DRAFT for Interim Use and Comment

U.S. NUCLEAR REGULATORY COMMISSION

DESIGN-SPECIFIC REVIEW STANDARD FOR mPower™ iPWR DESIGN

APPENDIX A. Hazard Analysis

Introduction

A hazard analysis (HA) is a process for examining an instrumentation and control (I&C) system throughout its development lifecycle to identify hazards (i.e., factors and causes), and system requirements[1] and constraints to eliminate, prevent, or control them. Hazard analyses examine safety related I&C systems, subsystems, and components, their interrelationships and their interactions with other systems, subsystems, and components to identify unintended or unwanted I&C system operation including the impairment or loss of the ability to perform a safety function.

This Appendix provides an approach to evaluate HAs used in the design of a digital I&C system. Experience with complex systems in general and with digital systems for critical functions in diverse application sectors in particular (including lessons learned from NRC experience in recent licensing reviews) has revealed that current hazard analysis techniques such as fault tree analysis (FTA) and failure modes and effect analysis (FMEA), by themselves, do not assure the discovery of (or assure absence of) system-internal hazards rooted in system development activities. In contrast, a hazard analysis should facilitate a more focused I&C system review and should help to ensure traceability among regulatory requirements, architectural considerations, and system requirements to enable a more effective, and efficient I&C licensing review.

The application should contain HA information sufficient to ensure that the applicant has identified the hazards of concern as well as the system requirements and constraints to eliminate, prevent, or control them. These system requirements and constraints ensure I&C system independence, redundancy, determinism, and diversity and defense-in-depth, which are the fundamental design principles described in Section 7.1 of this Design Specific Review Standard (DSRS).

---

[1] The design of digital I&C systems is governed by the legal requirements set forth in NRC regulations, including those in several of the General Design Criteria in 10 CFR Part 50, Appendix A and 10 CFR 50.55a(h), which incorporates by reference IEEE std. 603-1991. NRC guidance endorses other IEEE standards, and these IEEE standards, as well as IEEE std. 603-1991, are written in terms of so-called functional, performance, design, and other "requirements." These terms are well-understood in the I&C technical community, but, except as used in IEEE std. 603-1991, are not legal requirements. To avoid confusion, this DSRS section will use the "requirements" terminology of the IEEE standards that are not incorporated into NRC regulations in connection with references to such standards. These "requirements," as referenced in this DSRS section, should be understood as recommendations that the NRC staff considers adequate to satisfy portions of NRC regulatory requirements, but which are not the only acceptable methods of compliance. The functional, performance, design, and other requirements of IEEE std. 603-1991, which are legal requirements, will be explicitly identified as originating from IEEE std. 603-1991.

DRAFT for Interim Use and Comment

This appendix does not endorse any particular technique(s) for the development of HA. Rather, the information contained in this appendix provides examples of topics that the reviewer should consider in determining the adequacy and completeness of an HA. The reviewer will evaluate the adequacy of the application of any particular HA technique or combination of techniques to a topic identified below on a case by case basis.

A. HA Scope

This HA review guidance applies to any I&C system or element of a system to which a safety function is allocated, or on which a safety function depends, or which could impair a safety function. Impairment includes:

- not providing the function,
- providing the function when not needed,
- providing the function at the wrong time or for too long a duration or for too short a duration or out of sequence,
- providing the function based on incorrect value of the controlled parameter or variable,
- providing the function erratically, e.g. creating chatter or flutter of the controlled variable or parameter,
- Interfering with another action.

HA of an I&C system or I&C system element includes interaction with both its internal and external environment within the scope of Chapter 7 review areas. An applicant's HA could inform overlapping areas, such as human-machine interface systems, but these are outside the scope of Chapter 7 review of an applicant's HA.

HA is iterative and should be performed at every phase in the system development lifecycle to identify new hazards that could arise as the design is implemented in software and hardware.

B. HA Information to be reviewed

The applicant's HA should describe and define each I&C system to be analyzed, and identify each loss or impairment of safety function that the I&C system should prevent.

For each system, the reviewer should consider at a minimum, the areas identified below. For each identified area, the reviewer will confirm whether the applicant performed an HA adequate to identify the hazards that could lead to impairment or loss of a safety function during all modes of operation (such as power operating mode, cooldown mode, hot shutdown mode, refueling mode, etc.). In addition, the reviewer will confirm that the applicant evaluated the impact of each identified hazard on the safety system, its subsystems and components, and their interrelationships. The reviewer will also confirm that the design provides the necessary hazard restrictions and controls in the form of architectural and environmental constraints, or additional safety features to show that safety functions will be accomplished.

<u>Evaluation Topics</u>

1. I&C system functions and constraints are properly allocated between hardware and software.

   1.1. There should be no undesirable or unintended functions

2. System behavior should be completely and correctly understood and specified, and the system should behave in a predictable and repeatable manner

2.1. All states, including failure mode states, safe state regions, and safely recoverable process states, are known.
2.2. System is in a known state at all times, e.g. through positive monitoring and indication.
2.3. Each transition from a current state (including initial state) to some next state is known.
2.4. Analysis of the system should demonstrate that conflicts among shared system resources will not interfere with correct, timely execution of a function.

3. Expected values, type, and range of system inputs and outputs are known, monitored and verified.

4. Conditions such as degradation, drift, and unacceptable deviation that could lead to unanalyzed system states should be detectable by the I&C system and appropriate intervention provided before impairment or loss of the safety function.

5. Boundaries of each I&C safety system and the interfaces, interactions, and inter-dependencies with other systems should be specified (including physical, functional, temporal, etc.)

   5.1. Redundancy should not be compromised through a dependency or interference.

   5.2. System interactions should be limited to those necessary to accomplish the safety functions.

   5.3. System interactions and interconnections that preclude complete V&V should be avoided, eliminated, or prevented.

   5.4. System independence should be assured across lines of defense-in-depth, redundant divisions, and monitoring and monitored elements of system (e.g., there is no unintended or undesirable communication pathway).

6. The nature of change in a monitored physical phenomenon (such as pressure, temperature, flow, or neutron flux density) is correctly characterized in the I&C systems.

7. Internal hazards that could be generated by the I&C system. For example, excessive load or demand on resources by the I&C system, such as electric power overload due to a short circuit or communication bus overload.

8. External hazards such as disruption in I&C system conditions and physical conditions in the environment that may impair a safety function, e.g.:

   8.1. Water intrusion.

   8.2. Uncontrolled transfer of energy into the system. Such energy may take various forms, e.g.: heat; light; vibration; radiation; electromagnetic radiation.

   8.3. Interruption of services (primary; secondary; other forms of back-up), e.g. electric power supply.

   8.4. Disturbance in services, propagating to a disturbance in a main signal, e.g.: electric power supply; service water; service air.

   8.5. Breaching of isolation barriers, e.g. cable penetration; other duct penetration.

   8.6. Adverse conditions in temperature, pressure, or humidity/moisture, e.g. too high or too low or rapid changes.

C. HA Information to be considered for Inspections, Tests, Analyses, and Acceptance Criteria (ITAAC)

ITAAC will be used to verify that the I&C system has been implemented and installed in accordance with the approved design and performs its safety functions. To the extent that system implementation and installation involves HA, the ITAAC will be used to verify that the HA was adequate. Activities in the scope of ITAAC would verify that the constraints through hazard analyses have been satisfied. Section 14.3.5 of the DSRS will provide specific ITAAC evaluation criteria.
The reviewer should ensure appropriate ITAAC associated with HA are identified by the applicant since hazards that could lead to the impairment or loss of safety function can be generated as the design is implemented. The sections below provide two examples. It is the applicant's responsibility to identify additional contributory hazards and the appropriate ITAAC commitments associated with the implementation of their design.

I&C systems development process contributory hazards

The I&C development process can contribute to hazards that could lead to the impairment or loss of system safety function. For example, the development process may include erroneous, incomplete, or improperly implemented I&C system requirements. The application may provide information associated with contributory hazards as the system is developed, and the reviewer should evaluate this information for adequacy during the review of the application. However, an applicant need only submit the information required by the regulation governing the content of the application. Detailed HA information beyond the level of the FSAR will be reflected in the scope of ITAAC. The reviewer should confirm that the HA information includes the necessary controls for the various contributory hazards and the associated commitments for each phase of the development process. In determining whether a license can be issued, the reviewer will confirm that the application identifies ITAAC for the I&C safety systems that reflect HA during each phase of the development process that is not completely reviewed in either the design certification or COL review.

In the review of information associated with HA during each phase of the development process described in the application, the reviewer will consider hazard controls and commitments associated with life-cycle phases for I&C safety systems. Examples of such controls for contributory hazards are listed below, but this list is not exhaustive and is dependent on the specific design implementation.

1. I&C Requirements are analyzed for completeness, e.g.:
   1.1. I&C requirements should be correctly identified and translated into derived constraints on all system elements
   1.2. I&C requirements should account for inter-relationships and interactions with the environment in all configurations and modes (including degraded ones), and changes from one to another.
   1.3. I&C requirements should include time-dependencies, relationships and constraints.
2. I&C requirements should be formulated to maintain the plant in a safe state.
3. I&C requirements and their dependencies with other I&C requirements should be identified, evaluated, and tracked.
4. Each requirement associated with a hazard should be traceable and subject to configuration control.

5. Methods to describe, represent, or specify architectures should support transformations or mappings across architectural descriptions, e.g., transformation from system conceptual or I&C requirements level to system design level to software design level to software implementation level to procedure or subroutine or function level.
6. Methods to describe, represent, or specify architectures should support transformations or mappings across dissimilar elements, e.g., interactions across hardware and software elements.
7. Methods to describe, represent, or specify architectures should support transformations or mappings across elements from different sources or suppliers.

Software-related contributory hazards

The I&C safety software can contribute to hazards that could lead to the impairment or loss of system safety function. For example, the software may use non-deterministic tasks such as interrupts. The applicant may provide information associated with contributory hazards as the software is developed, and the reviewer should evaluate this information for adequacy during the review of the application. However, an applicant need only submit the information required by the regulation governing the content of the application. The adequacy of detailed information beyond the level of the FSAR will be verified in the context of ITAAC. The reviewer should confirm that the HA information includes the necessary controls for the various contributory hazards and the associated commitments. The reviewer will confirm the application identifies the appropriate ITAAC for HA during software development that is not completely reviewed in determining whether a license can be issued.

In the review of information associated with HA during software development described in the application, the reviewer will consider hazard controls and commitments. Examples of such controls for contributory hazards are listed below, but this list is not exhaustive and is dependent on the specific software implementation.

1. The behavior of an element (e.g., a software unit) should be a composite of the behaviors of its constituent elements, with well-defined unambiguous rules of composition.
   1.1. Interfaces of elements are unambiguously specified, including behavior.
   1.2. Interactions across elements occur only through their specified interfaces, i.e., interactions adhere to principles of encapsulation.
2. The system should be modularized, and thereby avoid unnecessary interdependence.
3. Each element should be internally well-structured. For example:
   3.1. A software unit implementing one or more safety functions is composed from semantically unambiguous functions using well-defined unambiguous rules of composition.
   3.2. Paths from inputs to outputs avoid unnecessary coupling.
4. The system design should favor simple approaches and avoid system behavior that increases complexity, e.g.:
   4.1. Tasks should be executed in a deterministic manner
   4.2. Tasks in execution should run to completion
   4.3. Resources such as memory and processor execution time should be allocated statically
5. Naming conventions and data dictionaries should be established for ease of comprehension and bidirectional traceability.