U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Digital Instrumentation and Controls Licensing and Inspection Workshop (Afternoon Session)

February 10, 2021

Workshop Agenda (PM)

- ISG-06 Alternate Review Process Reflection: NRC
- ISG-06 Alternate Review Process Reflection: Industry
- Open Discussion and Next Steps
- Public Comments

ISG-06 ALTERNATE REVIEW PROCESSES REFLECTION: NRC

Comparison of Tier 1 and ARP

Comparison of Tier 1 and ARP

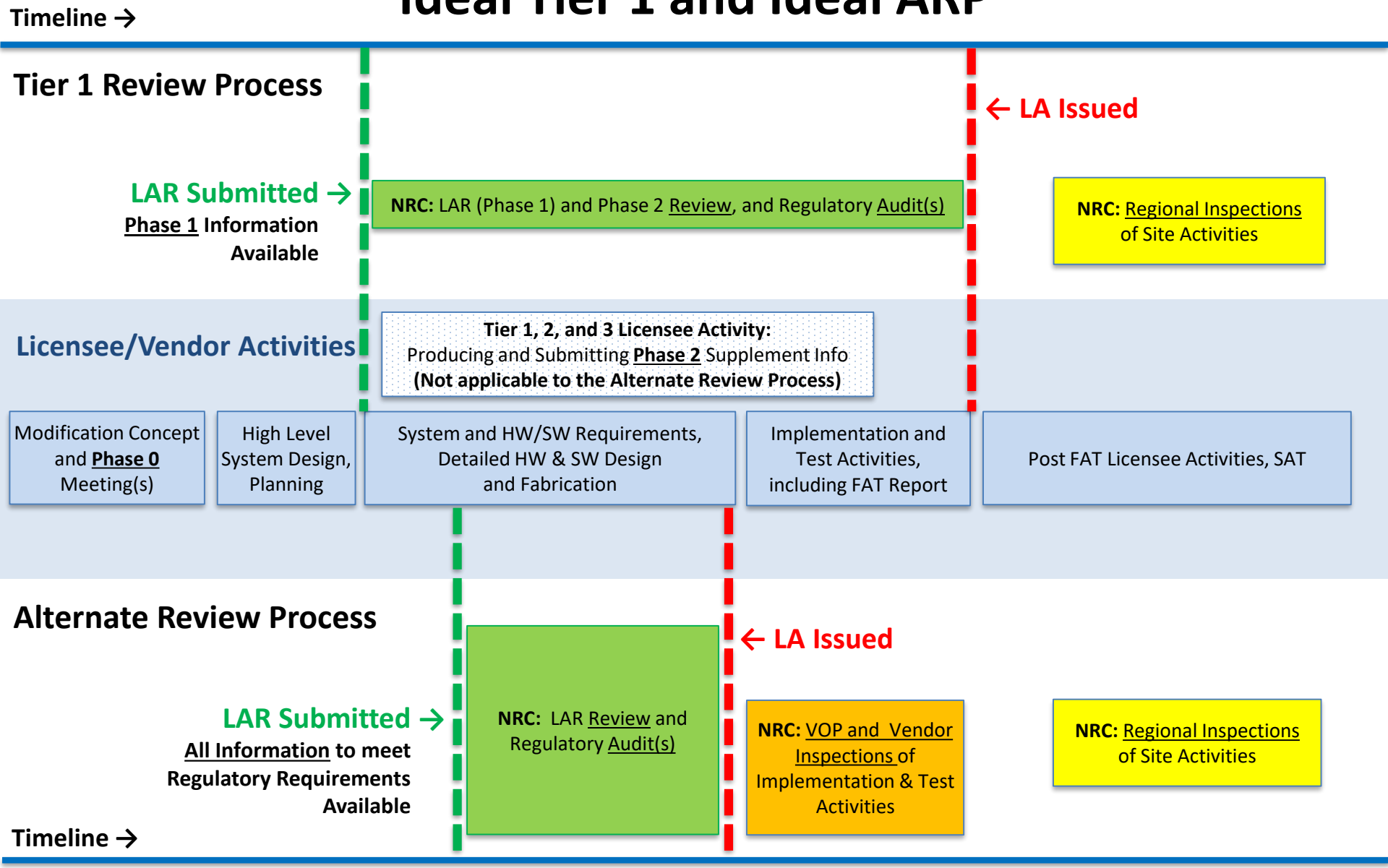
- Tier 1 Process:
  - is based on the evaluation of design outputs.
  - should be used when the system design is based on an NRC approved platform and the design is expected to be implemented and tested prior to issuance of the license amendment.

- Alternate Review Process:
  - is based on the evaluation of design plans/processes and licensee commitments to implement those plans/processes.
  - should be used when the system design is based on an NRC approved platform and an approved license amendment is needed or desired prior to implementing the system design.

Licensing and Oversight Comparison Summary

	Tier 1, 2, and 3 Review Process	Alternate Review Process
Document Submittals	2 Submittals (LAR – Phase 1) (Supplement – Phase 2)	1 Submittal (LAR)
Design Changes After LAR Submittal	Design changes submitted during the Phase 2 review (before FAT) can be reviewed as part of the LAR review	Design changes during Implementation and Testing phases will need to be performed under 10 CFR 50.59, or new LAR approval
License Conditions	None (Typically)	Potentially: • Implementation of high quality software development process (e.g., NQA-1-2015) • Vendor oversight • Resolution of plant specific action items identified in the topical report • Implementation and Test activities (e.g., FAT)
Inspection Scope	• Regional Inspection of Post FAT Licensee Activities (e.g., Installation, Maintenance, Training, Operations, Plans, SAT)	• VOP Implementation Inspection • Vendor Inspection of later lifecycle phases (e.g. FAT) • Regional Inspection of Post FAT Licensee Activities (e.g., Installation, Maintenance, Training, Operations, Plans, SAT)

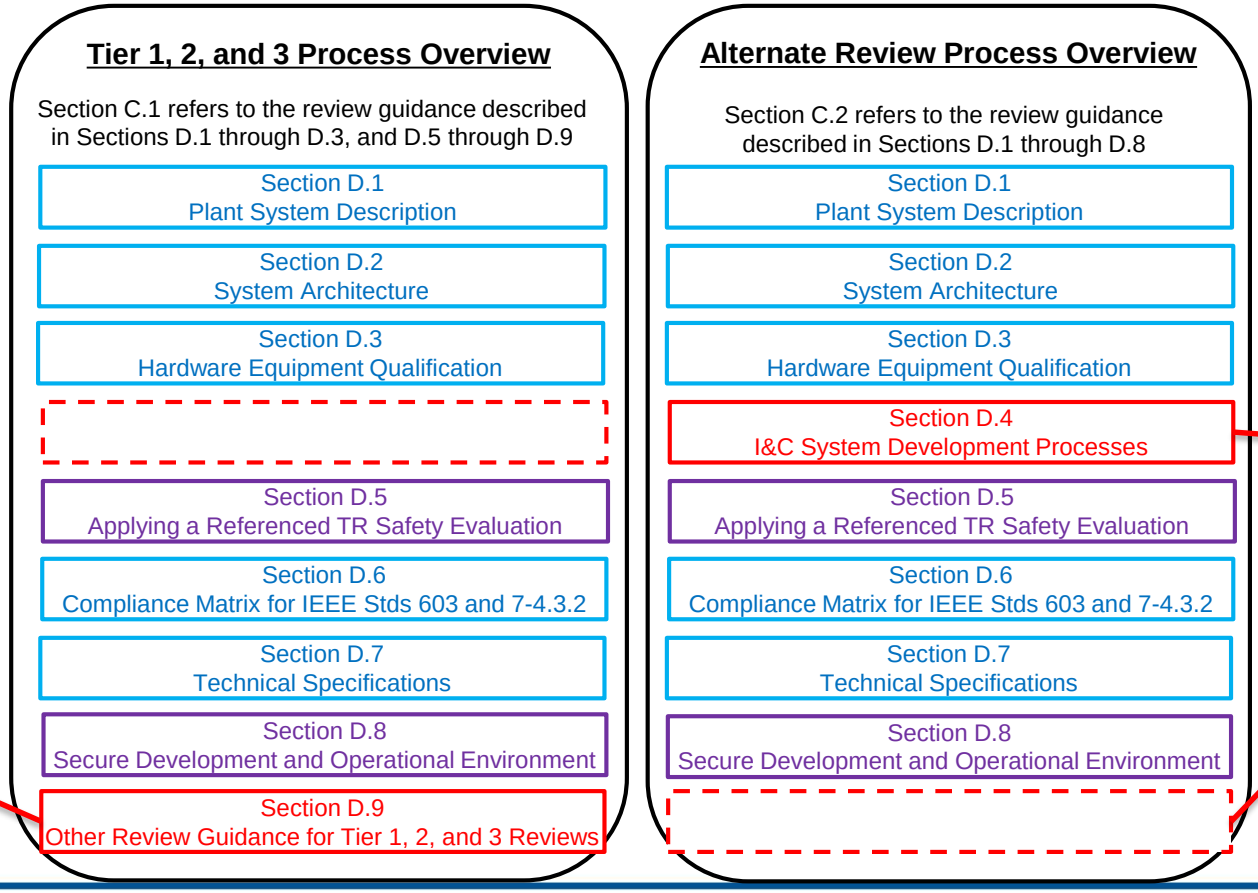
Comparison of Licensing and Oversight Activities
Ideal Tier 1 and Ideal ARP



ISG-06 Rev. 2 Structure & Focus Areas

(1) The design meets the applicable regulatory criteria

(2) The design is developed and will be developed using a high quality process



Review of Software Design, Implementation, & Test Plans and Processes

Review of design outputs (Implementation and Test Results Information)

Licensee Commitments that Implementation and Test Activities will be adequately implemented

Needed for Item (1)

Needed for Item (2)

Needed for Items (1) & (2)

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Alternate Review Process Focus Areas

- (1) The design meets the applicable regulatory criteria
- (2) The design will be developed using a high quality process
- Some attributes of development activities are critical to our early regulatory compliance finding for certain 10 CFR 50.55a requirements and implementing standards. For example:
  - following the development plans and processes, consistent with the LAR
  - following the VOP, consistent with the VOP summary
  - completing PSAIs
  - completing FAT
  - demonstrating risk-significant attributes of the final design specified in the LAR

Generic Lessons Learned: License Review Processes

- The characteristics of the Tiered Process and the ARP as described in the ISG may be considered the ideal scenarios for each review process.
- Reality: Both the information that is submitted and the system development timelines can vary from that which is assumed in the ISG.
- While piloting the ARP in pre-submittal and review activities, the staff has identified some unique challenges:
  - Conducting the licensing review based on the VOP Summary and regulatory commitments related to future activities.
  - Defining the role of licensing audit and Appendix B inspections of licensee development activities during the technical reviews.
- NRC may need to adjust its approach and consider aspects of both processes to resolve some technical issues in an efficient and timely manner.

Pre-submittal Meetings, and Licensing Review Efficiency

Pre-submittal Interactions

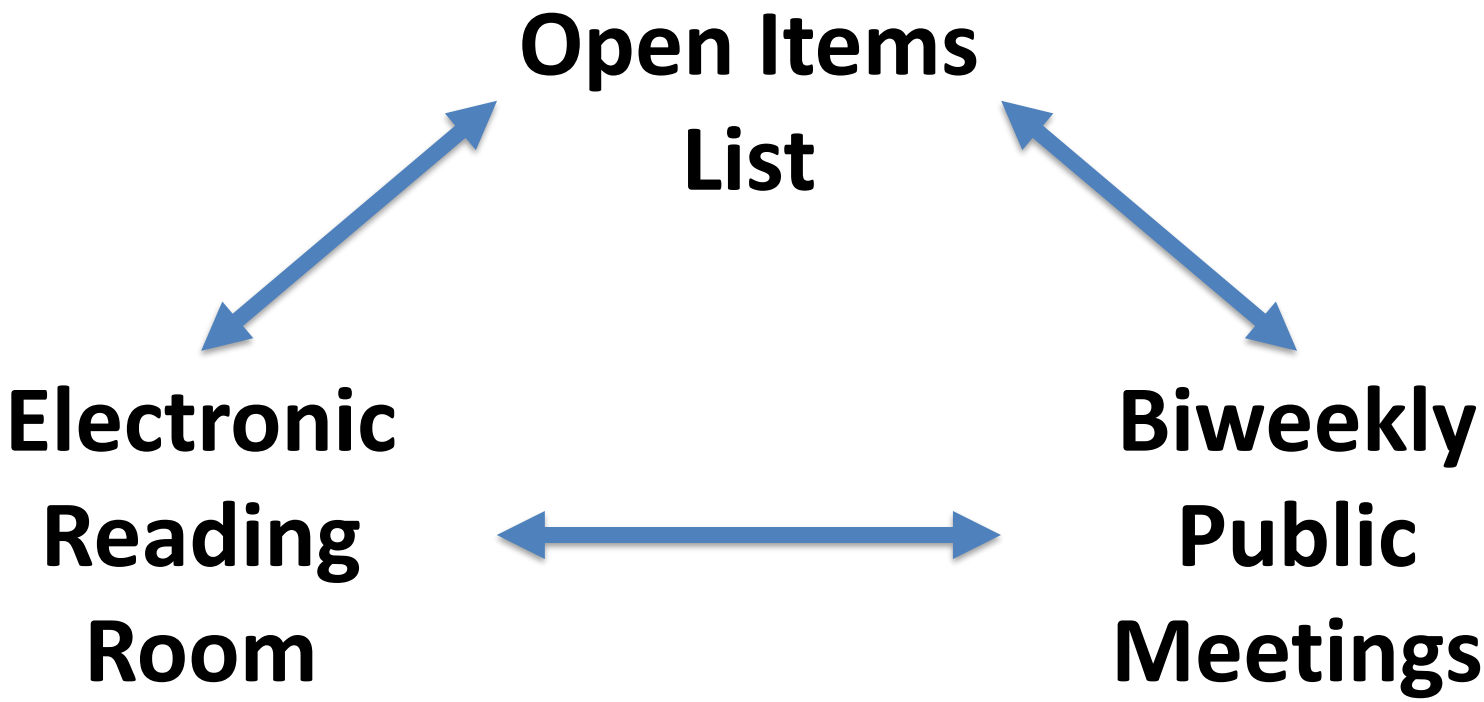
Multiple pre-submittal meetings have proven to be beneficial:

- to the licensee for preparing a LAR that can be accepted for review
- to the staff for preparing for the review

The following topics have been shown to be important in early interactions:

- Licensee-identified LAR Review Process and system development schedule
- ISG-06 Enclosure B table applicability and information availability
- Description of deviations from NRC guidance or the approved platform
- Details of the overall I&C systems architecture to demonstrate the fundamental I&C design principles of Redundancy, Independence, Diversity, and Determinism
- Approach for addressing potential CCF
- Vendor Oversight Process and planned activities
- Approach for Equipment Qualification testing before and after LAR submittal

Licensing Review Efficiency



Licensing Review Efficiency

- **Open Items List**
  - A means to clarify staff questions
  - Early identification of potential Requests for Additional Information (RAIs) and audit activities
  - Reduces RAIs and review time

- **Electronic Reading Room** (e.g., portal, SharePoint, Box.com)
  - Used to perform virtual audits of undocketed material
  - Minimized document submittals
  - Allows for auditing of living documents which are revised throughout the review (e.g., System Requirement Specifications and Vendor Oversight Plan)
  - Helps identify which document or portions of a document need to be docketed

- **Biweekly Public Meetings**
  - Provides a means to discuss open items, potential RAIs, audit planning activities
  - Closed portions used to discuss proprietary information
  - The frequency of the meetings is adjusted based on need and scheduling conflicts

Vendor Oversight Plan and Inspection Activities

VOP and VOP Summary

- ISG-06 ARP is based on staff evaluation of the docketed summary of the VOP in lieu of licensee submitting the entire VOP.
- The VOP framework should supplement the licensee's overall QA program descriptions with specific system, hardware, and software development activities, including a description of the proposed
  - development life cycles,
  - development documents to be produced, and
  - management activities that will be implemented in the design and development of digital I&C safety-related systems
- The VOP Summary will be reviewed against the requirements of Appendix B to 10 CFR Part 50.

Vendor Oversight Plan Level of Detail

- The NRC staff summarized what guidance in BTP 7-14 that vendor oversight should address, during a previous ISG-06 workshop.
- Specific guidance on what information should be presented in the VOP summary was not provided in ISG-06.
- Recent lessons learned shows that more detail may be necessary in the VOP summary for the staff to make a reasonable assurance finding that implementation of the oversight activities will ensure that design outputs and FAT results meet the system and development process requirements.

Software Development

- The ISG-06 ARP specifies that the LAR should include:
  - a description of the software life cycle processes to be used;
  - identification of any planned exceptions and clarifications; and
  - a description of how these planned exceptions and clarifications meet the underlying regulations.
- These items can be satisfied for LARs referencing an NRC approved Software Program Manual (SPM) for the development of application software.
- The VOP and VOP Summary should address how the licensee's oversight activities, that will verify the software development processes and the lifecycle design outputs, meet the software development process descriptions summarized in the LAR or any referenced SPM.

Interface with Inspections

- Inspections of licensee's oversight activities as documented in the VOP will be conducted in accordance with IP 35017, "Quality Assurance Implementation Inspection."
  - IP 35017 was updated in 2020 to address digital I&C LARs
- Inspections of vendor system development activities will be conducted in accordance with:
  - IP 43002, "Routine Inspections of Nuclear Vendors"
  - IP 35710, "QA Inspection of Software Used in Nuclear Applications"
- The NRC staff is evaluating IP 52003 for revision to address site activities for the digital I&C modifications and testing.

ARP Licensing vs Inspection

	LICENSE REVIEW (Submittal Review & Audits)	INSPECTIONS (Vendor & Licensee)
Scope	**System Design Information:** • System Architecture • System Requirements Specification • Equipment Qualification Results • D3, Redundancy, Independence, Determinism	
	Sufficiency of System Development Processes: • BTP 7-14 (B.3.1) Review of Plans • Crediting of SPM as applicable • Resolution of PSAIs or commitments to address PSAIs	**Appendix B Implementation of Processes:** • Design changes • Design outputs for implementation and testing lifecycle phases • Factory Acceptance Tests • Site Acceptance Tests
	<u>Sufficiency</u> of Vendor Oversight Plan for: • Verification and Validation • Configuration Management • Design Activities • Implementation Activities • Integration Activities • Testing Activities • Installation Activities	**Appendix B Implementation of VOP:** **(during Detailed Implementation, V&V, and FAT)** • Verifying oversight of vendor activities performed during those phases meet requirements for design control (e.g., design changes, independent V&V) • Verify that documentary evidence exists to ensure that the procured system conform to procurement requirements • Verifying that appropriate corrective actions were taken to address any deficiencies identified during oversight activities of the vendor • Verifying that the licensee performed required external audits on the vendor for activities performed during the above phases

ADAMS Accession No. for the one pager of this table is ML20267A173.

ARP Licensing vs Inspection

	LICENSE REVIEW (Submittal Review & Audits)	INSPECTIONS (Vendor & Licensee)
Findings	**Compliance Findings:** • 10 CFR 50.55(a) (IEEE-603-1991 criteria) • GDCs • Appendix B (e.g., QA Plan, VOP Summary)	• **Inspection Findings Against Appendix B to 10 CFR Part 50**
	Not in Scope[1]	**Not in Scope**
	• Implementation of software and hardware • Design output documentation and detailed V&V results for lifecycle phases after detailed software and hardware design • Resolution of Non-Conformances • Factory Acceptance Test Results	• Sufficiency of Design • Conformance with IEEE 603 & 7.4-3-2 • Vendor Oversight Plan Sufficiency (which may be audited during the LAR review to support the VOP summary review)

[1] These items would be subject to detailed license review and audit under the traditional review process

Other Technical Review Areas

Crediting of Self-Diagnostics to Eliminate Surveillance Requirements from Technical Specifications

- Self-diagnostics of digital I&C safety-related systems could be credited to either reduce or eliminate I&C surveillance testing.
- Supporting FMEA needs to be provided as part of technical basis.
- Licensees will need to provide analyses to justify the crediting of self-diagnostics for TS surveillance requirement reduction or elimination.
- Licensees will need to still perform periodic functional tests of the self-diagnostics features to satisfy BTP 7-17 guidance.
- Licensees will need to provide a description of plant administrative controls that will provide assurance (defense-in-depth) that faults are captured and investigated.
  - This may include items such as operator rounds, and system engineer monthly reports that evaluate and document the health, errors, and faults of the safety system.

Accident Analysis and Defense-in-Depth and Diversity

The following information needs to be clearly identified in the LAR:

- Chapter 15 events that credit functions performed by the modified system
- Potential changes to Design Basis Accident Analyses
- Acceptability of the new response times and methods used (including calculations)
- Approach for addressing potential CCF, such as the D3 strategy and D3 coping analysis

Human Factors Engineering

- NUREG-0700, Rev. 3, "Human-System Interface Design Review Guidelines (ADAMS Accession ML20162A214), provides detailed acceptance criteria for HFE design attributes; both are referenced in SRP Chapter 18 and NUREG-0711 mentioned in the ISG.
- NUREG-0700, Rev. 3 references the following IEEE Standards:
  - IEEE Std. 497-2002, "IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear power Generating Stations"
  - IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems in Nuclear Power Generating Stations"
  - IEEE Std. 603-1998, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations"

Use of Risk Insights

- The staff implemented the Integrated Review Team (IRT) approach outlined in LIC-206, “Integrated Risk-Informed Decision-Making for Licensing Reviews.”
- The staff is utilizing risk insights to the extent practical to aid current and future DI&C reviews.
- NRR’s Division of Risk Assessment (DRA) supports the IRTs, as necessary, with qualitative risk insights to inform the scope and depth of the review.
- This activity is at an early stage for DI&C reviews; the extent of its applicability will be plant-specific, dependent on the proposed change, and availability of risk insights.

Open Discussion

Acronyms

ADAMS – Agencywide Documents Access and Management System
ARP – Alternate Review Process
ASME – American Society of Mechanical Engineers
BTP – Branch Technical Position
CCF – common cause failure
D3 – Defense-in-Depth and Diversity
DI&C – Digital Instrumentation and Controls
DRA – Division of Risk Assessment
FAT – Factory Acceptance Test
FMEA – Failure Modes and Effects Analysis
GDC – General Design Criteria
HW – Hardware
HFE – Human Factors Engineering

Acronyms

HSSSR – high safety-significant safety-related
IEEE – Institute of Electrical and Electronics Engineers
I&C – Instrumentation and Controls
IP – Inspection Procedure
IRT – Integrated Review Team
ISG – Interim Staff Guidance
LAR – License Amendment Request
MP – Modernization Plan
NEI – Nuclear Energy Institute
NQA – Nuclear Quality Assurance
NRC – Nuclear Regulatory Commission
OpE – operational experience
QA – Quality Assurance

Acronyms

RAI – Requests for Additional Information
RIS – Regulatory Issue Summary
RG – Regulatory Guide
SAT – Site Acceptance Test
SDOE – Secure Development and Operational Environment
SPM – Software Program Manual
SW – Software
SWCCF – software common cause failure
TR – Topical Report
TS – Technical Specifications
VOP – Vendor Oversight Plan
V&V – Verification and Validation