NEI 20-07

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

January 12, 2021

NUCLEAR ENERGY INSTITUTE

Agenda

- Reasons for moving on from the NEI 16-16 approach

- Overall concept and structure of NEI 20-07

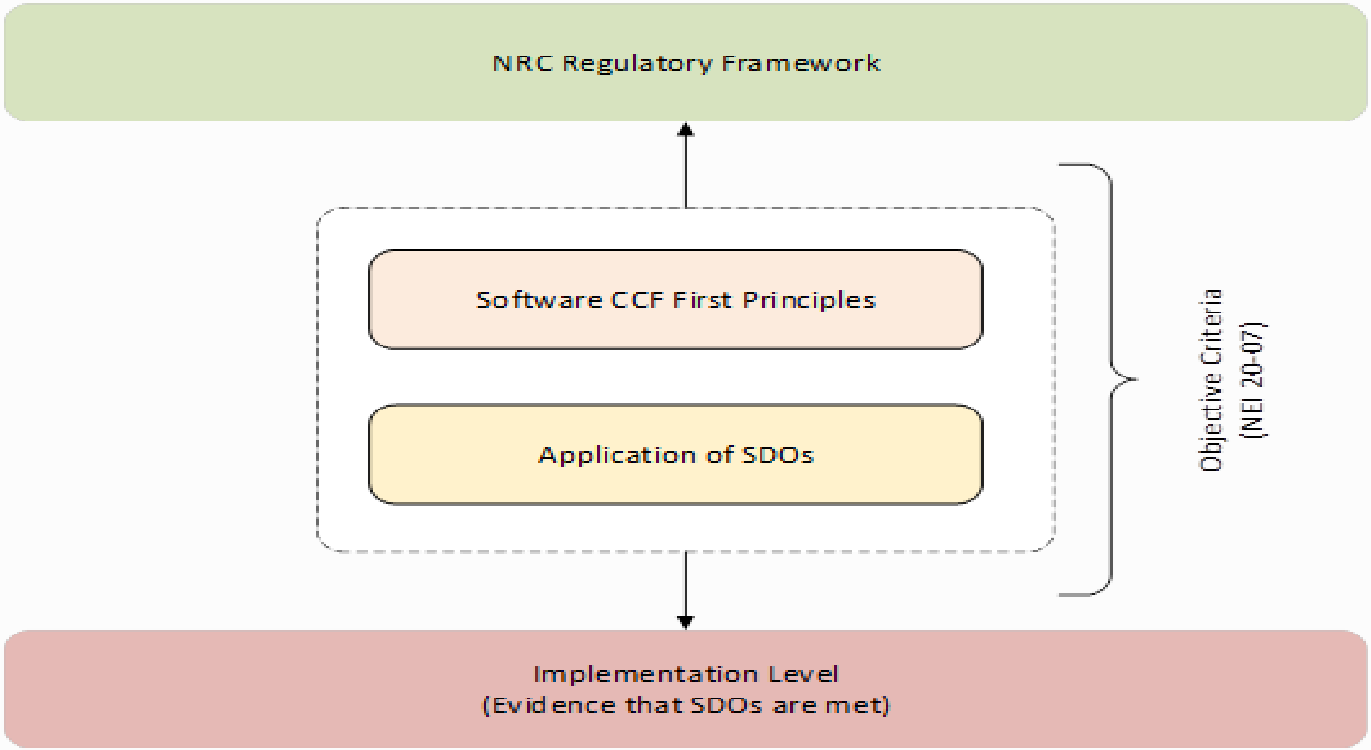
This Photo by Unknown Author is licensed under CC BY

Departure from NEI 16-16 Approach

- NEI 16-16:
  - Too much technical detail with no clear tie to regulation or standards
  - Included hardware defensive design measures without establishing a technical basis for each
- NEI 20-07:
  - Focuses the guidance on quality software development
  - Enables use of state-of-the art defensive design measures based on industry standards without being overly prescriptive

This Photo by Unknown Author is licensed under CC BY-SA

NEI 20-07 Approach



NRC Regulatory Framework

Software CCF First Principles

Application of SDOs

Objective Criteria
(NEI 20-07)

Implementation Level
(Evidence that SDOs are met)

1st Principles

1. Software quality depends on complete and correct requirements, design, review, implementation, and testing
2. Concurrent triggering conditions are required to activate a latent software defect
3. The effects of a software CCF can be reduced by design
4. Operating history can provide evidence of software quality

1st Principles Connect to Regulations

Each of the 1st principles has a clear connection to various NRC regulations to include:

- 50.55(a)(h)
- Various 10 CFR Part 50, Appendix A “General Design Criteria (GDC)”
- Various 10 CFR Part 50, Appendix B “Quality Assurance” Criterion

Safe Design Objectives (SDOs)

- SDO Definition: Objective criteria for addressing the potential for a software defect being introduced during the software development and integration processes
  - Approximately 70 defined SDOs that yield software quality
  - Provided for both platform and application software
  - Formulated using IEC 61508 and EPRI research

SDO Examples from NEI 20-07

- Application software requirements are derived from, and backward traceable to, the functional and performance requirements of the affected plant systems and their design and licensing bases (10.1.3.1)
- A hazard analysis method is used to identify hazardous control actions that can lead to an accident or loss, and application software requirements and constraints are derived from the identified hazardous control actions (10.1.3.2)

This Photo by Unknown Author is licensed under CC BY-SA

SDOs Connect to 1st Principles

- Each SDO:
  - is linked to one or more 1st principle
  - has established goals
- SDOs → 1st Principles → NRC Regulations
- Creates a verifiable and defensible chain

This Photo by Unknown Author is licensed under CC BY-NC-ND

Assurance Case

- Document adherence with the SDOs
- Traceable method to clearly demonstrate how each SDO was met
- Justification for any exceptions taken to a given SDO

Summary

- 1st Principles completely describe the progression from systematic failures (latent software defects) to CCFs in plant systems
- Each 1st Principle aligns with one or more NRC regulations
- Meeting Safe Design Objectives (SDOs) supports and upholds the 1st Principles
- Various defensive design meaures can be used to meet SDOs as evidenced and documented by the Assurance Case

This Photo by Unknown Author is licensed under CC BY-NC-ND

Proposed Schedule

- Fall 2020 – NEI 20-07 provided to NRC Staff for pre-endorsement/informal review
- January 12, 2021 – Initial public meeting to kickoff the document review
- February/March XX, 2021 - public meeting to begin detailed discussion of NEI 20-07
- Q2 and Q3 2021 - Future public meetings to discuss NEI 20-07 content
- Q4 2021 – NEI 20-07 submittal for NRC formal endorsement