NRC Workshop on Digital Instrumentation and Controls (DI&C)

Licensing and Inspection Lessons Learned from Recent DI&C Modernization

March 23, 2022

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

RECENT DIGITAL I&C LICENSING LESSONS LEARNED

- Intent of the Alternate Review Process
- Deviations from the ISG-06 Guidance
- Licensing and System Development Schedules Overlap
- Information Submittals and Licensing Audits
- Vendor Oversight Plan and Summary
- Integrated Licensing Reviews
- Licensing Success Path

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

Current DI&C Licensing Activities

- **Waterford 3**
  - Core Protection Calculator System
  - LAR submitted in July 2020
  - LA issued in August 2021
  - FAT & SAT inspections completed
- **Turkey Point Units 3 & 4**
  - Reactor Protection System, Engineered Safety Feature Actuation System, Nuclear Instrumentation System
  - Multiple pre-submittal meetings since 2020
  - LAR submittal expected in 2nd Quarter of 2022
- **Limerick**
  - Reactor Protection System, Nuclear Steam Supply Shutoff System, Emergency Core Cooling System
  - Multiple pre-submittal meetings since 2020
  - LAR submittal expected in 3rd Quarter 2022
  - D3 LAR submitted in February 2022

Intent of the Alternate Review Process

- To allow for issuance of a license amendment (LA) prior to completion of the system Implementation and Test life cycles phases.

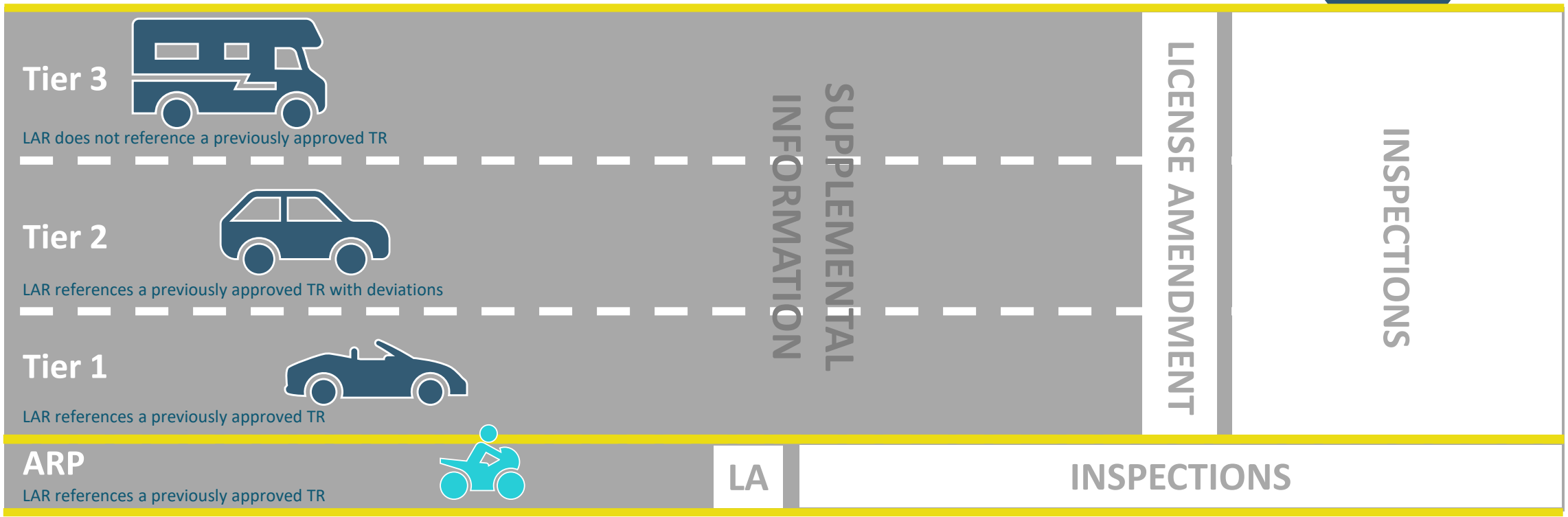
- Focus is on:
  - the system design (to demonstrate it meets regulatory requirements),
  - the development process (to demonstrate it is of sufficiently high quality),
  - a summary of the licensee's vendor oversight plan (VOP),
  - and additional commitments to perform vendor oversight and implement the remaining development phases under the licensee's quality assurance program after the LA is issued.

- Final system implementation and testing (e.g., FAT) is subject to verification through NRC inspection processes, in addition to the site inspections.

"Digital Instrumentation and Controls, DI&C-ISG-06, Licensing Process," Revision 2 (ADAMS Accession No. ML18269A259)

Intent of the Alternate Review Process

ISG-06 DI&C Licensing Highway



The ARP was developed to address an industry need to expedite the DI&C licensing review process

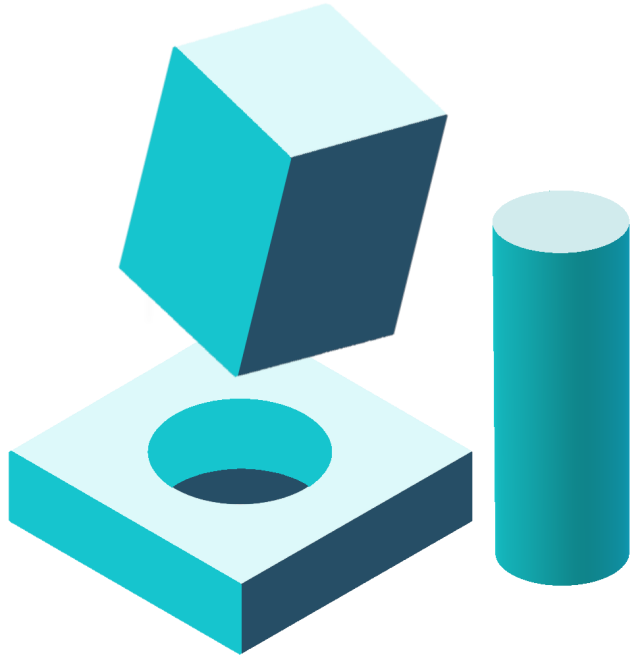
U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Intent of the Alternate Review Process

- To quickly support upcoming DI&C modifications
  - All information provided in a single high-quality submittal
  - i.e., no RAIs or supplemental information
- Vision of first applications would be for DI&C upgrades similar to past modifications:
  - One for one digital replacements of safety systems (e.g., Oconee, Diablo Canyon, Hope Creek)
  - Major changes to the control room with significant HFE needs were not identified
  - Crediting self-diagnostics to eliminate SRs was not considered
- Use of the ARP for more complex modifications would be considered after gathering lessons learned

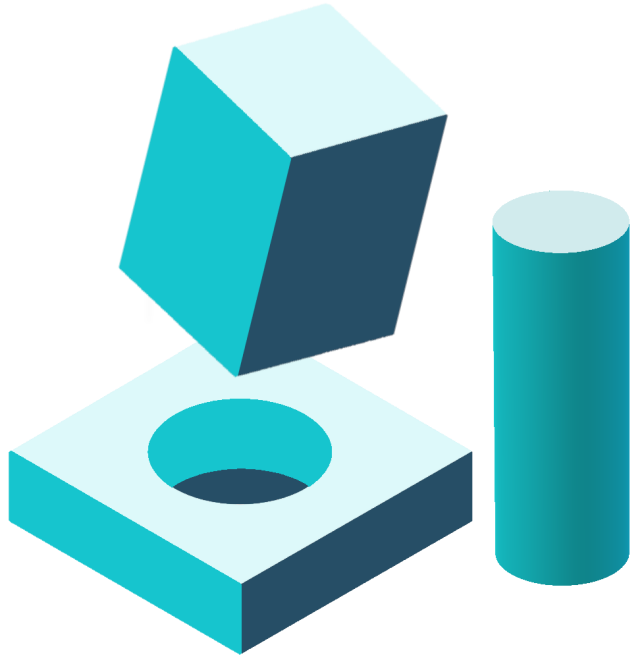
Deviations from the ISG-06 Guidance

- Experience has shown that actual applications tend to deviate from the ISG-06 guidance (e.g., LAR contents, supplemental information, licensing and life cycle development timelines).
- Minor or modest deviations are not necessarily impediments to the review, if addressed early in pre-application meetings.
- A key challenge is attempting to apply a specific ISG-06 process when the scope of the amendment and timing of design information no longer aligns.



Deviations from the ISG-06 Guidance

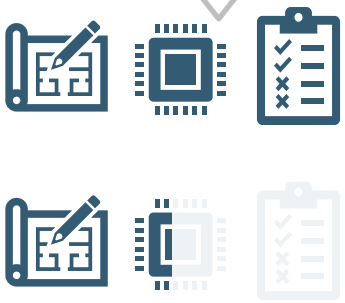
- Licensing review scope/schedule, and staff and licensee expectations need to adjust in order to address these deviations:
  - Potential for additional information to be audited or docketed
  - Changes to licensing review and LA issuance schedules
  - Changes to licensing audit and inspection scopes and schedules
- Staff and licensees need to be flexible to allow for consideration of other characteristics or aspects of the application, such as:
  - the level of detail in the VOP
  - the use of regulatory commitments
  - the safety significance of the modification



Licensing and System Development Schedules Overlap

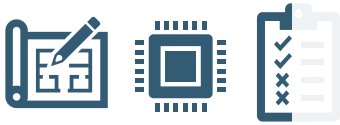
ISG-06

- The Tier 1 Review Process licensing review schedule overlaps with the system design, implementation and testing life cycle phases.
- The ARP compressed the licensing review schedule to overlap with the system design and early implementation life cycle phases.

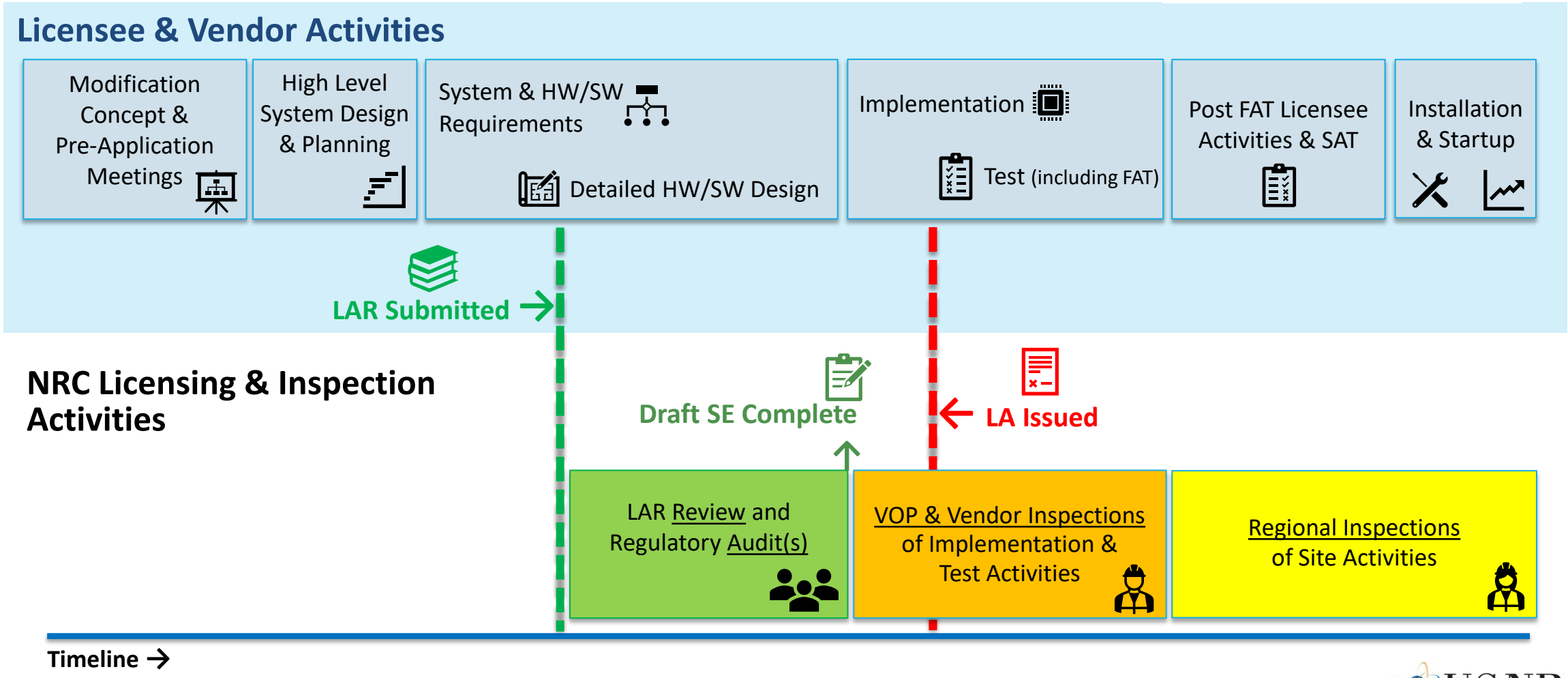


Deviations from ISG-06

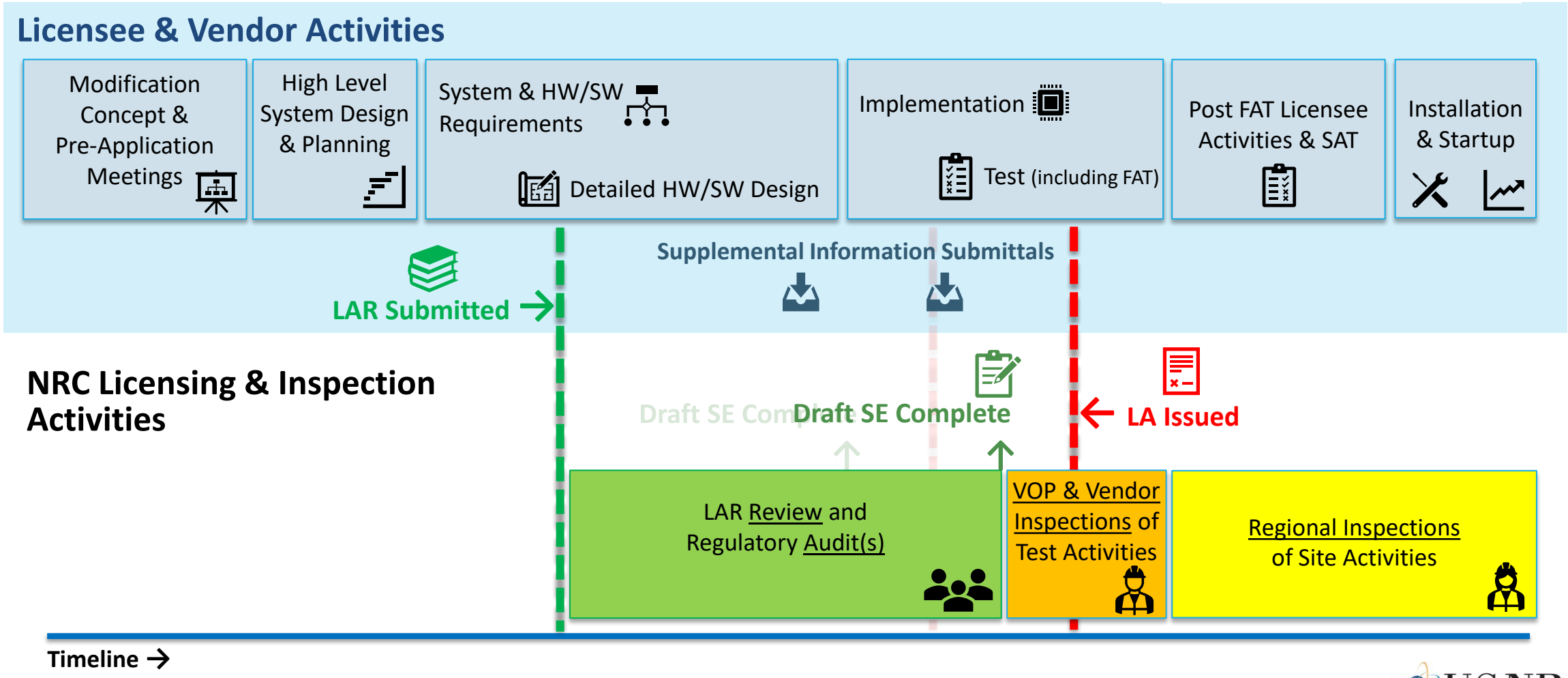
- The actual system development schedule appears to have also been compressed.
  - Implementation is occurring in parallel with the latter half of the requested licensing review.
- Supplemental information submittals (e.g., EQ, SR eliminations) may impact the review schedule:
  - EQ testing is often deferred to later stages of the project and EQSRs are provided as late supplements to the LAR.
- This has resulted in licensee development and NRC review schedules that are effectively neither the ARP or Tier 1 Review Process as envisioned in ISG-06.



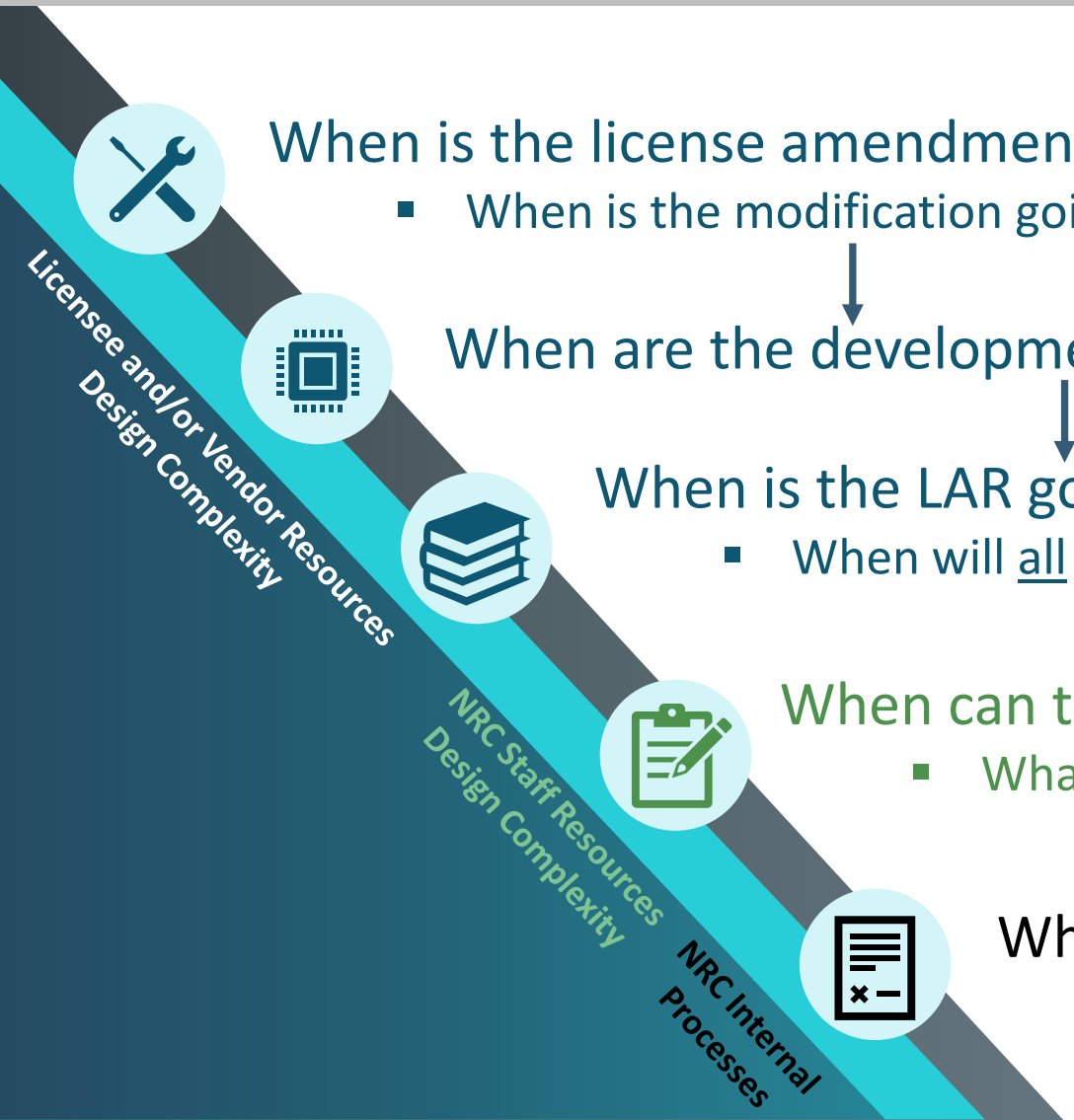
Licensing and System Development Schedules Overlap – Model Case ARP



Licensing and System Development Schedules Overlap – Actual



Licensing and System Development Schedules Overlap – Factors



When is the license amendment (LA) needed?

- When is the modification going to be installed?

When are the development life cycle phases started and completed?

When is the LAR going to be submitted?

- When will all the information be submitted?

When can the NRC staff complete the draft SE?

- What is the time needed to perform the licensing review?

When can the LA be issued?

- What are the post-draft SE activities?

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

Information Submittals

ISG-06 Enclosure B

		Tier			Plant-Specific Information Submitted with License Amendment Request (Phase 1 for Tier 1, Tier 2, and Tier 3)
	AR	1	2	3	
1.1	X				**(Summary of) Application Software Planning and Processes** (see D.4)
1.2	X				**(Summary of) Vendor Oversight Plan** (see C.2.2)
1.3	X	X	X		**Approved Topical Report Safety Evaluation** (see D.5)
1.4	X	X	X	X	**System Description** (see D.1)
1.5	X	X	X	X	**System Architecture** (see D.2)
1.6	X	X	X	X	**(Summary of) Hardware Equipment Qualification** (see D.3)
1.7	X	X	X	X	**(Unified Compliance/Conformance Matrix for) IEEE Stds 603-1991 and 7-4.3.2-2003** (see D.6)
1.8	X	X	X	X	**(Changes to) Technical Specifications** (see D.7)
1.9	X	X	X	X	**Setpoint Methodology and Calculations** (see D.7)
1.10	X	X	X	X	**Secure Development and Operational Environment** (see D.8)
1.11		X	X	X	**Software Requirements Specification** (see D.9.1)
1.12		X	X	X	**Software Design Specification** (see D.9.2)
1.13		X	X	X	**Design Analysis Reports for Platform Changes** (see D.9.3)
1.14		X	X	X	**System Response Time Analysis Report** (see D.9.7)
1.15			X	X	**Design Report on Computer Integrity, Test and Calibration, and Fault Detection** (see D.9.7)
1.16				X	**Commercial-Grade Dedication Plan** (see D.9.9)
1.17				X	**Quality Assurance Plan for Hardware** (see D.9.10)
1.18				X	**(Summary of) Hardware Development Process** (see D.9.10)

Information Submittals

ISG-06 Enclosure B

- The ISG-06 Enclosure B tables identify the typical information to be submitted depending on the applicable review process.
  - This information is based on the life cycle information and outputs subject to staff review or audit, as well as on any application-specific aspects of the LAR.
  - Note that the tables assume a model case application and do not account for deviations from the ISG-06 guidance.
- Different information from that identified in Enclosure B may need to be provided, depending on the scope and complexity of the system modification and other associated requests.
- The information submitted for an actual application and the timing of submittal may resemble something in between the ARP and Tier 1 columns.

Information Submittals

Surveillance Requirements Elimination

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

- 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.

Licensing Audits

- Virtual audits of undocketed material and “living documents” (e.g., the VOP) have proven to be very effective.
- Providing questions (e.g., open items) to the licensee in advance of virtual audit calls improved the effective use of the audit time.
- In-person audits of the vendor should be performed during the licensing review to familiarize the technical reviewers and inspectors with the system and interfaces.
- The scope of the information to be audited should include those vendor and licensee documents that are developed during the licensing review in order to support the draft SE.

Integrated Licensing Reviews

- A DI&C modification encompasses various technical review disciplines, including:
  - Instrumentation and Controls
  - Human Factors Engineering
  - Reactor Systems
  - Cyber Security
  - Electrical Engineering
  - Technical Specifications
  - Vendor Inspections
- Depending on the application, the staff responsible for these disciplines may be involved in the licensing review and/or inspections.
- The responsible staff reviews the information necessary to make a safety determination using the review criteria found in the SRP for all relevant review areas.
- The guidance in ISG-06 is primarily focused on the DI&C portion of the review.

Integrated Licensing Reviews

Diversity and Defense-in-Depth

Overview

- Depending on the application, I&C, Reactor Systems and HFE staff may be involved in the diversity and defense-in-depth (D3) portion of the review.
- A systematic approach used to analyze a proposed DI&C system for common cause failures (CCFs) that can occur concurrently within a redundant design.
- Per Branch Technical Position (BTP) 7-19, CCFs can be addressed through the following ways:
  - Eliminate the potential for CCFs from further consideration
  - Use of diverse means to mitigate CCFs
  - Consequences of a CCF may be acceptable
- Reactor Systems reviews are focused on the reanalysis of the SAR Safety Analysis (Chapter 15) events with assumed CCFs.

Integrated Licensing Reviews

Diversity and Defense-in-Depth

Reactor Systems

For **Reactor Systems** reviews, the following items, at a minimum, are expected to be includes in the D3 Analysis:

- Identification and selection of Transients and Accidents to be considered in combination with a CCF
  - Addresses all Chapter 15 events
    - Including both anticipated operational occurrences and postulated accidents
  - Other credible events, such as those initiated by spurious actuation, that are not already analyzed in Chapter 15
- Description of what systems are lost due to CCF (i.e., reactor trip system, engineered safety features actuation system, etc.)
- Identification and description of credited diverse equipment
  - Both existing and new systems if applicable
  - May be non-safety grade if it is of sufficient quality
- Identification and description of credited operator actions (reviewed by HFE as appropriate)
- Evaluation and/or analysis of each event

Integrated Licensing Reviews

Diversity and Defense-in-Depth

Event Categorization and Analysis

Events may be categorized in determining what level of detail is required to be provided. Example categories include:

- Events where the CCF has no adverse effect
  - The assumed failed system (i.e., reactor trip) is not credited in the analysis
    - Fuel handling accident, single dropped PWR control rod
  - Other than identification, these events require no analysis
- Events terminated by a diverse system
  - Diverse system may include existing systems, manual operator actions, or new diverse systems
  - Description of the event should be provided including comparison of diverse system actuation timing versus base times
  - New analysis may need to be performed
    - if diverse system timing is significantly different than base time (i.e., Chapter 15 event had reactor scram at ~5 seconds while operator action is credited to scram at 10 minutes)
    - little to no margin to acceptance criteria

Integrated Licensing Reviews

Diversity and Defense-in-Depth

Event Categorization and Analysis (continued)

Events may be categorized in determining what level of detail is required to be provided
Example categories include:

- Events bounded by another event
  - Inadvertent SG relieve valve opening may be bounded by steam line break
  - Other than identification, these events require no analysis

- Events that analysis is required to demonstrate acceptance criteria are met
  - Events that were not eliminated by other categories
  - May be analyzed using either best estimate methods (i.e., using realistic assumptions to analyze the plant's response to DBEs) or conservative methods (i.e., design-basis analysis)
  - Analysis must demonstrate events meet acceptance criteria as defined in Section B.3.3 of BTP 7-19

Integrated Licensing Reviews

Diversity and Defense-in-Depth

Reactor Systems Review Findings

- D3 analysis considered all relevant events

- Events were categorized correctly
  - Events where CCF has no adverse effect
  - Events terminated by a diverse system
  - Events needing to be analyzed

- Verified that the D3 analysis demonstrated that consequences of identified CCF remain acceptable
  - Should the CCF occur, the facility will remain within the appropriate acceptance criteria for the limiting events applicable to the proposed DI&C system or component

Integrated Licensing Reviews

Diversity and Defense-in-Depth

Precedents

Examples	Methods Credited	Summary Description
Oconee (Reactor Protection System & Emergency Safety Features Actuation System)	**Existing Equipment** **Manual Operator Action** **Diverse Actuation System** **Consequence Calculation**	Anticipated Transient Without Scram (ATWS) equipment and MOA credited for most safety functions. Diverse Manual controls added to support MOAs Two automatic DAS added for High Pressure Injection and Low Pressure Injection. Use of analog was design choice by licensee.
NuScale & Diablo Canyon (Reactor Protection System & Emergency Safety Features Actuation System) **Wolf Creek** (Main Steam Isolation)	**Internal Diversity** **Design Measures** **Existing Equipment**	For NuScale, internal diversity was credited, where the Field Programmable Gate Arrays (FPGAs) used for two divisions were diverse from the FPGA in the other two divisions. For Diablo Canyon, existing diverse systems, including ATWS were credited. Design measures such as automatic self-testing, self-calibration and surveillance testing were also credited. For Wolf Creek, internal diversity among the different channels of the MSFIS were credited, where the software algorithms used to program two channels were different from the ones used for the other two channels.
Shearon Harris (Adoption of Westinghouse SSPS Topical Report)	**Simple Design**	Augmented approach using very high number of possible states were tested, and an analysis demonstrated that the remaining untested possible states were functionally irrelevant.
Hope Creek & Browns Ferry (Power Range Neutron Monitoring System)	**Manual Operator Action**	Existing MOAs Credited
AP1000 & APR1400 (Integrated Control and Protection System)	**Diverse Actuation System** **Manual Operator Action** **Consequence Calculation**	AP1000 – FPGA-based DAS with hardwired system-level manual controls on a separate panel. The MOA capability within the DAS is credited for a few safety functions such as initiating the automatic depressurizations system. APR1400 – FGPA-based Automatic Diverse Protection System that initiates three automatic functions. One manual reactor trip function is also credited. A FPGA-based diverse indication system is included to display plant parameters during a CCF of the safety-related displays. FPGA-based.

Integrated Licensing Reviews

Human Factors Engineering

- As discussed in ISG-06, HFE review guidance is an area not within the scope of ISG-06.
- Guidance on NRC Human Factors Engineering (HFE) technical reviews is contained primarily in NUREG-0711, Rev.3, "Human Factors Engineering Program Review Model" (ADAMS Accession No. ML12324A013).
- Industry is proposing more significant control room modifications than were considered when ISG-06 was revised with the ARP.
- NRC staff have identified possible scheduling challenges with regards to the review of integrated system validation (ISV) testing and development timelines proposed by applicants.
- NRC staff are considering possible alternatives to having completed ISV test results available prior to issuance of a licensing amendment:
  - Early-stage results from a *multi-stage validation* (MSV) test program
  - *Alternative testbeds* for the completion of ISV testing
- *This topic will be discussed further later during this workshop.*

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

Integrated Licensing Reviews
SDOE and Cyber Security Considerations

- IEEE Std. 603-1991, Clause 5.9 “Control of Access” is the basis for the review of the secure development and operational environment (SDOE).
- Section D.8 of ISG-06 discusses SDOE reviews and refers to the guidance in RG 1.152, Rev. 3.
- ISG-06 provides guidance to the Office of Nuclear Reactor Regulation (NRR) staff to coordinate with the Office of Nuclear Security and Incident Response (NSIR) staff on matters related to cyber security.
- The licensing review of a DI&C modification **does not** include a cyber security review (compliance with 10 CFR 73.54). However, the DI&C modifications are subject to NRC inspections.
- The Regions, with NSIR support, perform cyber security inspections of the DI&C modification.
- NRR, NSIR and Regional staff work together to ensure adequate coverage and understanding of the SDOE and cyber security aspects of the modification:
  - Security requirements for technical security controls to be implemented by the vendor
  - Supply chain requirements of the cyber security plan
  - Security impact analysis of the modification (NEI 08-09 E.10.5, RG 5.71 C.10.5)

Integrated Licensing Reviews

SDOE and Cyber Security Considerations

The combination of SDOE and the cyber security programmatic provisions address the secure design, development, and operation of digital safety systems.

	SDOE	Cyber Security
Focus	Safety Quality and integrity of the safety system. (non-malicious act)	Security Prevention of radiological sabotage. (malicious act)
Regulation	10 CFR 50, "Domestic Licensing of Production and Utilization Facilities"	10 CFR 73.54, "Protection of Digital Computer and Communication Systems and Networks"
Regulatory Guide (RG)	RG 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants"	RG 5.71, "Cyber Security Programs for Nuclear Facilities."

Vendor Oversight Plan (VOP) and Summary

- The staff recognizes the need for guidance for developing the VOP and VOP Summary.
- The staff plans to develop this guidance after the licensing actions for the Turkey Point and Limerick applications.
- For the Waterford 3 LAR review, the staff evaluated whether the licensee's oversight activities, as described in the VOP Summary, meet the following criteria to Appendix B of 10 CFR Part 50:
  - Criterion III, "Design Control"
  - Criterion V, "Instructions, Procedures, and Drawings"
  - Criterion VII, "Control of Purchased Material, Equipment, and Services"
  - Criterion XVI, "Corrective Action"

Vendor Oversight Plan (VOP) and Summary

- 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 and VOP Summary should address how the licensees' 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.

Vendor Oversight Plan (VOP) and Summary

- If the full VOP is not a lengthy document, it may be beneficial for the licensee and the staff if it is submitted with the LAR, instead of the VOP Summary.
- Engineering procedures that are used to implement the VOP should be described, including how they fit into the overall site QA program.
- Critical characteristics that will be verified by VOP activities should reflect system and architecture design specific to the application reviewed.
- Identification of all documents that will be reviewed and approved as an engineering design document should be identified.
- Identification of all lifecycle activities, including V&V activities should be described.
- The VOP and VOP Summary should describe the VOP change controls.

Vendor Oversight Plan (VOP) and Summary

- VOP audits during the licensing review serve several purposes:
  - The review the full VOP (in the case when only the VOP Summary was docketed)
  - To verify how the licensee is implementing the VOP
  - To determine if there is reasonable assurance that the licensee will implement the VOP after issuance of the LA

- For Waterford 3, VOP audits were conducted essentially throughout the LAR review timeframe:
  - Focus was on VOP activities described in the VOP Summary plus details of implementation provided in the VOP to ensure consistency.
  - The pandemic required these activities to be conducted virtually.

- The VOP audit should occur after the vendor audit (or vendor inspection) to be able to focus on specific items that will be audited.

Vendor Oversight Plan (VOP) and Summary

- The licensee's implementation of VOP activities may not occur sequentially in accordance with the development lifecycle.
  - For example, oversight activities for the implementation phase may take place after observance of the FAT.

- Licensee's VOP audit reports may lag the actual observed vendor activity by over a month.
  - This creates a challenge to the staff reviewing the licensee's VOP audit reports, as they are seeing issues identified months in the past and may be not aware of their resolution in a timely manner.

- If the licensee's VOP audit report will be issued after the completion of the draft SE, the staff may need to consider if an NRC audit of the vendor is more practical to support the licensing review.

Licensing Success Path

- If an application follows the Tiered or ARP guidance according to the ISG, this maximizes the regulatory certainty and scheduler certainty.
- If not, then the staff and the licensee need to consider:
  - the licensing review schedule – what is a reasonable review time (based on the complexity of the modification and information availability) and does the schedule support the installation date?
  - information needs – it could be a mix of ARP and Tier 1 information from Enclosure B (depending on the modification and the review schedule)
  - information availability – what is submitted and when?
- This approach could be more efficient and provide advantages to the licensee in terms of flexibility to address licensing process deviations.

Licensing Success Path

- Staff and licensees need to be flexible to allow for consideration of other characteristics or aspects of the application, such as: the level of detail in the VOP, the use of regulatory commitments, and the safety significance of the modification.

- This may:
  - likely still result in a LA issuance date being earlier than that of the Tier 1 process
  - decrease some inspection activities that could be captured instead through traditional licensing audit processes

- If the necessary information can be provided in a timely manner to support the licensing review, and the license amendment is issued in time to support the planned installation date, then that's a ***SUCCESS!***

Licensing Success Path

OPEN DISCUSSION

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

Acronyms

ADAMS – Agencywide Documents Access and Management System
ARP – Alternate Review Process
BTP – Branch Technical Position
CCF – common cause failure
D3 – Defense-in-Depth and Diversity
DI&C – Digital Instrumentation and Controls
FAT – Factory Acceptance Test
FMEA – Failure Modes and Effects Analysis
GDC – General Design Criteria
HW – Hardware
HFE – Human Factors Engineering
IEEE – Institute of Electrical and Electronics Engineers
I&C – Instrumentation and Controls
IP – Inspection Procedure
ISG – Interim Staff Guidance
ISV – Integrated System Validation
LAR – License Amendment Request
MSV – Multi-Stage Validation
NEI – Nuclear Energy Institute
NQA – Nuclear Quality Assurance
NRC – Nuclear Regulatory Commission
NRR – Office of Nuclear Reactor Regulation
NSIR – Office of Nuclear Security and Incident Response
OpE – operational experience
QA – Quality Assurance
RAI – Requests for Additional Information
RG – Regulatory Guide
SAT – Site Acceptance Test
SDOE – Secure Development and Operational Environment
SPM – Software Program Manual
SW – Software
TR – Topical Report
TS – Technical Specifications
VOP – Vendor Oversight Plan
V&V – Verification and Validation