
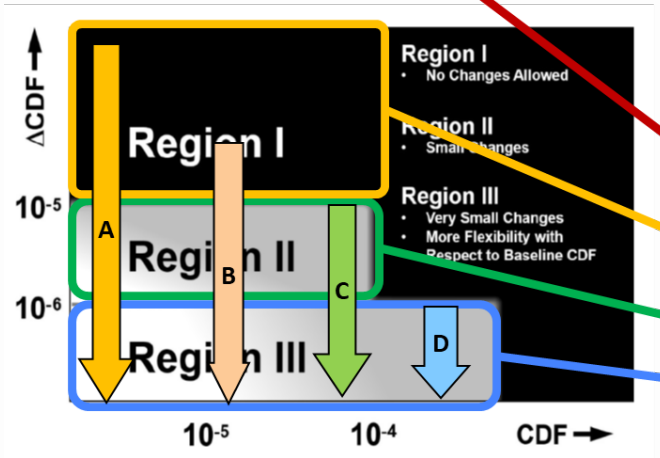


Figure 5. Acceptance guidelines* for large early release frequency

- Establish RRO
  - Create bounding assessment: calculate the change in risk from the baseline PRA model when the entire HSSSR system fails
  - The delta risk is then mapped to the regions described in RG 1.174
  - The delta risk is used to determine the RRO

Addressing HSSSR Systematic CCF – Step 1

- Establish RRO (cont.)
  - Establish RRO band (A-D)



Risk Reduction Objectives

RRO	Change in Core Damage Frequency – CDF (per year)	Change in Large Early Release Frequency – LERF (per year)
Change the Design	ΔCDF > 1E-3	ΔLERF > 1E-4
A	1E-4 < ΔCDF ≤ 1E-3	1E-5 < ΔLERF ≤ 1E-4
B	1E-5 < ΔCDF ≤ 1E-4	1E-6 < ΔLERF ≤ 1E-5
C	1E-6 < ΔCDF ≤ 1E-5	1E-7 < ΔLERF ≤ 1E-6
D	ΔCDF ≤ 1E-6	ΔLERF ≤ 1E-7

Addressing HSSSR Systematic CCF – Step 2

- Develop STPA loss scenarios based on Step 1
- Identify and allocate systematic control methods to eliminate or mitigate loss scenarios
- Score control methods to achieve a sufficient effectiveness commensurate with the RRO

Addressing HSSSR Systematic CCF – Step 2

Develop STPA loss scenarios based on Step 1

What is a Loss Scenario?

- Loss Scenario - describes the causal factors that can lead to the unsafe control actions (that lead to hazards).
  - Loss scenarios are reasons why a UCA can manifest itself, or reasons why a control action is not executed or executed improperly.
  - Two types of loss scenarios
    - Why would Unsafe Control Actions occur?
    - Why would control actions be improperly executed or not executed, leading to hazards?

Loss Scenario Types from STPA Handbook

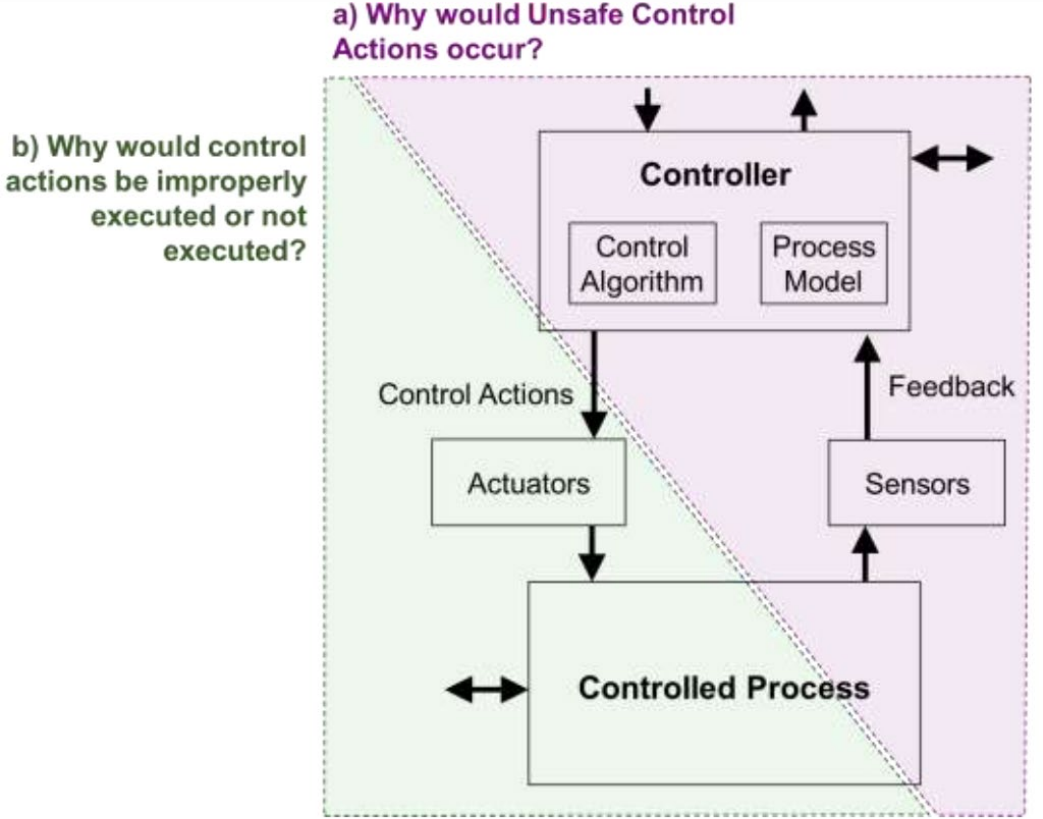


Figure 2.17: Two types of scenarios that must be considered

Loss Scenarios

- For each UCA developed from the hazard analysis, loss scenarios are created that can be sourced from:
    - Unsafe controller behaviors
    - Inadequate feedback and information
    - Failures in control paths
    - Failures in controlled processes
- For each loss scenario, systematic control methods are developed to eliminate or mitigate the loss scenario

Loss Scenario Sources

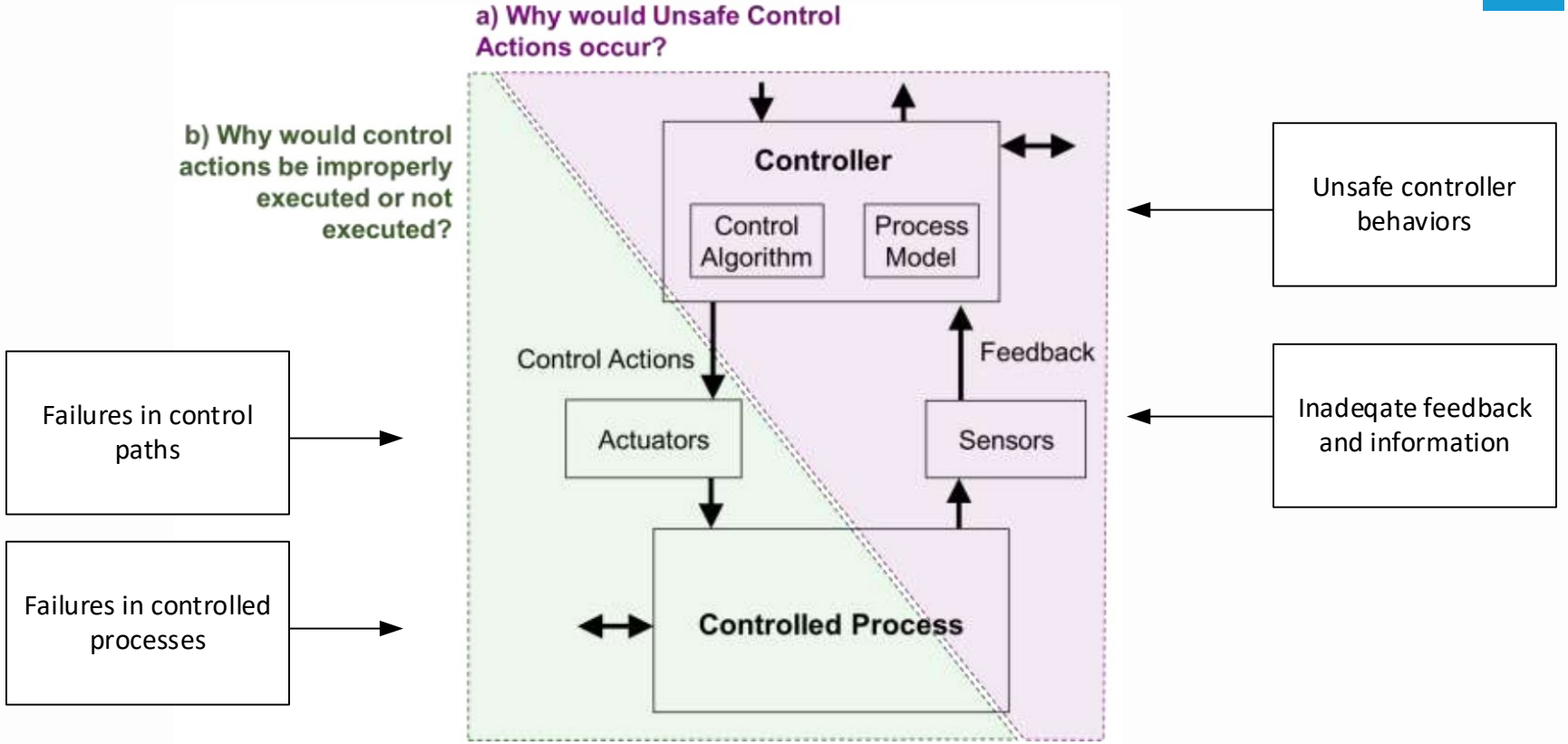


Figure 2.17: Two types of scenarios that must be considered

Addressing HSSSR Systematic CCF – Step 2

- Develop STPA loss scenarios based on Step 1
- Identify and allocate systematic control methods to eliminate or mitigate loss scenarios
- Score control methods to achieve a sufficient effectiveness commensurate with the RRO

Identify and allocate systematic control methods to eliminate or mitigate loss scenarios

- What is a systematic control method?
  - They are methods that can be implemented to eliminate or mitigate a loss scenario
- The identification of systematic control methods suitable for any given loss scenario is highly dependent on the characteristics of the loss scenario itself
- For each systematic loss scenario, the assessment identifies what systematic control method or methods to apply to eliminate or mitigate the loss scenario

Identify and allocate systematic control methods to eliminate or mitigate loss scenarios

- Allocate control methods to the system elements in the HSSSR system
  - A control method could be solely applied to one element in the HSSSR system (e.g., a particular controller)
  - A control method may need to span multiple elements in the HSSSR system to be fully applied (e.g., multiple controllers or controller and equipment under control)

Addressing HSSSR Systematic CCF – Step 2

- Develop STPA loss scenarios based on Step 1
- Identify and allocate systematic control methods to eliminate or mitigate loss scenarios
- Score control methods to achieve a sufficient effectiveness commensurate with the RRO

Score control methods to achieve a sufficient effectiveness commensurate with the RRO

- A scoring method is used as a qualitative approach to assess control method effectiveness
- There are two parts to this process:
  - Part 1:
    - Apply pre-scored systematic control methods for the control algorithm commensurate with the RRO (adapted from IEC 61508, e.g., Annex A in Part 3)
    - These are techniques and measures that need to be followed commensurate with the RRO

Score control methods to achieve a sufficient effectiveness commensurate with the RRO

- Scoring Part 2:
  - Score the balance of the systematic control methods that eliminate or mitigate loss scenarios
  - Each control method is scored for its type and each control method is scored for its strength
  - It is the combination of the control method type and strength that provides an assessment of control method effectiveness

Score control methods to achieve a sufficient effectiveness commensurate with the RRO

- The are two characteristics to a control method that eliminated or mitigated a loss scenario
  - Control Method Type (e.g., administrative, procedure, technical, etc.)
  - Control Method Strength (e.g., the degree to which control method can prevent, detect, respond, and recover from a loss scenario before the UCA occurs)

Score control methods to achieve a sufficient effectiveness commensurate with the RRO

- The scoring methodology uses elements of standard information theory, and in particular the key measure of entropy
  - Entropy is a measure of the information content in a system. When each piece of information is defined, a log base 2 equation is used to measure the combined information content.
  - Control method information, defined by its “type” and “strength”, is combined using the log base 2 approach to provide a scoring for its overall effectiveness
  - It’s a way to provide a defined scale for the qualitative assessment of control method effectiveness

Score control methods to achieve a sufficient effectiveness commensurate with the RRO

- The control method effectiveness score is compared to RRO benchmark for control method effectiveness
- This provides a means to assess if the control method effectiveness is commensurate with the RRO
- If the control method effectiveness is not commensurate with the RRO then NEI 20-07 will describe considerations to increase control method effectiveness.

Summary and Conclusion

Summary and Conclusion

- This “NEI 20-07” approach to addressing CCF is based on assessing the potential risk of the HSSSR system replacement and the necessary control methods to lower the risk to non-risk significant
- It is a 2-step process that establishes an objective based on risk insights and control methods commensurate to achieve a risk reduction objective
- The NEI 20-07 approach falls under “alternative methods” as described in BTP 7-19 (p. 19-8) to addressing HSSSR system CCF that is risk informed and performance based
- A traceability record is created tracing the losses, hazards, UCAs, loss scenarios, and control methods to mitigate loss scenarios

Proposed Schedule

- July 1, 2021 – Present NEI 20-07 systematic approach to addressing CCF
- August 31, 2021 – NEI draft revision of NEI 20-07 incorporating NRC feedback
- September 30, 2021 - Peer review and industry feedback on NEI 20-07 draft revision
- October 29, 2021 – Submit NEI 20-07 draft revision for NRC feedback
- November 30, 2021 – Public meeting to obtain NRC feedback
- Q1 2022 – NEI 20-07 submittal for NRC formal endorsement