Revision Log

Revision	Description of Changes
0	Initial Issue.

EXECUTIVE SUMMARY

Hazard Analysis (HA) is a process for examining an instrumentation and control (I&C) system throughout its development life cycle to identify hazards (i.e., factors and causes), and I&C requirements and constraints to eliminate, prevent, or control those hazards. HAs examine safety-related I&C systems, subsystems, and components and 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 white paper is written to describe the SMR-160 HA methodology for explanatory purposes with the NRC. This is part of the pre-application activities that support the development of a construction permit application (CPA) as part of a two-step license approach under Title 10 of the Code of Federal Regulations (CFR) Part 50, "Domestic licensing of production and utilization facilities". The objective is to familiarize NRC staff with the HA process of the SMR-160 and solicit feedback on the compliance of the design with applicable regulations and identify any areas that the NRC identifies may be higher potential licensing risk that require a more thorough discussion.

Statement of Limitation

Although required by regulation, as is covered in this report, there is limited implementation guidance for the methods of conduct for a Hazard Analysis. The satisfaction of requirements in the methodology chosen is explained in depth by this report. The development of the methodology was done in accordance with existing guidance but was not a derivative of it. Additionally, the nature of the Hazard Analysis process is one that is revisited over the lifecycle of the plant. It is recognized that not all aspects of the design, like operating procedures, are known; not all corrective actions from the Hazard Analysis are implemented. This limitation is the reason behind reperforming the Hazard Analysis throughout the lifecycle of the plant.

Table of Contents

Executive summary 2
1.0 Introduction 4
1.1 Scope 4
1.2 Purpose 4
1.3 Objective 4
1.4 Terms and Acronyms 5
2.0 Regulatory Basis for Hazard Analysis 6
3.0 Methodology 10
3.1 Hazard Identification Methodology 10
3.2 Hazard Evaluation Methodology 16
3.3 Hazard Control Methodology 16
4.0 References 18

List of Figures

Figure 1-1 Hazard Analysis Scoping Boundary 4
Figure 3-1 Coverage of Analysis Methods by System Detail (From EPRI Guide) 11
Figure 3-2 Coverage of Analysis Methods by Lifecycle Phase (From EPRI Guide) 11
Figure 3-3 Coverage of Analysis Methods by System Behavior (From EPRI Guide) 11
Figure 3-4 Blending FFMEA or FTA results with a DFMEA (From EPRI Guide) 13

List of Tables

Table 3-1 Potential Benefits of FTA to Various Analyses (From EPRI Guide) .. **Error! Bookmark not defined.**

1.0 INTRODUCTION

1.1 Scope

SMR-160 Hazard Analysis scope, per the requirements of IEEE 7-4.3.2 [1], covers all safety systems, their functions, and immediate interfaces with non-safety systems. When scoping the Hazard Analysis, IEEE 7-4.3.2 Annex D and the NuScale DSRS [2] provide complimentary and ample coverage of system bounding for HA purposes. This scope boundary (illustrated in Figure 1-1) [[

]]

[[

]]

Figure 1-1 Hazard Analysis Scoping Boundary

1.2 Purpose

The purpose of this whitepaper is to describe the methodology for performing the HA for the SMR-160.

This whitepaper will address the goals of the HA including:

- Identify single failure vulnerabilities
- Prevent loss of safety functions or critical functions
- Prevent inadvertent actuation
- Protect equipment

1.3 Objective

The objective of this white paper is to familiarize NRC staff with the I&C HA of the SMR-160 and solicit feedback on the compliance of the design with applicable regulations and identify any areas that the NRC identifies may be higher potential licensing risk that require a more thorough discussion.

1.4 Terms and Acronyms

A master list of terms and acronyms is contained in the SMR-160 Project Systems List, Acronyms, and Glossary of Terms [3]. The following are additional terms or acronyms used specifically in this report:

HA	Hazard Analysis
DSRS	Design Specific Review Standard
[[	]]
[[	]]
[[	]]
PSA	Probabilistic Safety Assessment
RPP	Reactor Protection Processor
PSS-CCP	Plant Safety System Component Control Processor

2.0 REGULATORY BASIS FOR HAZARD ANALYSIS

The regulations surrounding the performance of the HA stem from the 10CFR50 [4] requirement to satisfy IEEE Std. 603 [5] and ensuing guidance that can be found in IEEE standards and Regulatory Guides. This section lays them out in the logical progression from broadest to most specific guidance.

10 CFR 50.55a (h)(3) [4] directs that

Safety systems. Applications filed on or after May 13, 1999, for construction permits and operating licenses under this part, and for design approvals, design certifications, and combined licenses under part 52 of this chapter, must meet the requirements for safety systems in IEEE Std. 603–1991 and the correction sheet dated January 30, 1995.

IEEE Std. 603-1991 [5] in section 4.8 and 4.9 requires design basis analysis that points to hazard analysis

> "4.8 The conditions having the potential for functional degradation of safety system performance and for which provisions shall be incorporated to retain the capability for performing the safety functions (for example, missiles, pipe breaks, fires, loss of ventilation, spurious operation of fire suppression systems, operator error, failure in non-safety-related systems).
>
> 4.9 The methods to be used to determine that the reliability of the safety system design is appropriate for each safety system design and any qualitative or quantitative reliability goals that may be imposed on the system design."

and, more influentially, references additional guidance on the application of the criteria

> "Guidance on the application of these criteria for safety systems using digital programmable computers is provided in IEEE/ANS 7.4.3.2-1982."

Regulatory Guide (RG) 1.153, Revision 1 [6] in 'Section B. Discussion' endorses RG 1.152 Revision 1 [7] as an acceptable method of meeting regulatory requirements for digital computers in safety systems:

> "Section 1.2 of IEEE Std. 603-1991 references IEEE/ANS 7.4.3.2-1982. Revision 1 to Regulatory Guide 1.152, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants," endorses the 1993 version, IEEE Std. 7-4.3.2-1993, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations." Thus, Revision I to Regulatory Guide 1.152 constitutes an acceptable method of meeting the regulatory requirements for digital computers."

Regulatory Guide (RG) 1.152, Revision 1 [7] in 'Section B. Discussion' stipulates that nuclear power plants using digital safety systems must meet all requirements of IEEE Std. 7-4.3.2-1993 [8]:

> "Conformance with the requirements of IEEE Std 7-4.3.2-1993, "Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," with the exception of relying solely on quantitative reliability goals (Section 5.15), is a method acceptable to the NRC staff for satisfying the Commission's regulations with respect to high functional reliability and design quality requirements for computers used as components of a safety system."

In **RG 1.152 Revision 3** [9], section C.1. Function and Design Requirements directly states in nearly identical language that conformance to the updated IEEE Std. 7-4.3.2-2003 [8] is sufficient for computerized safety systems.

> "Conformance with the requirements of IEEE Std. 7-4.3.2-2003 is a method that the NRC staff has deemed acceptable for satisfying the NRC's regulations with respect to high functional reliability and design requirements for computers used in the safety systems of nuclear power plants. As addressed in Section B above, the NRC does not endorse Annexes B-F of IEEE Std. 7-4.3.2-2003.

In seeking to satisfy **IEEE Std. 7-4.3.2-2003** [8] requirements, we find that hazard analysis is directly named as a necessary exercise of plant design in section 5.5.1.

> "Design for PDD (programmable digital device) integrity ... A hazard analysis (see Annex D for guidance) shall be performed to identify and address potential hazards of the system."

RG 1.152 Rev 3 [9] also states that, even though Annex D of IEEE Std. 7-4.3.2-2003 [8] is not endorsed due to lack of execution guidance as mentioned above, it is useful for scoping the hazard analysis.

> "Annex D, "Identification and Resolution of Hazards," provides general information on the use of qualitative or quantitative fault tree analysis (FTA) and failure modes and effects analysis (FMEA) techniques throughout the system development life cycle. The staff agrees that FTA and FMEA are well-known techniques for analyzing potential hazards; however, the NRC has not endorsed this annex because it provides inadequate guidance concerning the use of FTA and FMEA techniques. While this Annex is not endorsed, the hazard identification guidance in Annex D may provide useful information on the assessment of the susceptibility of digital safety systems to inadvertent access or undesired behavior of connected systems.""

It is of note that the NRC has published in its **2019 review of RG 1.152 Rev 3** [9] that a revision is required to endorse IEEE Std. 7-4.3.2-2003 [8] along with its revised Annex D.

> "Based on results of the periodic review, a revision to RG 1.152, Revision 3, is warranted.... The staff anticipates that the RG can be simplified and IEEE Std 7-4-3.2-2016 may be endorsed with few exceptions and minimal clarifications."

Specifically, the following line of guidance from **Annex D.2 of IEEE Std. 7-4.3.2-2003** [8] was used in generating this report.

> "The scope of the hazards analysis includes the safety system's external boundaries that interface and interact with the rest of the plant (including non-I&C elements)"

In **DNRL-ISG-2022-01** [10] Safety Review of Light-Water Power-Reactor Construction Permit Applications, the NRC provides clarifications to the existing review guidance in NUREG–0800 regarding instrumentation and control, specifically pointing to Nuscale's design specific review standard (DSRS) [2]:

> "The guidance in SRP Chapter 7, "Instrumentation and Controls," is system focused and does not take advantage of such a unifying framework. The DSRS guidance aims to address all the significant aspects of the I&C design in a unified manner through this

framework to minimize the repetition of the requirements in a system-focused approach. The structure of the DSRS guidance reflects an integrated I&C design using digital technology; introduces the use of an integrated hazards analysis approach to the I&C reviews; consolidates the various methods discussed in SRP Chapter 7; and provides a consistent, comprehensive, and systematic way to address the potential hazards associated with the I&C systems in a unified framework."

Having established the requirement and basis for performing a HA, referenced **NuScale's DSRS** [2] for more concrete and succinct guidance, as supported by DNRL-ISG-2022-01 [10], of how to perform it:

"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 the following:

• not providing the function when it is needed

• providing the function when it is not needed

• providing the function at the wrong time, for too long or too short a duration, or out of sequence

• providing the function based on an 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 or function

…

Evaluation Topics

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

A. 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.

A. All states, including failure mode states, safe state regions, and safely recoverable process states, are known.

B. System is always in a known state (e.g., through positive monitoring and indication).

C. Each transition from a current state (including initial state) to some next state is known.

D. 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 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.).

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

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

C. System interactions and interconnections that preclude complete verification and validation should be avoided, eliminated, or prevented.

D. 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 should be identified. 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. External hazards such as disruption in I&C system conditions and physical conditions in the environment that may impair a safety function should be identified. For example:

A. Water intrusion

B. Uncontrolled transfer of energy into the system

i. Such energy could take various forms (e.g., heat; light; vibration; radiation; electromagnetic interference).

C. Interruption of services

i. Services could be primary, secondary, or other forms of back-up (e.g., electric power supply).

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

E. Breaching of isolation barriers (e.g., cable penetration; other duct penetration)

F. Adverse conditions in temperature, pressure, or humidity/moisture (e.g., too high or too low or rapid changes)"

In summary, 10CFR50.55a (h)(3) [4] requires satisfaction of the requirements of IEEE 603 [5] for safety systems. RG 1.152 [9] further expounds on this to stipulate that following the regulations of IEEE 7-4.3.2 [8] satisfies the requirements of IEEE 603 [5] for digital safety systems. IEEE 7-4.3.2 [8] states that a hazard analysis is needed for digital safety systems due to inadequacies in past safety analysis techniques, and NuScale's DSRS [2] is used to determine the scope.

3.0 METHODOLOGY

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

]]

EPRI Report 3002000805 (EPRI guide) [12], supplementary to IEEE 7-4.3.2 Annex D [1], provides comprehensive, practical, cost-effective methods for identifying hazards in digital systems before the systems are put into operation and meets several key objectives to this end:

1. Evaluate the capability of each method for identifying potential vulnerabilities in a digital I&C system, including hazardous interactions with plant components and plant systems
2. Demonstrate the workability of each method on practical examples based on experiences reported by EPRI members
3. Provide a step-by-step procedure for each method so that users can adapt them into a procedure format
4. Provide worked examples to demonstrate each method in a step-by-step manner
5. Use the results to identify the comparative strengths and limitations of each method
6. Provide guidance on how to blend multiple methods to gain efficiencies in the analysis, limit the analytical effort, or limit corrective actions such as design changes or the application of administrative controls to the identified hazards

As such, this HA will be accomplished in accordance with the EPRI guide [12] to ensure execution of a satisfactory HA.

The HA is comprised of three stages: Hazard identification, Hazard Evaluation and Hazard Control.

3.1 Hazard Identification Methodology

The EPRI guide [12] advocates for a blended approach where two or more methods are applied. This is done to use results from one method: as an input to another method, to limit the effort required by another method or, possibly most importantly, to identify the potentially critical hazards to be further evaluated by another method and limit the need for corrective actions to those which address critical hazards. The compatibility of the analyses chosen for this blended approach is described summarily below.

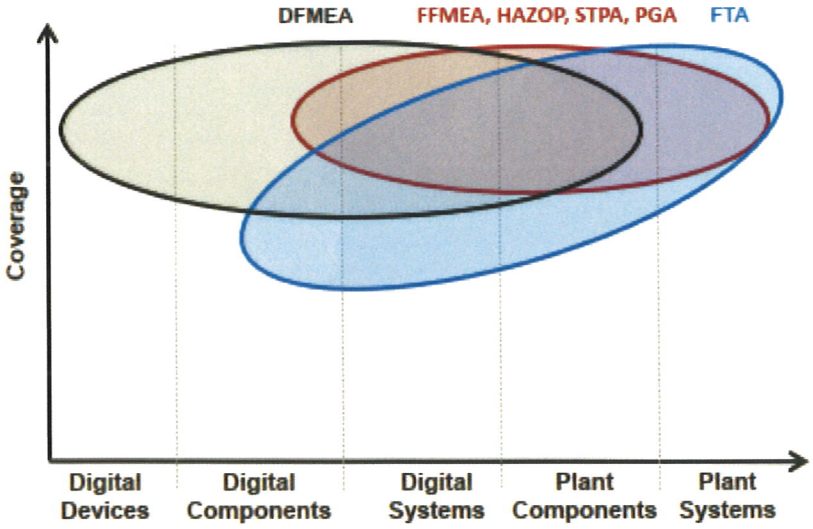

Figure 3-1 Coverage of Analysis Methods by System Detail (From EPRI Guide)

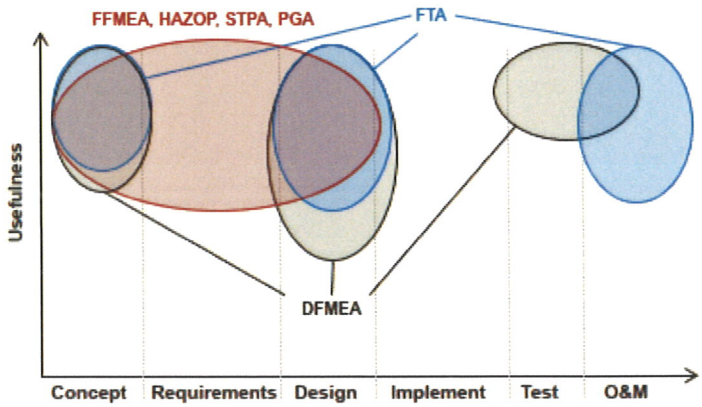

Figure 3-2 Coverage of Analysis Methods by Lifecycle Phase (From EPRI Guide)

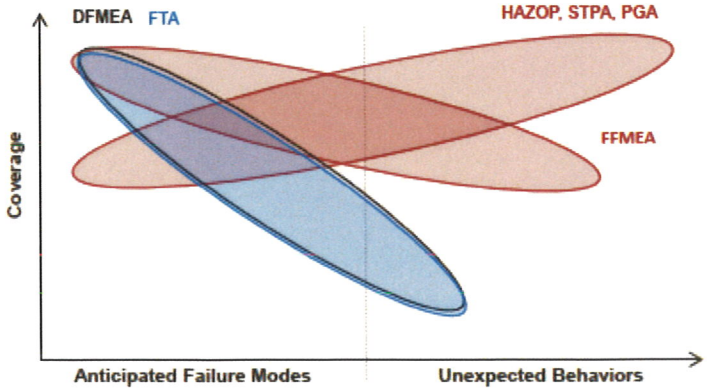

Figure 3-3 Coverage of Analysis Methods by System Behavior (From EPRI Guide)

Figure 3-1, Figure 3-2, and Figure 3-3 are from the EPRI guide [12] and show the coverage of different types of safety analyses. Best practice is to choose a combination of analyses that cover as much of the various dimensions as possible. [[

]]

[[

]]

[[

]]

[[ ]]

As a result, SMR-160 concluded that this is an effective blend of hazard analyses that fully satisfies all regulatory requirements for digital safety system HA. The below subsections capture descriptions of implementation for the above methods.

3.1.1 [[ ]]

[[

]]

3.1.2 [[ ]]

[[

]]

3.1.3 [[ ]]

[[

]]

3.2 Hazard Evaluation Methodology

The evaluation portion of the Hazard Analysis aims to combine the hazards identified in each of the subsidiary analyses and verify that safeguards in other plant capabilities exist for each hazard. From this evaluation, the most threatening hazards are identified, so they can be addressed in the Hazard Control Step. Major steps of evaluating hazards are to:

1. Categorize all identified hazards – categorization allows similar hazards to be more efficiently analyzed.
2. Determine effects of hazards – how the hazard impacts system function needs to be determined to allow its significance to be understood.
3. Evaluate the significance of hazards – significance is a measure of consequence and likelihood. The significance impacts how the hazard gets controlled, such as whether it is mitigated or eliminated.

3.3 Hazard Control Methodology

Hazard control is the process that enacts actions to mitigate, eliminate, or justify hazards that do not have adequate prevention, detection, or corrective methods. For hazards with high safety significance, elimination is the preferred methodology of controlling the hazard. Elimination is typically accomplished by changing the design to eliminate the hazard. In situations where the

hazard cannot be eliminated through design, lowering the significance to acceptable levels is preferred. When the hazard cannot be eliminated or have its significance reduced, detection methods should be put in place to mitigate the risk of the hazard. As a final option to address a hazard that cannot be addressed in other ways, procedures or training can be put in place to mitigate it. It may be acceptable to justify a hazard as acceptable if the significance is low enough.

The final step is documenting how each hazard has been controlled. [[

]]

4.0 REFERENCES

[1] IEEE 7-4.3.2, *IEEE Standard Criteria for Programmable Digital Devices in Safety Systems,* 2016.

[2] Chapter 7 Appendix A, *Design-Specific Review Standard for NuScale SMR Design, ADAMS Accession No. ML15355A316,* Revision 0.

[3] Holtec International, HI-2146109, *SMR-160 Project Systems List, Acronyms, and Glossary of Terms,* Revision 4.

[4] Nuclear Regulatory Commission 10 CFR 50.55a, *Codes and standards,* 2022.

[5] IEEE 603, *IEEE Standard Criteria for Safety System for Nuclear Power Generating Stations,* 1991.

[6] Nuclear Regulatory Commission RG 1.153, *Criteria for Safety Systems,* Revision 1, 1996.

[7] Nuclear Regulatory Commission RG 1.152, *Criteria for Use of Computers in Safety Systems of Nuclear Power Plants,* Revision 1, 1996.

[8] IEEE 7-4.3.2, *IEEE Standard Criteria for Programmable Digital Devices in Safety Systems,* 2003.

[9] Nuclear Regulatory Commission RG 1.152, *Criteria for Use of Computers in Safety Systems of Nuclear Power Plants,* Revision 3, 2011.

[10] Nuclear Regulatory Commission DNRL-ISG-2022-01, *Safety Review of Light-Water Power Reactor Construction Permit Applications,* 2022.

[11] JEXU-1041-1016-P, *MELTAC Platform Software Program Manual,* Revision 0.

[12] EPRI 3002000509, *Hazard Analysis Methods for Digital Instrumentation and Control Systems,* June 2013.

[13] Holtec International HI-2220167, *SMR-160 Plant Level Function Identification and Decomposition Report,* Revision 0.

[14] Holtec International HI-2220942, *Functional Failure Modes and Effects Analysis,* Revision 0.

[15] JEXK-0135-1009, *Failure Mode and Effects Analysis (FMEA) for Reactor Trip (RT) and Engineered Safety Features (ESF),* Revision A.