Licensing Modifications to Digital Safety Systems (Lessons Learned and Moving Forward)

Abstract

The purpose of this information is to explore lessons learned during recent safety evaluations of digital safety system topical reports and system modifications using the licensing processes outlined within Interim Staff Guidance 06 (ISG-06) "Task Working Group #6: Licensing Process," and facilitate discussions on incorporating improvements to the licensing of digital instrumentation and control (I&C) systems.

From 2006 to 2011 the NRC worked with the industry to develop guidance including ISG-06 to facilitate improvements to the licensing process for digital I&C systems. The Diablo Canyon Process Protection System upgrade was then selected to become the pilot project for the use of ISG-06.

The increased use of modern technologies in I&C safety system designs has posed challenges to both licensees and the NRC review staff. The enhanced capabilities and features available to these systems have introduced new levels of complexity and uncertainty, which are challenging to address using the current licensing approach. Approaches to evaluate digital I&C system designs are discussed including the potential of pre-Factory Acceptance Test (FAT) license amendment approvals and simplifying the regulatory infrastructure by eliminating redundant guidance currently found in multiple sources. The paper includes examples of potential improvements that are not explicitly included in current licensing process.

1 INTRODUCTION: DIGITAL INSTRUMENTATION AND CONTROLS (I&C) LICENSING

The approach used by the NRC staff to review and approve a License Amendment Request (LAR) for digital I&C safety systems involves several steps. The NRC review includes the life cycle design process for a digital safety system to support reaching the determination of reasonable assurance of safety. The technical requirements associated with a high quality design process are enumerated in several IEEE standards which are endorsed by the NRC in regulatory guides. The licensing criteria associated with the review of digital I&C safety systems are documented in Chapter 7 of the Standard Review Plan (NUREG-0800), which in turn refers to a series of regulatory guides that provide criteria for various aspects of digital safety systems. The licensing process can be summarized by addressing the following four questions:

What will be done to ensure the necessary degree of safety is achieved?

How will this be done?

Will it be done correctly?

Is the product good enough or is it safe?

The information and processes used by the NRC staff to answer these questions and provide a reasonable assurance safety determination proceeds along the following:

First: The NRC staff performs an assessment of what the vendor or licensee is planning to do in order to make a determination that planning activities will increase the likelihood of achieving a high quality design. The assessments are intended to provide information needed to answer the preceding "what, and how" questions. The early assessments focus on reviewing the various plans for the digital system development activities. For this reason, the current process expects submittal of planning documentation at the time of: (1) vendor submittal of a topical report, or (2) LAR submittal.

Second: The NRC staff reviews the information that describes "What will be done" or, in other words, the programs and procedures that will be used to implement the plans. These programs and procedures are often developed and refined as the work is performed, and are often unavailable until a later stage of the software development life cycle. For this reason, the staff does not require these procedures to be submitted at the time of the initial LAR submittal. However, for those activities which will occur fairly early in the design life cycle, the current process expects preliminary procedures to be available for audit. The exact timing of when these procedures should be made available can vary depending on how far activities have proceeded along the development life cycle.

Third: The NRC staff audits the implementation activities to verify they were accomplished pursuant to the established plans and procedures. This activity is intended to allow auditors to access whether the system development is correctly being performed. These are sometimes called thread audits. This portion of the evaluation is usually performed during on-site audits, where NRC staff has the opportunity to observe activities in-progress and to interview personnel performing development and verification and validation (V&V) activities.

Fourth: The NRC staff reviews the results of the completed activities to determine the degree to which project goals were achieved. This activity is intended to answer the final question; "Is the product good enough?" or "Is it safe?" This is done by reviewing the documentation of the final results, such as test reports, V&V reports, corrective action reports, etc. These documents form a substantial portion of the basis for the NRC staff's conclusion that the license amendment can be issued.

2 ISG-06 PROCESS BACKGROUND AND DISCUSSION

ISG-06 was developed to provide guidance for the NRC staff's review of license amendments for installation of digital I&C equipment in accordance with existing licensing processes. This ISG also identifies the information the NRC staff should review for digital I&C equipment and times that the information should be provided or made available to the NRC. This information is intended to allow technical reviewers to assess digital I&C upgrade applications to ensure they sufficiently address the areas within the I&C review scope. These review areas correspond to Chapter 7, of NUREG-0800.

Key objectives considered during the development of ISG-06 were:

- Establish a graded approach to performing Digital I&C safety evaluations.
  (The Three-Tier Review Concept: 1, 2, and 3)
- Provide clear guidance to identify submittal requirements for supporting documentation/information.
  (Annex B)
- Provide an evaluation process that can be performed in parallel with the system / software development activities for the systems.
  (Phases of review)
- Facilitate the licensing activity by consolidating guidance from multiple sources into a single reference for ease-of-use.

The following sections explain how each of these objectives was addressed within ISG-06 and provide a characterization of the degree to which each has been achieved and are effective based on experience with the guide.

2.1 THE THREE-TIERED REVIEW CONCEPT

The level of effort, information required, and time needed to review and approve a digital safety system depends in part on whether the system design implements a previously approved digital platform or equipment. To clarify this, ISG-06 adopted three tiers of possible review for licensees to consider when submitting a digital safety system licensing application.

Tier 1: Applies a previously approved platform with no deviations from its topical report, review to focus on plant specific aspects, least review effort expected.

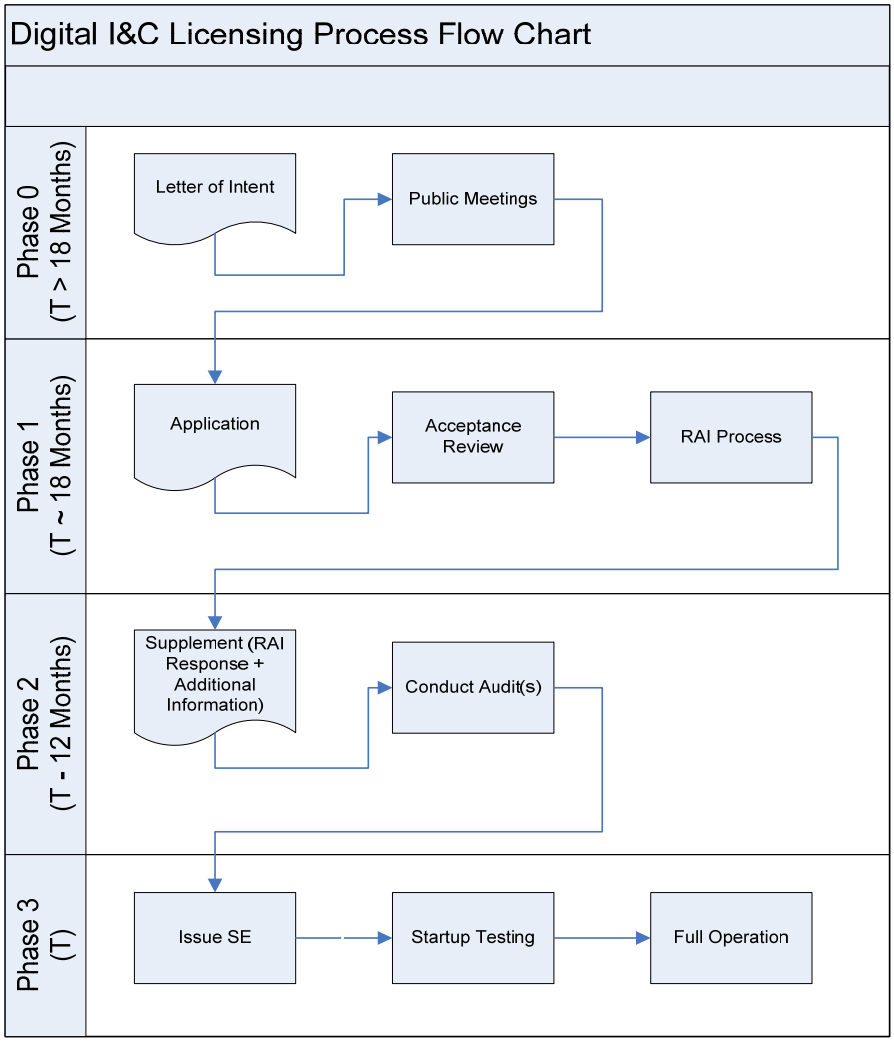
Tier 2: Applies a previously approved platform with deviations, moderate review effort expected.

Tier 3: Applies a new (not previously approved) platform, more extensive review effort expected including a thorough review of technical areas.

Since the publication of ISG-06 in 2011, the NRC has performed reviews of digital I&C systems at all three tiers. Although the tier-based concept reflects some insight into the level of effort required to complete these safety evaluations, there are other factors such as scope of the modification, complexity of functions performed by the I&C system and completeness of design at the time of review, which could be used to further refine the level of effort needed to complete a safety evaluation.

2.2 THE PHASED SUBMITTAL CONCEPT

The figure that follows is a block diagram of the digital safety system licensing process as described within ISG-06. It is a simplified version of Enclosure C to ISG-06 that also shows the lead time of activities for an 18-month evaluation from LAR submittal. The lead time represents time prior to an anticipated safety evaluation issuance (requested approval). For example ‘T > 18 months’ means ‘greater than 18 months from requested approval date.’ The figure depicts the ISG-06 phased submittal concept, which can be implemented in parallel with a digital safety system’s development.



Enclosure C Digital I&C Licensing Process Flow Chart

The phases are defined in ISG-06 as follows:

Phase 0 Pre-application phase - During this phase the staff will gain an understanding of the overall design concepts. Key technical safety review topics would be discussed such as diversity and defense-in-depth, significant variances from current guidance, complexity of the system(s), software quality assurance programs, and other unique or complex topics associated with the proposed design. These meetings and summaries are critical to prepae the licensee and NRC staff for an efficient licensing action.

The intent of this approach is to facilitate a means by which licensees can effectively communicate key system design and licensing attributes to the NRC staff. The process also provides licensees with staff feedback on the regulatory acceptability of the safety system during the process as early as practical and well in advance of a license application submittal.

Phase 1 Initial Application Phase - This phase begins when the license amendment request is submitted to the NRC and includes the acceptance review process (LIC-109). An Initial Review of Application is performed and Requests for Additional Information are sent to the applicant.

Phase 2 Continued Review and Audit - Following response to the Phase 1 RAIs but at least 12 months prior to the requested approval date, the licensee is expected to submit a supplement containing sufficient information to address aspects of the review areas not submitted in the initial LAR or subsequent RAIs.

Phase 3 Implementation and Inspection - This phase begins with the issuance of the license amendment and safety evaluation and concludes the NRR activities. Phase 3 also includes the licensee's implementation of the amendment and NRC Regional inspection activities.

ISG-06 defines a consistent licensing process for digital safety systems by:

- identifying the regulatory requirements, guidance, and acceptance criteria, that should be addressed in a license amendment request;
- defining the level of detail and timing for the information and documentation to be provided in a license amendment request; and,
- defining the protocols for development of a license application and details of how the NRC staff review will be conducted.

This phased approach accounts for the reality that some information needed for the regulatory decision may not be available when the license amendment request is submitted.

3 ISG-06 PILOT PROJECT BACKGROUND

In October of 2011, Diablo Canyon submitted a license amendment request to replace the Eagle 21 process protection system with a new system composed of two subsystems. One of these subsystems is based on the Tricon V10 programmable logic controller (PLC) platform and the other is based on the Westinghouse Advanced Logic Systems (ALS) FPGA platform.

ISG-06 had recently been developed, but many of its processes had not been used. Therefore, PG&E applied for this project to be classified as a pilot for the use of ISG-06 licensing process. The NRC approved this request and granted a fee waiver in accordance with 10 CFR 170.11(b). The NRC conducted its safety evaluation of the proposed PPS system using the ISG-06 licensing processes to approve the digital modification and issue the license amendment.

In spite the best efforts to make process improvements via ISG-06, digital I&C safety system evaluations continue to be challenging. The concepts introduced by ISG-06 were intended to streamline and clarify the digital I&C review processes. In some ways these objectives were achieved and the new ISG-06 process provided benefits. However, in other ways, some challenges were not sufficiently addressed. The licensing experience using ISG-06 provides an opportunity to reevaluate lingering process-related challenges.

The Diablo Canyon review provided additional insights into the ISG-06 safety evaluation process and has identified several opportunities for improvement. The following subsections discuss observations from ISG-06's use and present ideas on how digital I&C licensing processes could be further improved.

3.1 CONCEPTS THAT HAVE WORKED

ISG-06 Matrix – This is a spreadsheet that is based on the document list provided in ISG-06 Enclosure B. Early on, the Licensee developed this matrix as a convenient way to map ISG-06 required information to vendor and licensee documents that would demonstrate compliance with pertinent review criteria.

The NRC staff found this matrix to be very useful during the acceptance review and later when evaluating phase II document submittals. However, subsequent changes were not made to the matrix after completing the acceptance review to maintain the matrix.

When the NRC staff plans and performs evaluation activities, the NRC staff continues to think about of how to complete the safety evaluation (SE) report (the NRC staff's deliverable product). The NRC staff found that using the SE report template (Enclosure D) as a guide for evaluation activities becomes more useful than the matrix once evaluation activities begin. Use of the SE report template also provided greater confidence that all of the required areas would be covered in the SE report. Although the NRC staff saw no need to revise the matrix, the NRC staff did refer to the matrix to locate supporting submittal information.

Some of the documents referenced within the matrix were superseded as the project progressed. Regardless, the NRC staff could generally find required information in newer version of documents with the same identification number. Although an alternative approach could have been taken, the NRC staff saw the benefit of minimizing the number of living documents that would need to be updated and supplemented as the evaluation progressed. For this reason, the ISG-06 matrix was allowed to remain static.

Open Items List – At the beginning of the evaluation, the NRC developed an Open Items (OI) list document to track questions from the NRC staff arising from the document reviews. Each entry to the OI list includes a section for licensee response as well as an update and comments section to keep track of the OI status. The OI list also identifies OI's which require formal licensee response and these OI's were then submitted to the licensee in the form of a Request for Additional Information (RAI) Letter.

The Open Item List has been a useful tool to coordinate RAI generation and responses and facilitate periodic conference calls.

Use of SharePoint (or equivalent) sites – For various licensing activities, applicants and licensees established and controlled SharePoint sites to provide NRC staff access to their documentation. Availability of early access to documentation (e.g., versions prior to docketed submittal, audit-only) by NRC staff can help reduce the completion time of the safety evaluation. Under ISG-06, use of SharePoint sites directly supported auditing activities in Phases 2 and 3. Two benefits from the use of SharePoint sites are the reduction in travel costs and improved planning and execution of on-site audits.

Beyond audit support, SharePoint sites have been useful for identifying specific limited information for placement on the docket to expedite the safety evaluation. Additionally, SharePoint sites could be leveraged to support the living document concept, which is discussed under Section 3.4.

3.2 CONCEPTS THAT HAVE NOT WORKED

The three-tier review concept, as a means to a scalable licensing review, does not seem to have provided the degree of efficiency improvements needed for broad adoption of digital I&C by licensees. The level of resources and time to perform a digital system review depend on factors beyond the degree an application references an approved topical report and its status. Other factors that could be considered in order to further scale licensing reviews include:

- Scope of modification including complexity of the safety system design.
- Results of diversity and defense-in-depth (D3) analyses including availability of existing diverse actuation systems in the plant design.
- Planned timeframe for implementation of modification.
- Scope of a referenced licensing topical report (TR) approval as characterized by its Application Specific Action Items. Not all platform TR's are alike and some TR SE's achieve a greater degree of approval and thus require fewer resources during the application development evaluation.
- The degree individual plant-specific characteristics, such as environmental conditions, or unique design features challenge the applicability of previously approved platforms or equipment.
- Whether the modification requires changes to technical specifications.
- Whether the modification requires setpoint (analytical value) changes or includes revised instrument accuracy calculations.

Because the three-tier review concept of ISG-06 does not account for these factors, it does not characterize the level of evaluation effort required for a given digital I&C system with sufficient fidelity and predictability. As such, ISG-06 fails to provide the kind of licensing process certainty that industry seeks to facilitate its broad adoption of digital I&C by accommodating the broad range and scope of digital I&C system modifications seen in the LARs.

3.3 CONCEPTS THAT NEED MORE DEVELOPMENT

Though somewhat effective in addressing the parallel development and review processes, the phases defined in ISG-06 could be refined to address document volatility along with availability of some documents late in the project life cycle. These documentation characteristics are realities for many, if not most, projects.

3.4 NEW CONCEPTS UNDER CONSIDERATION

Living Document Concept - Some documents associated with software development are expected to be revised as system development activities progress. These are sometimes referred to as "living documents." Such documents could be classified as such. For these living documents, a decision of which version of the document should be submitted and when (i.e. what phase) the document is to be submitted could be made during the acceptance review. It is not necessary for applicants to submit multiple versions of living documents to support the safety evaluation. However, the submitted living document should be sufficient to demonstrate conformance to applicable regulatory requirements. In some cases it may also be necessary to provide accessibility to current versions of a living document for audit during a safety evaluation.

Additional document-specific guidance on document volatility could be provided within Section D of ISG-06.

Phase 2a Confirmatory Information - The initial Phase 2 document concept was design output documents that would not be available for submittal at the time of LAR could be submitted at a later time as the system design was completed. We have observed that some of these documents such as Summary Test Reports (D.4.4.2.4) are confirmatory in nature and can be distinguished from those which require detailed licensing evaluation and assessment. Such confirmatory reports would not be subjected to the early submittal requirements of other Phase 2 documents.

Conditional Letter of Regulatory Conformance - The NRC has received significant industry feedback on the timing of safety evaluations relative to project schedules. Although this was not a challenge for the Diablo Canyon pilot, the NRC staff recognize this challenge could place other development projects at risk, because significant investment may be incurred prior to achieving the regulatory approval (i.e., regulatory certainty). It has been suggested that SE's should be completed using design information and should be independent of verification and validation (V&V) activities including factory acceptance test. As suggested, factory acceptance testing could be verified by NRC staff on a confirmatory inspection basis. To date, the NRC has not adopted this suggestion based on the following:

- *Safety evaluation conclusions cannot contain conditional requirements.*
- *Experience has shown; significant design changes are often initiated as a result of test performance of the systems. Such changes have the potential to invalidate safety conclusions.*
- *In absence of system test results or conditional requirements, it may be more difficult to reach and convey the basis for a reasonable assurance safety conclusion within the SE report.*

The suggestion might be addressed if the NRC could provide some regulatory assurance earlier in the design process and before the systems are built and tested. Although there is some agreement among the NRC review staff on a conceptual basis with this kind of proposed change, current licensing processes do not permit issuance of SE's without having either sound basis for the safety conclusions or contingencies / follow-up activities upon which the SE conclusions rely.

One possible approach to address programmatic risks perceived by applicants would be to add a step to the licensing process to issue a Conditional Letter of Regulatory Conformance. Such a letter would necessarily exclude any actual safety conclusions, so it would not be a substitute for a safety evaluation or license amendment. Instead, a Conditional Letter of Regulatory Conformance could provide a statement to indicate the status of the NRC staff's review and the status of the regulatory acceptability of the proposed system prior to performance of system design implementation or testing (pre-FAT).

After issuing this letter, an applicant might have a higher degree of confidence the proposed system, as designed, meets regulatory requirements and will be accepted via the subsequent safety evaluation.

The proposal to add a Conditional Letter of Regulatory Conformance to the review process would be similar to what is currently done as part of the acceptance reviews for license amendments. Characteristics of the letter would include:

- Exclude safety conclusions or approval of license amendment;
- Provide status of safety evaluation activities at completion of design; and,
- Provide a provisional regulatory compliance statement.

It is not yet known whether applicants would obtain a sufficient level of confidence from such a letter with respect to minimizing programmatic risk commensurate with investment. If industry would not obtain a sufficient level of confidence from such a letter, then additional work would be needed to align license review and inspection activities in a way that meets all licensing requirements. Any movement of licensing activities to inspection activities would needs to be coordinated among NRC headquarters inspection staff and I&C staff, and corresponding regional staff.

Similar to a significant design change which would invalidate after an issued SE's safety conclusion, contingencies / follow-up activities would likely require an additional licensing action. Setting the exclusion of conditional requirements aside, any need for a second licensing action is an efficiency issue that relates to programmatic risk rather than a risk to public health and safety. A revised licensing process could provide licensees greater latitude in this area. A revised licensing process could provide the licensee an option, which could be identified during Phase 0 meetings and become part of the LAR.

3.5 ADDITIONAL CHALLENGES IDENTIFIED

Challenge – Improve Logical Organization: ISG-06 is not logically organized by topical review subject.

The current layout of ISG-06 is:

A – Introduction
B – Purpose
C – Digital I&C Review Process
D – Review Areas
1. System Description
2. Hardware Development Process
3. Software Architecture
4. Software Development Process
5. Environmental Equipment Qualifications
6. Diversity and Defense-In-Depth
7. Communications
8. System, Hardware, Software, and Methodology Modifications
9. IEEE 603
10. 7-4.3.2
11. Technical Specifications
12. SDOE

This current list of review areas does not facilitate efficient use. Some sections overlap with others and some sections, such as Section 9, cover many different safety review topics. Similarly, Section 9 is also not logically organized by safety review topic. One observation is that Sections 9, 10, and 12 could be eliminated because they repeat guidance provided elsewhere.

There is also overlap between the sections and topics covered in IEEE Std 603 and IEEE Std 7-4.3.2. These overlaps unnecessarily complicate the evaluation. Although it makes sense to organize by safety review topic, it is recognized that several of the relevant standards encompass many topics.

The clause-by-clause evaluation technique provided in ISG-06 to address the clauses within IEEE standards provides limited value. It is more efficient and maintainable to directly apply the relevant IEEE standard clauses, as applicable. An alternative would leave the introductory paragraphs in the IEEE Standards sections and delete the clause by clause summaries from ISG-06.

Another option would be to group sections and clauses by safety review topic and include them together in their related safety review topical area. The outline below illustrates a conceptual draft for this approach.

1. System Description
2. System Development Process (See BTP 7-14)
    a. Planning Processes (Refer to Section B.3.1 of BTP 7-14)
    b. Process Implementation (Refer to Section B.3.2 of BTP 7-14)
    c. Process Design Output (Refer to Section B.3.3 of BTP 7-14)
3. Diversity and Defense-In-Depth (Refer to BTP 7-19)
4. Communications (Refer to ISG 04 until new IEEE 7-4.3.2 is endorsed)
5. Technical Specification Evaluation
6. Equipment Environmental Qualifications
7. Secure Development and Operating Environment (SDOE)

This format should also align with the enclosure B tables, which leads into the next challenge.

Challenge – Ensure Direct Correlation between Submittals and SE: The process does not provide a direct correlation between the required information and the resultant NRC staff safety evaluations, which will be illustrated in the following example.

The following list shows the twelve planning areas covered by BTP 7-14.

BTP 7-14 Plans:

1. Management Plan
2. Development Plan
3. Quality Assurance Plan
4. Integration Plan
5. Installation Plan

6. Maintenance Plan
7. Training Plan
8. Operations Plan
9. Safety Plan
10. Verification and Validation Plan
11. Configuration Management Plan
12. Test Plan

Of these, four are omitted from the current ISG-06 enclosure B. They are: Installation, Maintenance, Training, and Operations. However, the template in ISG-06 Enclosure D includes evaluation sections for all 12 plans.

In fact, the NRC staff does not evaluate all 12 plans during the licensing review. For example, the corresponding sections of the Oconee safety evaluation do not provide an evaluation for all 12 plans. This is typical, and this practices is the apparent reason submittal of the 4 plans was omitted from ISG-06. If these sections are not needed within the SE report, then they should be deleted from ISG-06. This is only an example. A similar situation exists in other review areas, so additional efficiencies can be gained by broadly addressing this challenge.

Challenge – Improve Usability for Topical Reports: In addition to the Diablo Canyon pilot, the NRC also applied the ISG-06 process to several platform topical report reviews. The ISG-06 process is, in large part, not applicable to topical report reviews, because the ISG-06 process is written specifically to address license amendments. As such for topical reports, the NRC staff uses significantly revised topical report specific versions of the Enclosure B tables. Additionally, the information submitted for a platform topical report and its SE report layout substantially differ from the current ISG-06 enclosures.

One possible way to address this challenge would be to develop a new subset of guidance and tables applicable to platform topical report reviews. This would require creation and addition of new regulatory review guidance that is tailored to platform topical reports, a new Appendix B table, and possibly new templates for topical report reviews.

4 OPTIONS FOR MOVING ISG-06 INTO PERMANENT GUIDANCE

This section provides three path forward options to address the digital I&C licensing process guidance provided by ISG-06. Each option has its advantages (+) and drawbacks (-). Regardless, the ultimate objective remains to move this process guidance to a more permanent home and to sunset the ISG-06 document.

- Revise ISG
    - + Shortest way to adopt changes
    - - Leaves inconsistencies in place
    - - Follow-up actions necessary to incorporate into more permanent guidance
    - - Does not eliminate duplicate guidance
    - – Would not apply to new reactor evaluations

- Incorporate ISG into Standard Review Plan (Ch. 7)
    - - Would take longest amount of time
    - + Most technically correct solution
    - - Will impact several sub-chapters
    - + Would apply to both operating and new reactor evaluations
- Move to a new Branch Technical Position (to be part of Standard Review Plan)
    - + Medium time to implement
    - - Would not likely apply to new reactor evaluations