Draft ISG-06, "Licensing Process," Revision 2 Tabletop Exercise
June 13-14, 2018

Sample Recommended Inspection Items

Alternate Review Process-Specific Inspection Items

1. Verify licensee and vendor activities related to the application design, including:
    a. Verify that procedures are implemented to ensure design requirement documentation is reviewed, approved, baselined, updated as necessary, and placed under configuration control.
    b. Verify that a process is implemented to establish a software baseline at the completion of each design activity.
    c. Verify that procedures are implemented to ensure that changes made to the software are evaluated, reviewed, approved, and documented. Verify the documentation includes provisions for documenting a description of the change, rationale for the change, identification of the software baseline affected by the change, and status of the change throughout the implementation process.

2. Verify licensee and vendor activities related to the application implementation, including:
    a. Verify that implementation activities, such as the creation of an executable code, development of operation documentation, software unit testing, and management of software releases are completed in accordance with a documented implementation plan.
    b. Verify that procedures are established and implemented for compliance with coding rules, methods, and standards.

3. Verify licensee and vendor activities related to the application integration, including:
    a. Verify that the plans and methods for integrating function divisions of software (units) are adequately documented. The plan should include a schedule, resource and staffing estimates, and criteria for the commencement of software integration. The software integration plan should also identify what is being integrated, define the integration environment, discuss the management of interfaces, define the integration sequence, and discuss the qualification testing to verify integration has been completed satisfactorily. Refer to BTP 7-14 Section B.3.1.4.4.
    b. Verify that there are provisions in procedures to ensure the complete integration of all software units and comprised software modules or any other division of functional parts.

4. Verify licensee and vendor activities related to the application software testing, software integration testing, software qualification testing, system integration testing, system qualification testing, and factory acceptance testing, including: (Reference BTP 7-14 Section B.3.1.12)

    a. Verify that there are provisions documented in procedures to ensure that all software requirements are covered by acceptance testing.
    b. Verify that documentation supporting software testing includes the following:
        i. Qualifications, duties, responsibilities, and skills required of persons and organizations assigned to testing activities
        ii. Special conditions and controls, equipment, tools, and instrumentation needed for the accomplishment of testing
        iii. Test instructions and procedures that incorporate the requirements and acceptance limits in applicable design documents
        iv. Test prerequisites and the criteria for meeting these requirements and acceptance limits
        v. Test items and the approach taken by the testing program
        vi. Test logs, test data, and test results
        vii. Acceptance criteria
        viii. Test records that indicate the identity of the tester, the type of observation made, the results and acceptability, and the action taken in connection with any deficiencies
        ix. Test plans, activities, tasks, test cases, test coverage methods and standards
    c. Verify that the results of testing are documented, reviewed, analyzed and approved, by a qualified individual to ensure test requirements have been fulfilled.
    d. Verify that there is a documented method to identify and resolve discrepancies between actual and expected integration test results.
    e. Assess whether the process established to incorporate changes to the software due to test results, is adequate to ensure that all test anomalies are documented and resolved.
    f. Anomalies discovered during testing may impact system and software requirements. Verify the actions taken to address testing anomalies include revision to system and software requirement documentation and subsequent design documentation as necessary.
    g. Verify that DI&C system testing is conducted on a completely integrated system, in which all hardware and software functionality has successfully passed integration testing and have been combined into one final system.

5. Verify licensee and vendor activities related to the application verification and validation, including: (Reference BTP 7-14 Section B.3.1.10)

    a. Verify that procedures are established and implemented for performing design reviews, alternate calculations, or testing to verify the adequacy of the software design. Verify the verification of the software design is performed by qualified individuals who were not responsible for or involved in the software design.
    b. Verify that procedures are established and implemented for management reviews, technical reviews, inspections, walkthroughs, and audits.
    c. Verify that procedures are established for the documentation and resolution of all non-conformances identified during the software development lifecycle.
    d. Verify that procedures are established for problem identification, extent of condition, and risk mitigation for issues that have the potential to significantly impact the system quality.

e. Verify that measures are established for conducting reviews which ensure conformance of the software to design requirements and satisfactory completion of the software development activities/phases.

6. Verify licensee and vendor activities related to the application configuration management processes, including: (Reference BTP 7-14 Section B.3.1.11)

   a. Verify that procedures are established and implemented for the control of appropriate records of software development activities which include:
      i. Identification and control of all software designs and code
      ii. Identification and control of all software design functional data (e.g., data templates and data bases)
      iii. Identification and control of all software design interfaces
      iv. Control of all software design changes
      v. Control of software documentation (e.g., user, operating, and maintenance documentation)
      vi. Control of software vendor development activities for the supplied safety system software
      vii. Control and retrieval of qualification information associated with software designs and code
      viii. Software configuration audits
      ix. Status accounting
   b. Verify that provisions are included in procedures ensure software tools used to support system development and verification and validation processes are controlled under configuration management.

7. Verify licensee and vendor activities related to the application secure development and operational environment, including:

   a. Verify that vulnerability assessments are updated periodically as the design progresses, and closed assessments and requirements documents reopened and revised as necessary to reflect any required changes to the system, architecture, system, hardware, software, and HSI, including appropriate verification and validation through analysis, review, and test. Verify that any gaps identified during verification and validation are resolved through the same process. See Section [x.y] of this SE.

   b. Verify that for each identified vulnerability in the secure operational environment, the vulnerability assessment determined whether the vulnerability was 1) eliminated by the design, 2) mitigated to the extent practicable in the design, 3) eliminated or mitigated by installation practice and administrative procedures after installation at the licensee, or 4) represents an unresolved vulnerability that will require long-term monitoring. See Section [x.y] of this SE.

   c. Verify that the transformation from the system design specification to the design configuration items of the secure operational environment are correct, accurate, and complete. Verify that the developer implemented secure development environment procedures and standards to minimize and mitigate any inadvertent or inappropriate alterations of the developed system. Verify that hidden functions and vulnerable features embedded in the code, their purpose and their impact on the integrity and

reliability of the safety system are accounted for. See RG 1.152, Revision 3, Regulatory Position 2.4.

d. Verify that that the secure operational environment design requirements and configuration items intended to ensure reliable system operation are part of the validation effort for the overall system requirements and design configuration items. Verify that the developer correctly configured and enabled the design features of the secure operational environment. Verify the developer tested the system hardware architecture, external communication devices, and configurations for unauthorized pathways and system integrity. See RG 1.152, Revision 3, Regulatory Position 2.5.

Site Inspection Items

8. Ensure that the new platform Keyswitch (used for setting the system operating mode) is added to the Key Control Procedure.
9. Ensure that the platform OOS switch operations are appropriate for testing activities such that no test is performed to render a platform system safety function inoperable without first declaring the affected channel inoperable and entering the appropriate limiting condition for operation (LCO) for this condition.

   The licensee has committed to place reactor protection system (RPS) channels out-of-service prior to changing any associated configuration parameters. Ensure procedures which include activities for changing configuration parameters include steps to declare the affected channel inoperable prior to operation of the platform OOS switches.
10. Perform a comparison of the required platform system software configuration data to the software installed onto the delivered plant RPS equipment.
11. Verify the RPS operating procedures, and maintenance procedures are consistent with the design capability of the platform RPS system and plant technical specifications.
12. Ensure the licensee performs an evaluation of the RPS User Documentation (e.g. technical manuals, training material, procedural changes) associated with the platform RPS system prior to plant startup.
13. Perform a review of procedures that are to be used to control operation of the platform maintenance workstation (MWS) computers. Ensure that the use and limitations of use of the MWS features are consistent with Section [xy], of this SE.
14. Verify that the licensee's software training plan for the platform system is acceptable. Reference BTP 7-14 Section B.3.1.7.
15. Verify that the licensee's software operations plan for the platform system is acceptable. Reference BTP 7-14 Section B.3.1.8.

16. Ensure that the modification test plan specifies the necessary testing to be performed during and after installation of the platform RPS system and that the test procedures are prepared, reviewed, approved, controlled and performed under the existing operating procedures.
17. Ensure the RPS design control package includes an update of the plant USFAR to reflect the modified platform RPS system specific design bases.
18. Verify the licensee has developed and implemented measures to control the use of portable media such as USB flash drives or portable disk drives which can be connected to the platform MWS.
19. Verify the licensee has developed and implemented measures to control access to the [facility where the platform RPS system SAT will be performed].
20. For the platform MWS's, verify the MWS application security level settings are setup by the licensee prior to installation of platform RPS equipment into the plant.