www.holtec.com
www.smrllc.com

SMR-160 I&C Hazard Analysis Overview

Date: 02/08/2023

Presented By: Collin Parry

SMR, LLC, A Holtec International Company
Krishna P. Singh Technology Campus
One Holtec Boulevard
Camden, NJ 08104, USA

[Not Export Controlled]

Agenda

- Introductions
- Purpose and Outcome
- Regulatory Basis
- Methodology Overview
- Discussion and Questions

Objective

- The objective is to familiarize NRC staff with the methodology for I&C Hazard Analysis of the SMR-160 including soliciting feedback on :
  - The compliance of the methodology with applicable regulations
  - Areas that have higher potential licensing risk that require a more thorough discussion.

Acronyms

- DSRS — Design Specific Review Standard
- MELCO — Mitsubishi Electric Corporation
- PSS — Plant Safety System
- CCP — Component Control Processor
- PCS — Plant Control System
- DAS — Diverse Actuation System
- FTA — Fault Tree Analysis
- DFMEA — Design Failure Modes and Effects Analysis
- FFMEA — Functional Failure Modes and Effects Analysis

Regulatory Basis

- 10 CFR 50.55a (h)(3)

  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

  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...

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

- RG 1.153 Revision 1

  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

- RG 1.152 Revision 1

  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.

- RG 1.152 Revision 3

  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...

  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.

  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.

- IEEE Std. 7-4.3.2-2003

  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...

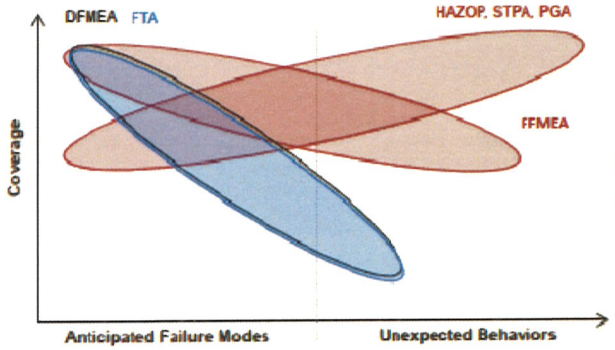
  The scope of the hazards analysis includes the safety system's external boundaries that interface and interact with the rest of the plant (including non-I&C elements)

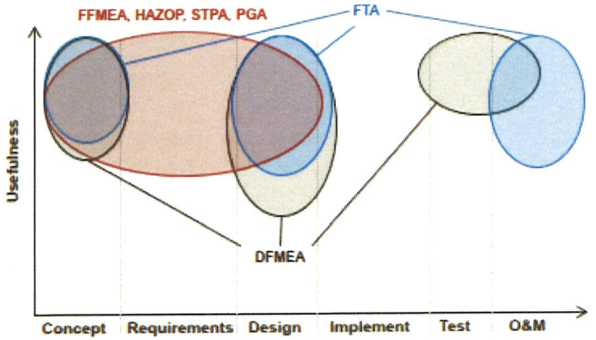
Methodology Overview

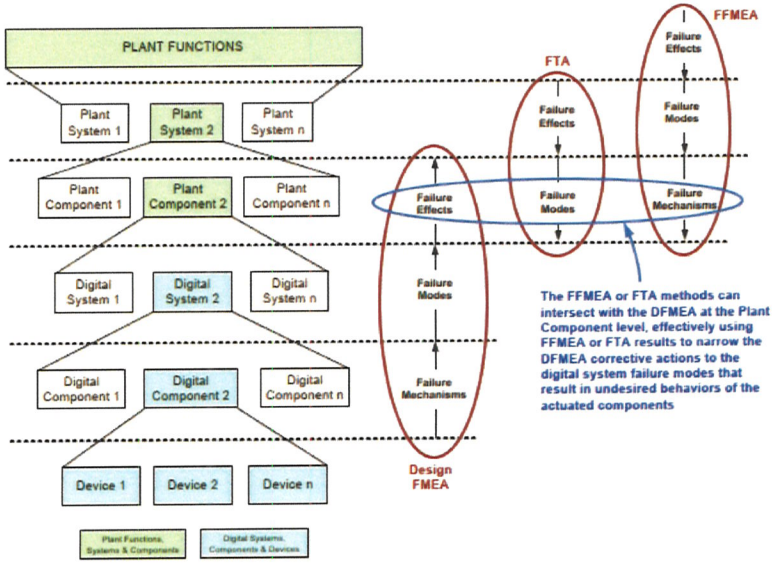
- Performed in accordance with EPRI 3002000805, it is comprised of 3 stages
  - Hazard Identification
  - Hazard Evaluation
  - Hazard Control

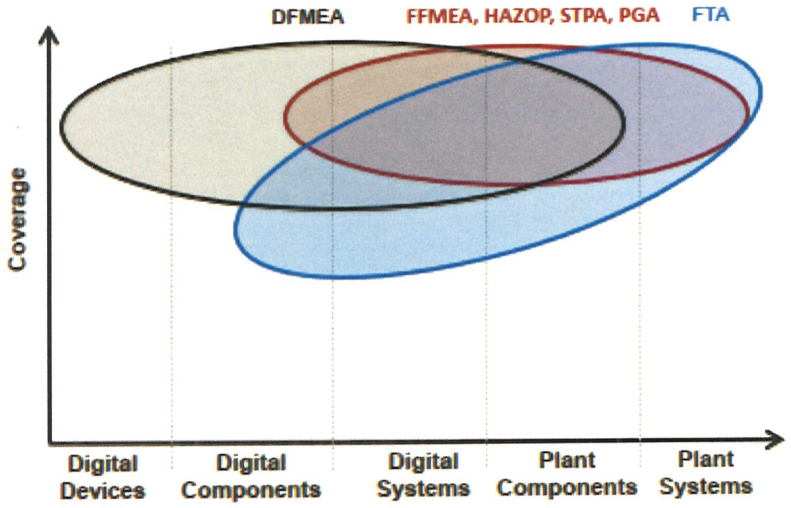
Hazard Identification Methodology

- DFMEA, FFMEA and FTA were chosen as the best combination for this HA because of their effective coverage, the existing design team and vendor experience in performing them, and their suitability for application early in the design phase.









Hazard Identification Methodology

- The FTA methodology is a method that postulates high-level plant failures and identifies the component faults required to achieve them. This top-down approach provides a plausibility and risk structure for certain failures and ensuing analyses to address them.
- The DFMEA identifies potential failures at the digital component level in SMR-160's digital safety systems and works bottom-up to identify resultant failures at the system function level. This postulates credible failure modes and their effects. Where these results and those of the top-down FTA approach intersect are of the most concern.
- The FFMEA method is used to identify the causes of unwanted or unacceptable failure mechanisms at the plant component level, which can be blended with the results of a DFMEA to focus design changes or other corrective actions on mitigating or eliminating significant failures. This coverage extends digitally controlled components to plant functions. As such, the scope of the FFMEA addresses a unique range of analysis that overlaps the FTA in scope and DFMEA in execution. This third layer of analysis ensures adequate coverage over the entire range of plant functions and shows continuity between the top-down FTA and bottom-up DFMEA processes.

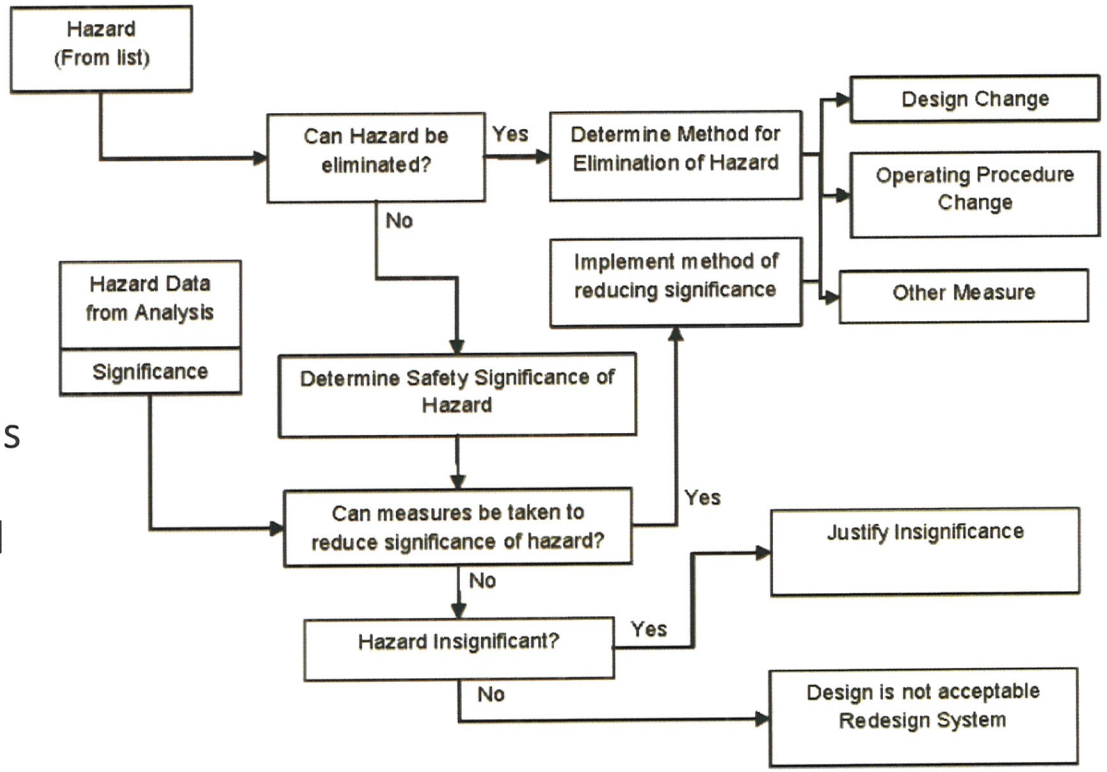
Hazard Evaluation Methodology

- 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.

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
  1. High safety significance- elimination through design change preferred.
  2. If elimination not possible– lower the significance to acceptable levels using design changes.
  3. Detection methods and procedural changes are least preferred due to desire to minimize Human Factors Engineering load.



Questions or Comments?