DRAFT for Interim Use and Comment

U. S. NUCLEAR REGULATORY COMMISSION

DESIGN-SPECIFIC REVIEW STANDARD FOR mPower^{TM} iPWR DESIGN

Appendix C

Simplicity

Introduction

Simplicity is considered to be a cross-cutting principle that affects the fundamental design principles. For safety instrumentation and control (I&C) systems, designers and regulators are faced with the question of what measures should be in place in order to maintain other design principles such as independence and defense-in-depth with reasonable confidence. At a generic level, it is difficult to define and control simplicity/complexity for digital safety I&C systems. When faced with several design options on how to implement a function, from a safety perspective, the more simple design options are those that accomplish the function and address potential hazards with the most confidence and clarity. Additional guidance on hazards is contained in Appendix A, "Hazard Analysis."

This Appendix provides an approach to evaluate whether simplicity has been considered in the design of the digital I&C system. Although there are no regulations, standards, or guidance to address the aspect of simplicity for digital I&C systems, recent experience in reviews of light water reactor applications has shown that complex I&C systems challenge the demonstration of conformance with safety system design criteria such as independence. In this context, the NRC considers simplicity as supporting all fundamental design principles for developing safety systems with high reliability. The application should contain sufficient information on the simplicity of the design to support the staff's determination of reasonable assurance of safety from the perspective of the fundamental design principles: independence, diversity and defense-in-depth, redundancy, and determinism. The reviewer should verify that the approach described in the application addresses specific effects of simplicity such as testability or proof-of-determinism.

Without the information related to the simplicity of the I&C system, the review of the fundamental design principles may take on a more segmented review approach resulting in a less streamlined, more complicated, and more resource-intensive review effort.

Relevant Information to Support Consideration of Simplicity during Design Review

The application should provide sufficient information to demonstrate that the design of the I&C systems considered simplicity both in the functionality of the system, as well as, in its implementation. With this information, the reviewer should confirm that simplicity attributes such as single function, fixed number of inputs and outputs, fewer configuration parameters, high testability, software architecture with no branching and minimal interrupts, etc. , are considered and incorporated in the design. These attributes help contribute to simplicity and enable high efficiency in the design.

The following areas related to the design of a plant's I&C systems should be considered in order to demonstrate that such systems meet the fundamental design principle of simplicity:

1. I&C system architecture
2. Hazards analysis
3. Independence
4. Redundancy
5. Determinism
6. Diversity and defense-in-depth

The staff should consider whether: (1) the I&C design is as simple as practical, and (2) that any added complexity does not diminish the design's conformance to the fundamental design principles. For those areas that exhibit complexity, the application should provide a full description regarding any complexity added to the I&C system design, as well as, a justification necessary to directly support the safety function. More complex design alternatives require a more resource intensive review by the staff and could potentially lengthen the review.

The reviewer should consider the following items in evaluating simplicity in an I&C system design:

1. This review is concurrent with the other fundamental design principles of redundancy, independence, diversity, and determinism contained in Chapter 7.1.

2. I&C System Architecture: The I&C architecture information described in Appendix B of Chapter 7 should be carefully considered to determine if the I&C design includes unnecessary or nonessential features that are not part of the safety function. The reviewer should also consider the following:

    A. The application should provide a top-down decomposition of the I&C system. This decomposition facilitates a logical, modular description of interactions, signal flows, help with the definition of interfaces, and allows a more effective review.

    B. The selected architecture should provide a demonstration of a balance between simplicity in concept and the capacity to satisfy regulatory and performance requirements. This includes deterministic behavior, independence, and redundancy.

    C. A safety benefit should be independently verifiable and should outweigh any concerns associated with the complexity it may introduce in the design.

    D. Digital I&C system and software components should be organized in a manner that promotes design simplicity.

    E. After reviewing information related to the I&C system's architecture, the reviewer should consider whether:

        i. A structured and modular architecture is applied.
        ii. The system, hardware and software elements, all relationships among them, as well as properties of both are fully described and address relevant requirements

3. Independence: Material from the independence section may be used by the reviewer to identify how simplicity is addressed in the design while considering IEEE 603. Specifically, the reviewer should consider the following:

    A. Whether inter-channel communications or communications between a safety and a nonsafety system exist in this design.

    B. Whether simplicity is implemented to reduce or eliminate inter-divisional communication, or implemented physical uni-directional communication in function processing and critical signal paths.

    C. Whether the design maintains separation or segregation among I&C functions within the circuitry, as it enhances simplicity, verifiability and testability of individual functions.

    D. The reviewer should consider whether the application proposed simple design options in the approach to address IEEE Std. 603. The following design attributes support this approach:

        i. There is adequate separation or segregation among I&C functions.

        ii. There are no unnecessary inter-channel communications.

        iii. There are no unnecessary communications between a safety and a nonsafety system unless the safety system is out of service.

4. Redundancy: Material from the redundancy section may be used by the reviewer to identify how the design achieved redundancy and avoided unnecessary complexity. Specifically, the reviewer may consider the following areas that could help identify unnecessary complexity:

    A. Ancillary, more complex functions are kept independent of the primary I&C safety functions.

    B. The design provides simple connections between redundant trains.

    C. The proposed design did not consider inter-channel communications.

    D. There are no communications between a safety and a nonsafety system, unless the safety system is out of service.

    E. Through the review of redundancy, the reviewer may:

        i. Consider whether simplicity is factored in the design, particularly for the primary I&C functions.

        ii. Consider whether complex functions are kept independent of the primary I&C safety functions.

5. Determinism: Material from the determinism section may be used by the reviewer to identify how simplicity is addressed to demonstrate deterministic behavior. Specifically, the reviewer may consider the following:

    A. Simple algorithms are considered in the design of system modules. In general, simplicity should not be sacrificed to achieve performance that is not required.

    B. I&C systems are designed using a finite state machine approach with all states well defined.

    C. Through the review of determinism, the reviewer may:

        i. Consider whether nonsafety features are segregated from the main safety signal path.

        ii. Consider whether there are interrupt functions that could interfere with the performance of the safety function.

        iii. Consider whether early detection of failures is facilitated by the self-diagnostic functions.

6. Diversity and Defense-in-Depth: Simplicity of a software structure is promoted through simple logic, cyclical execution, static resource usage, and avoidance of external interrupts. Material from the diversity and defense-in-depth section may be used by the reviewer to identify how simplicity is addressed to demonstrate diversity. Specifically, the reviewer may consider the following:

    A. How potential common cause failures (CCFs) are addressed and how simplicity is considered to address failures.

    B. If basic software and application software are separated, and if it is implemented in a high level programming language.

    C. If basic software performs only the minimal necessary functions, such as initialization, periodic execution of required functions, and error handling.

    D. If application software is described in a graphically symbolized manner, so that functions can be easily understood, verified and validated.

    E. If the design is proposing dynamic allocation of memory.

    F. Through the review of diversity and defense-in-depth, the reviewer may:

        i. Consider whether basic software and application software are separated.

        ii. Consider whether basic software is implemented in a high level programming language.

        iii. Consider whether basic software performs only the minimal necessary functions, such as initialization, periodic execution of required functions, and error handling.

iv. Consider whether application software is described in a graphically symbolized manner, so that functions can be easily understood, verified and validated.

v. Consider whether there is dynamic allocation of memory.

7. The following are additional examples of system features that could introduce unnecessary complexity to the I&C design and should also be carefully considered:

   A. Features or functionalities added to operational enhancement.

   B. Features added that could introduce interrupts to the critical safety system performance.

   C. Features added to cope with particular types of hazards that could negatively impact other safety design features.

   D. Excessive use of self-diagnostics or use of self-diagnostics that significantly increase risk of module failure over any substantial benefit to reliability.

   E. Provisions for troubleshooting and maintenance, including built-in self-test features, and external testing of circuit boards if necessary - consider accessibility of test points, need for special test equipment, and coverage of built-in self-testing and diagnostics.