# ATTACHMENT 65001.XX

# INSPECTION OF DIGITAL INSTRUMENTATION AND CONTROL (DI&C) SYSTEM/SOFTWARE DESIGN ACCEPTANCE CRITERIA (DAC)-RELATED ITAAC

PROGRAM APPLICABILITY: 2503

## 65001.XX-01 INSPECTION OBJECTIVES

01.01 To verify that the COL applicant/licensee has developed the DI&C system design as committed in the system ITAAC.

01.02 To confirm by inspection that the COL applicant/licensee has adequately implemented the DI&C design process to yield a design that meets the ITAAC acceptance criteria.

01.03 To provide implementation guidance for use of the Appendices.

## 65001.XX -02 INSPECTION REQUIREMENTS AND GUIDANCE

02.01 Background. Inspection of Inspections, Tests, Analyses and Acceptance Criteria (ITAAC) associated with a Combined License (COL) is intended to support the Commission finding stipulated in 10 CFR Part 52.103(g), specifically that the COL acceptance criteria (ITAAC acceptance criteria) have been met, and that the facility has been designed and built to conform to the licensing basis. A portion of those ITAAC encompass safety-related digital instrumentation and control (DI&C) systems and associated software, the design details of which have been deferred under the Commission policy for Design Acceptance Criteria (DAC) as defined in SECY-92-053. The DI&C DAC-related ITAAC are to be inspected as the design process for the systems progresses and the licensee completes the ITAAC throughout the facility post-COL (construction) phase.

02.02 Inspection Requirements and Guidance.

a. General Inspection Requirements. The development of safety-related DI&C systems and software should progress in accordance with a formally defined Life Cycle. Although life cycle activities may differ between applicants and licensees, all share certain characteristics as outlined in Branch Technical Position (BTP) 7-14 of NUREG-0800 (Standard Review Plan). As stated in BTP 7-14, the NRC staff's acceptance of software for safety system functions is based upon: 1) confirmation that acceptable plans were prepared to control software development activities; 2) evidence that the plans were implemented in the software development life cycles; and 3) evidence that the process produced acceptable design outputs.

Generic inspection attributes and criteria for each DI&C Software Life Cycle Phase are provided within Appendices 1 through 6 of this IP. It is recognized that not all DI&C Life Cycle Phases may be inspected because they may not apply to each licensee's development program/process. The goal of this inspection activity is to examine the governing documents and samples of activities that demonstrate the implementation of these documents in order to provide a comprehensive inspection of the licensee's DI&C development process as delineated in the ITAAC.

The actual planning and scheduling of the DI&C inspections is dependent on the licensee's design development schedule and associated milestones. The guidance contained herein is intended to mirror a typical development life cycle. Inspections should not be planned until the completion of life cycle phases by the licensee can be anticipated and expected completion dates can be confirmed. All construction inspection activities should be coordinated through the Region II Center for Construction Inspection (RII/CCI).

Specific Guidance. Gather pertinent information and discuss inspection planning and scheduling issues with the CCI Branch Chief, or designee, for example:

- importance/prioritization of activities
- concurrent inspections to be conducted using other IPs
- status of previous NRC findings
- licensee responses to applicable Bulletins, Circulars, and Information Notices sent to licensee

Contact the licensee for information needed to prepare the inspection plan, for example:

- status of DI&C development activities, planned activities and schedule (used to focus inspection and determine required sampling during inspection)
- identification of individuals assigned key positions and functions described by the licensee's Software QA and V&V program
- availability of licensee personnel during the period tentatively scheduled for the inspection
- changes to Software QA or V&V program since any previous NRC inspection (e.g., policy, personnel , program description, implementing documents)

1. Requirements for Performance of Inspection. The inspection will be performed in accordance with the inspection plan. Adjustments to the inspection plan will be communicated to Region II/CCI to minimize impact to the licensee and to assist in revising inspection planning efforts accordingly. Unexpected events subsequent to approval of the inspection plan may result in changes to the inspection when conducted.

   Specific Guidance. Conduct the inspection in accordance with this IP and its associated appendices.

2. Requirements for Inspection Reporting. An inspection report and any findings will be prepared, approved, and released in accordance with Inspection Manual Chapter 0613.

   Specific Guidance. No specific guidance.

## 65001.XX -03 RESOURCE ESTIMATE

TBD

## 65001.XX-04 REFERENCES

1. 10 CFR Part 52, “Licenses, Certifications, and Approvals for Nuclear Power Plants”
2. Regulatory Guide 1.206, C.II.1.2.5, “ITAAC for Instrumentation and Controls (SRP Section 14.3.5) and C.III.5, “Design Acceptance Criteria”
3. Regulatory Guide 1.152, Revision 2. "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 2006. (ML053070150)
4. Regulatory Guide 1.168, Revision 1. "Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 2004. (ML040410189)
5. Regulatory Guide 1.169. "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants." Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, 1997. (ML003740102)
6. Regulatory Guide 1.170, “Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants”
7. Regulatory Guide 1.171, “Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants”
8. Regulatory Guide 1.172, “Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants”
9. Regulatory Guide 1.173, “Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants”
10. NUREG 0800 (SRP), Section 14.3, “Inspections, Tests, Analyses, and Acceptance Criteria”
11. NUREG 0800 (SRP), Branch Technical Position (BTP) 7-14, “Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems”
12. NUREG/CR-6101. "Software Reliability and Safety in Nuclear Reactor Protection Systems"
13. Inspection Manual Chapter 2503, “Construction Inspection Program: Inspections of Inspections, Tests, Analyses, and Acceptance Criteria (ITAAC) Related Work”

14. Inspection Manual Chapter 0613, “Documenting 10 CFR Part 52 Construction and Test Inspections” (ML082490463).
15. ASME NQA-1, “Quality Assurance Requirements for Nuclear Facility Applications,” American Society for Mechanical Engineers.
16. IEEE Std. 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations."
17. IEEE Std. 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations"
18. IEEE Std. 730-2002, “IEEE Standard Criteria for Software Quality Assurance Plans”
19. IEEE Std. 828-1990, “IEEE Standard for Configuration Management Plans”
20. IEEE Std. 829-1983, “IEEE Standard for Software Test Documentation”
21. IEEE Std. 830-1993, “IEEE Recommended Practice for Software Requirements Specifications”
22. IEEE Std. 1008-1987, “IEEE Standard for Software Unit Testing”
23. IEEE Std. 1012-1998, "IEEE Standard for Software Verification and Validation Plans"
24. IEEE Std. 1028-1997, “IEEE Guide to Software Configuration Management”
25. IEEE Std. 1074-1995, "IEEE Standard for Developing Software Life Cycle Processes"
26. IEEE Std. 1228-1994, "IEEE Standard for Software Safety Plans"

## 65001.XX -05 PROCEDURE COMPLETION

Implementation of this IP is considered complete when the required sample of attributes for the specified appendices is complete.

END

Appendices:

1. Inspection Guide for DI&C System/Software Life Cycle - Planning Phase
2. Inspection Guide for DI&C System/Software Life Cycle - Requirements Phase
3. Inspection Guide for DI&C System/Software Life Cycle - Design & Implementation Phase
4. Inspection Guide for DI&C System/Software Life Cycle - Integration Phase
5. Inspection Guide for DI&C System/Software Life Cycle - Validation & Test Phase
6. Inspection Guide for DI&C System/Software Life Cycle - Installation Phase

Attachment:

1. Revision History Sheet for IP 65000.XX

## Appendix 1. Inspection Guide for DI&C System/Software Life Cycle – Planning Phase

### A1.01 INSPECTION OBJECTIVES

Verify that the licensee's DI&C development process Planning Phase documents are consistent with the ITAAC design commitments and acceptance criteria.

### A1.02 SAMPLE SIZE

Inspection of DI&C DAC-related ITAAC will typically rely on selection of a sample of attributes for verification. Given the importance of the various Life Cycle Plans in defining and detailing the high quality design and development process expected for safety-related DI&C systems/software, inspection of a larger representative sample of attributes associated with the Planning Phase documents is appropriate.

### A1.03 INSPECTION REQUIREMENTS AND GUIDANCE

General Guidance.

A digital system/software development life cycle, such as that detailed in BTP 7-14, provides definition for a deliberate, disciplined, and high quality design and development process. Implementation of this process should result in a high quality DI&C system and supporting software. Verification of this design process should confirm, by evaluation against applicable standards and criteria, that the licensee and vendor procedures and plans are sufficient to accomplish this goal.

The Planning Phase activities will provide documents that will be used to oversee the DI&C development project as it progresses from one Life Cycle Phase to the next. The documents resulting from the Planning Phase include the following minimum set; additional documents may be required by the development organization as part of their standard business procedures.

- Software Management Plan (SMP)
- Software Quality Assurance Plan (SQAP)
- Software Configuration Management Plan (SCMP)
- Software Verification and Validation Plan (SVVP)
- Software Safety Plan (SSP)
- Software Development Plan (SDP)
- Software Integration Plan (SIntP)
- Software Installation Plan (SInstP)

General Acceptance Criteria for these Planning documents is detailed in BTP 7-14, Section B.3.1, and includes management characteristics, implementation characteristics, and resource characteristics. Not all specific characteristics occur for every Plan. Management characteristics for each Plan should include a stated Purpose, identify

Organizational and Oversight responsibilities, and account for risk and security management. Implementation characteristics should include Process Metrics as well as guidance on Procedure control and Recordkeeping. Resource characteristics should include details of Special Tools utilized in the development process, Personnel resources and qualification, and the Standards used to meet regulatory requirements. Inspection should focus on those aspects of the Plans which can impact the safety and quality of the resulting DI&C system/software design.

In addition to the inspectable attributes identified in the following sections for each of the individual Plans, other attributes may be identified in the Acceptance Criteria of the specific ITAAC. These additional attributes should be included in the scope of the Plan inspection.

Inspection Requirements.

A1.03.01 Inspection of Software Management Plan (SMP).

a. Review the licensee's SMP. Ensure that the SMP addresses the following specific management aspects of the software development project:

1. Organizational structure is defined. Responsibilities are known and documented, and a management structure exists to keep the SMP up to date through a configuration control process.

2. Oversight of vendors- the SMP should describe the interaction between licensee and system/software vendors, extension of QA requirements to vendors, what checks and audits the licensee will perform and their impact.

3. Independence between the software development group and the QA group, system/software safety group, and V&V group. If independence aspects are described in the planning documents of these organizations, such as the V&V Plan, Safety Plan or QA plan, the SMP should provide a pointer to those plans.

4. Personnel responsible for various items have the experience, training and qualifications to perform those duties.

b. Verify that the SMP demonstrates the following key attributes:

1. Project schedule includes time allotted for review (management, V&V, etc.) and audit

2. Project schedule includes time allotted to recover from unanticipated problems

3. Project work products and deliverables are well defined

4. Responsibilities documented and communicated to the development organization

5. Project constraints that may have an impact on safety are identified

6. Known risk factors identified

7. Required reports and technical documents identified

8. Training requirements known and documented

9. Internal review and audit processes identified

A1.03.02 Inspection of Software Quality Assurance Plan (SQAP).

a. Review the licensee's SQAP. Many aspects of software quality are described in the various Plans that are implemented for digital system/software development. This includes the Configuration Management Plan, the Software Safety Plan, and the Software Verification and Validation Plan.

   The SQAP shall comply with the requirements of 10 CFR Part 50, Appendix B, and the licensee's overall QA program. The SQAP should typically: 1) identify which QA procedures are applicable to specific software processes; 2) identify particular methods chosen to implement QA procedural requirements; and 3) augment and supplement the QA program as needed for software.

   Ensure that the SQAP addresses the following:

   1. SQA Management Tasks

   2. Documentation

   3. Standards, Practices, Conventions

   4. Reviews and Audits

   5. Problem Reporting and Corrective Action

   6. Control of Tools, Techniques, and Methodologies

   7. Supplier (Vendor) Control

b. Verify that the SQAP demonstrates the following key attributes:

   1. SQAP specifies which software products are covered by the Plan

   2. Project elements (organizations) that interact with the SQA organization are listed

   3. SQA organization is independent of the development organization, including cost and schedule

   4. Life Cycle development phases that will be subject to SQA oversight are listed

5. Required SQA tasks listed and described

6. Conflict resolution among organizations is described.

7. Required software documents are listed

8. Required reviews and audits are listed

9. Methods by which each review and audit will be carried out is described

10. SQAP includes provisions to assure that problems will be documented and corrected

A1.03.03 Inspection of Software Configuration Management Plan (SCMP).

a. Review the licensee's SCMP. Ensure that the SCMP addresses the following specific activities:

   1. Identification and establishment of production/development baselines

   2. Review, approval, and control of changes

   3. Tracking and reporting of changes

   4. Audits and reviews of the evolving products

   5. Control of interface documentation

b. Verify that the SCMP demonstrates the following key attributes:

   1. Product interfaces that have to be supported within the project are identified

   2. The required capabilities of the staff needed to perform SCM activities are defined

   3. The responsibilities for processing baseline changes is defined

   4. The SCMP specifies who is responsible for each SCM activity

   5. The organizational interfaces that affect the SCM process are identified

   6. SCM activities that will be coordinated with other project activities is described

   7. Describes how phase-specific SCM activities will be managed during the different life cycle phases

   8. Specific procedures exist to manage the change process

   9. Audit procedures are defined

10. Configuration identification scheme matches the structure of the software product

11. SCMP specifies which items will be placed under configuration control (configuration items (CI))

12. SCMP describes the authority of the Configuration Control Board (CCB)

13. CCB authority is sufficient to control safety-related changes to the CI baseline

14. SCMP requires the Configuration Control Board to assess the safety impact of change requests

15. Provisions are included for auditing the SCM process

16. SCMP provides for periodic reviews and audits of the configuration baseline, including physical audits of the baseline

17. SCMP provides for audits of suppliers and subcontractors, if such are used

A1.03.04 Inspection of Software Verification & Validation Plan (SVVP).

a. Review the licensee's SVVP. Ensure that the SVVP addresses the following specific activities.

1. Management of Life Cycle V&V. The major portion of the V&V Plan will describe the methods in which V&V will be carried out through the life of the development project. In general, the following activities should be required for each phase of the life cycle:

    a) Identify the V&V tasks for the life cycle phase.
    b) Identify the methods that will be used to perform each task.
    c) Specify the source and form for each input item required for each task.
    d) Specify the purpose, target and form for each output item required for each task.
    e) Specify the schedule for each V&V task.
    f) Identify the resources required for each task.
    g) Identify the risks and assumptions associated with each V&V task.
    h) Identify the organizations or individuals responsible for performing each V&V task.

2. Requirements Phase V&V. The V&V Plan should describe how the various V&V tasks will be carried out for the following:

    a) Software Requirements Traceability Analysis
    b) Software Requirements Evaluation (Report)
    c) Software Requirements Interface Analysis

d) System Test Plan Generation
e) Acceptance Test Plan Generation

3. Design & Implementation Phase V&V. The V&V Plan should describe how the various V&V tasks will be carried out for the following:

   a) Software Design Traceability Analysis
   b) Software Design Evaluation (Report)
   c) Software Design Interface Analysis
   d) Test Plan Generation
   e) Source Code Traceability Analysis
   f) Source Code Evaluation
   g) Source Code Interface Analysis
   h) Source Code Documentation Analysis

4. Integration Phase V&V. The V&V Plan should describe how the various V&V task will be carried out for the following:

   a) Integration Test Procedure Generation
   b) Integration Test Procedure Execution

5. Validation & Test Phase V&V. The V&V Plan should describe how the various V&V tasks will be carried out for the following:

   a) Acceptance Test Procedure Generation
   b) System Test Procedure Execution
   c) Acceptance Test Procedure Execution

6. Installation Phase V&V. The V&V Plan should describe how the various V&V tasks will be carried out for the following:

   a) Installation Configuration Audit
   b) Final V&V Report Generation

b. Verify that the SVVP demonstrates the following key attributes:

   1. SVVP references the SMP and/or SQAP

   2. Specific elements of the higher-level plans are addressed in the SVVP

   3. Scope of the V&V effort is defined

   4. V&V organization defined, along with its relationship to the development organization

5. Schedule defined that provides enough time for V&V activities to be effectively carried out

6. Tools, techniques, and methods to be used in the V&V process defined

7. Each task identified and tied into the project V&V goals

8. SVVP identifies method of handling anomalies encountered during each activity

9. V&V schedule and resource requirements are described in detail

10. SVVP identifies the responsibilities of the V&V participants

11. Defined procedure for management review of the V&V process

12. Procedure for the periodic assessment and updating of the V&V procedures, methods, and tools

13. Defined procedure for correlating V&V results with management and technical review documents

14. SVVP is coordinated with project Planning documents to ensure early availability of the Planning documents for the V&V effort

15. SVVP explicitly defines the activities required before the requirements development activities begin

c. Verify that the SVVP demonstrates the following Life Cycle Phase-specific attributes:

1. <u>Requirements Activities</u>

a) Concept documentation, software requirements specification (SRS), interface requirements, hazards analysis, and user documentation will be complete prior to beginning the V&V requirements analysis
b) SVVP explicitly defines the activities required during the requirements analysis
c) SVVP requires the performance of a software requirements traceability analysis that traces elements of software requirements to system and source requirements
d) SVVP requires that the SRS be evaluated for safety, correctness, consistency, completeness, accuracy, readability, and testability
e) SVVP requires that the SRS be evaluated for performance issues
f) SVVP requires that a system test plan and an acceptance test plan be generated during the requirements phase

2. Design & Implementation Activities

   a) SVVP requires the generation and dissemination of anomaly reports
   b) SVVP explicitly defines the activities required during design/implementation phase
   c) SVVP requires the performance of a design traceability analysis that traces elements of the detailed design and coding to elements of the software requirements
   d) SVVP requires a design evaluation (report)
   e) SVVP requires a design interface analysis
   f) SVVP requires that the software design document be evaluated against hardware requirements, operator requirements, and software interface requirements documentation
   g) SVVP requires a software component test plan, an integration test plan, and a test design be generated for use in later testing
   h) SVVP requires that the source code be evaluated for correctness, consistency, completeness, accuracy, readability, safety, and testability
   i) SVVP requires generation and use of test cases to help ensure the adequacy of test coverage
   j) SVVP requires the generation of test cases for software component, integration, system, and acceptance testing

3. Integration, Validation & Test, and Installation Activities

   a) SVVP explicitly defines the activities required during the integration and validation analysis and testing
   b) SVVP requires the performance of integration, system, and acceptance testing requirements sufficiently detailed so as to ensure that there is a very low probability of error during operation
   c) SVVP explicitly defines the activities required during the installation analysis and testing
   d) SVVP requires the performance of an installation configuration audit
   e) SVVP requires the generation of a final report

A1.03.05 Inspection of Software Safety Plan (SSP)

a. Review the licensee’s SSP. Ensure that the SSP addresses the following documentation that will be required as part of the software safety program:

   1. Results of all safety analyses

   2. Information on suspected or verified safety problems

   3. Results of audits performed on software safety program activity

4. Results of safety tests carried out on the software system

5. Records on training provided to software safety personnel and software development personnel

b. Verify that the SSP demonstrates the following key attributes:

1. Software safety organization is described and authority defined; authority sufficient to enforce compliance with safety requirements and practices

2. SSP provides a mechanism for defining safety requirements, performing software safety analysis tasks, and testing safety-critical features of the DI&C system

3. SSP describes what safety-related documents will be produced during the development life cycle; contents sufficient to ensure that known safety concerns are addressed in the appropriate places within the development life cycle

4. SSP identifies the safety-related records that will be generated, maintained, and preserved

5. SSP specifies the process of approving and controlling software tool use

6. SSP provides a means to ensure that safety-critical software developed by a subcontractor meets the requirements of the software safety program

A1.03.06 Inspection of Software Development Plan (SDP)

a. Review the licensee's SDP. The SDP should clearly state which tasks are a part of each life cycle, and state the life cycle inputs and outputs. The review, verification and validation of those outputs should be defined. The SDP should list the international, national, industry, and company standards and guidelines, including regulatory guides, which will be followed, and whether or not these standards and guidelines have previously been approved by the NRC staff.

b. Verify that the SDP demonstrates the following key attributes:

1. Technical standards that will be followed are listed

2. Technical milestones are listed

3. Milestones are consistent with the schedule provided in the SMP

4. Technical documents that must be produced are listed

5. Technical documents are consistent with those listed in the SMP

6. Milestones, baselines, reviews, and signoffs are listed for each document

7. Audit reports document that the SDP is being followed

A1.03.07 Inspection of Software Integration Plan (SIntP)

a. Review the licensee’s Software Integration Plan. The plan should describe the general strategy for integrating the software modules together into one or more programs, and integrating those programs with the hardware. Verify that the integration strategy includes integrating the various software modules together to form single programs, integrating the result of this with the hardware and instrumentation, and testing the resulting integrated product.

b. Verify that the SIntP demonstrates the following key attributes:

1. SIntP specifies the levels of integration required

2. SIntP is consistent with the software design specification

3. SIntP describes each step of the integration process

4. SIntP describes the environment that will be used to perform and test each integration step

5. Software and hardware tools that will be used to integrate the system are listed

6. SIntP includes instructions on how to carry out integration steps

7. SIntP includes a contingency plan in case the integration fails

8. SIntP includes a requirement for configuration control of the completed product

A1.03.08 Inspection of Software Installation Plan (SInstP)

a. Review the licensee’s SInstP. Ensure that the SInstP demonstrates the following key attributes:

1. General procedures for installing the software product are described

2. Materials required are listed in an Installation Package

3. Complete step-by-step procedures exist for installation in the operational environment

4. Expected results from each installation step described

5. Known installation error conditions and recovery procedures described

6. Installation Plan fully tested

Attachment 1

Revision History Sheet for IP 65001.XX

INSPECTION OF DIGITAL INSTRUMENTATION AND CONTROL (DI&C)
SYSTEM/SOFTWARE DESIGN ACCEPTANCE CRITERIA (DAC)-RELATED ITAAC

| Commitment Tracking Number | Issue Date | Description of Change | Training Needed | Training Completion Date | Comment Resolution Accession Number |
|---|---|---|---|---|---|
| ` | | | | | |