Industry Input to NRC Questions Presented during the June 8, 2017
MP4 Public Meeting Questions on ISG-06 Revision Proposal
7/5/2017

1) Transitioning BTP 7-14 criteria from LAR I&C licensing review into licensee's QA program:

   a) What information (i.e., specific BTP 7-14 sections) is being moved from the LAR licensing review to QA inspection space?

      Response: Technical reviews of software lifecycle processes and software work products would be removed from the LAR, to eliminate duplication. The licensees would continue to be responsible for ensuring good software. The licensees' nuclear Quality Assurance programs would continue to evaluate the Appendix B vendors. Elements of this compliance can be verified during USNRC inspections. The LAR would state that compliance is assured by a combination of USNRC and licensee work. The regulation continues to be based on 10 CFR 50.55(a)(h) and with the basic tenets of regulatory guidance from BTP 7-14 and other applicable BTPs, including BTP 7-19, as well as with the basic tenets of RGs 1.152, 1.28, 1.168, 1.169, 1.170, 1.171, 1.172, and 1.173.

   b) What regulatory compliance basis would justify moving this information to inspection space?

      Response: The licensee's technical, operations, and maintenance staff most familiar with the operation of the plant with the existing system must be the most familiar with the system's design. This familiarity should enable the licensee's staff to provide critical evaluations. Frequent vendor oversight by the licensee's technical, operations, and maintenance staff would help ensure that the vendor designs, implements, reviews, analyzes, and tests the replacement digital system appropriately to meet the plant system safety, technical, operational, maintenance, and licensing requirements.

      BTP 7-14 is based on the research performed by Lawrence Livermore for NUREG/CR-6101, *Software Reliability and Safety in Nuclear Reactor Protection Systems*. NUREG/CR-6101 is based on the assumption "that the computer system as a whole, as well as the hardware and instrumentation subsystems, will be subject to careful development, analysis, and assessment in a manner similar to that given here for the software." The report is based on the idea that "the assessor" and "the auditor" would both assure that the digital systems being produced would be safe, fulfill the system requirements, and be reliable. Industry has discussed this issue with one of the few remaining original Lawrence Livermore reviewers of the document, who reinforces the view that assessment is required, but that there is no requirement that the assessors be regulators. There is no regulatory compliance basis that forces these reviews into USNRC review space and the prescriptive requirements in BTP 7-14, other than in documents written by USNRC review staff such as BTP 7-14.

c) What information would industry provide to demonstrate that the inspection obligations are equivalent to the current licensing review/audit process?

Response: References for inspection guidance will be incorporated into DI&C ISG-06. There is no intent to reduce the level of design and verification and validation documentation produced. There are places where submitted documentation expectations will be adjusted in DI&C ISG-06, which are expected to be reflected into durable guidance as part of IAP MP 4B. The inspection guidance will be adjusted to reflect current software engineering best practices. Similar documents will be produced under the new guidance as were produced to satisfy BTP 7-14. Further, the USNRC will have the opportunity to work with the demonstration project, which provides the opportunity to adjust inspection guidance to ensure industry produces safe, reliable protection systems to replace the obsolete analog systems currently in use.

d) What additional information would be provided in the LAR to help the staff reach a reasonable assurance determination?

Response: The LAR will focus on providing a complete description, with appropriate figures and tables, of the currently licensed system as well as the interfaces between the existing system and the plant, the control room operators, the maintenance staff, and the engineering staff. The LAR would then describe the new system, discussing fulfillment (or modification, such as replacing manual actions with automated actions) of existing licensing requirements as well as the interfaces with the plant, control room operators, maintenance, and engineering.

The new system architecture will be compared to the existing system architecture and current regulatory expectations, describing how the system architecture implements the requirements in IEEE Std. 603 and the GDCs, but organized on how the architecture supports implementation of:

- Independence (including channel, division, and train, use of voting),
- Redundancy (and implementation of the single failure criterion),
- Deterministic behavior including sufficiently deterministic timing,
- Maintains or enhances the existing defense-in-depth,
- Avoiding unnecessary complexity in the system design.

The LAR will discuss the data communication issues in DI&C ISG-04. The LAR will also summarize the requirements and expectations for ensuring compliance to:

- Plant equipment qualification needs,
- Controlled, managed software development,
- Discuss how a secure development environment will be attained and how the architecture supports a secure operational environment (which may be redacted in the public documents),
- Discuss how cyber security vulnerabilities are to be assessed,

- Demonstrate how platform open items are resolved, or why the open item is not applicable to this design,
- Use of an approved setpoint methodology,
- Discuss any analytical or safety limit changes and their basis,
- Discuss any Technical Specification changes required or requested, and
- Controlled, managed software/hardware/HSI integration.

The combined coverage of each sub-clause within IEEE Stds. 603 and 7-4.3.2 will be demonstrated through a compliance matrix, referencing the discussion in the LAR. This will ensure that all topics defined by these two IEEE standards are discussed adequately within the LAR text, figures, and tables. The intent is not to provide additional information or duplicate existing information but to provide logically organized information rather than attempting to fragment the information into discussion of each clause and sub-clause within IEEE Stds. 603 and 7-4.3.2. This may require paragraph numbering within the LAR, to ensure that the compliance information is meaningful.

2) Adding more detail and explicit sections on architecture:

   a) What type of architecture is being considered for more detail: system architecture, software architecture, hardware architecture?

      Response: The USNRC review scope would primarily be the system architecture and system design. It is likely that the high level descriptions of the software architecture and hardware architecture are provided with the system design.

   b) Is the additional architecture detailed information intended to compensate for providing less BTP 7-14 information in the LAR?

      Response: Industry does not believe that "compensate" is the right word. The materials provided should be sufficient to assess whether the system provides adequate assurance of safety, as long as the utility ensures that their vendor implements a rigorous, controlled software lifecycle process, producing the appropriate documents and other work products, and subjecting those work products to a rigorous verification and validation. Through this rigorous process and documented software lifecycle, a safe, reliable system will result.

3) Replace Clause by Clause compliance to IEEE Std. 603 and IEEE Std. 7-4.3.2 in the LAR with a matrix that maps the clauses to the organized LAR content:

   a) Has industry considered other options for modifying the IEEE Std. 603 and IEEE Std. 7-4.3.2 clause sections in the LAR and ISG-06?

      Response: Industry believes that one statement of the requirements, organized logically, with appropriate traceability to ensure that each clause and sub-clause is addressed provides more value and illustrates the compliance more appropriately. Industry

experience with topical reports and LARs indicates that duplicating materials in a separate standards compliance matrix results in conflicts within the document, and is an unnecessary cost burden. Industry is willing to listen to alternatives.

4) Creating corresponding LAR submittal templates for licensee's use:

   a) Are the templates intended to address industry's near term licensing goals?

      Response: Yes, the templates should address the two scope items discussed during the June 8, 2017 public meeting. As part of IAP MP 4B, industry would like to discuss methods to be used to broaden the focus to Tier 2 and Tier 3 platforms.

      i) Large safety significant system modification (e.g., RPS/ESFAS) based on a previously approved platform with no subsequent major changes (i.e., close to ISG-06 Tier 1)

      ii) Protection system component or software upgrades

      iii) Modification of a previously qualified (Appendix B or CGD) small safety significant component

      Response: This is not part of the agreed-on DI&C ISG-06 scope.