



“Process Based” Digital I&C ITAAC Closure

Sarah DiTommaso

ITAAC & Inspection Support Manager

Westinghouse

Purpose

- **AP1000** Licensees have begun preparations for closure of process-based DI&C ITAAC 2.5.02.14 [Index Number 553.] and have received challenges by the NRC of the closure approach previously discussed which the AP1000 Licensees and Westinghouse want to discuss.
- Continue previous CIP public meeting discussions on this generic DI&C topic and discuss SNC Docketed Letter ND-16-0753.

Background

- Technologies with Digital I&C systems, including **AP1000**[®] contain “process-based” ITAAC covering I&C system development.
- Several previous Construction Inspection Program public meetings have discussed these types of ITAAC including May and November 2014 CIPTF meetings
- November 2014 CIPTF meeting discussed approach to closure of the ITAAC and information included in the ICN.

Background

- **AP1000** conclusion: Process-based DI&C ITAAC should be closed based on a process that has been exercised.
 - ITAAC Closure documentation is process **definition**
 - Closure timing is after each aspect of the defined process has experienced a sufficient degree of implementation and NRC inspection.
- ITAAC 2.5.02.13 (Index 552) was closed based on inspection of the processes and the NRC accepted this ITAAC completion notification.

Process-Based DI&C ITAAC

- Verbatim language of the ITAAC requires that the report concludes that the *processes* meet the requirements and not *implementation*.
- The balance between process *definition* and *implementation* affects ITAAC Closure:
 - Some degree of implementation of the process is prudent, in order to demonstrate the robustness and effectiveness of the process.
 - Fully understood and expected that the NRC will inspect implementation of these processes as part of ITAAC closure verification, which is also consistent with FSER statements.
 - Principle Closure Documents and ITAAC Closure Notification will discuss the inspection of the processes.
 - ICN along with NRC Inspection Reports of process implementation are utilized for ITAAC closure.

Challenges with ICN “Implementation” Approach

- Verbatim ITAAC language includes:
 - ITA - “Inspection will be performed of the process...”
 - AC – “A report exists and concludes that the process...”
- Five total ITAAC that fall into this category: 2.5.01.04, 2.5.02.11, 2.5.02.12, 2.5.02.13, 2.5.02.14
- Incorporation of implementation into the ICN creates condition where the PMS ITAAC can no longer be closed prior to fuel load and does not have a clear closure point.
 - Potential for design changes based on Start-Up Testing Lessons Learned
 - Implementation of PMS processes can occur beyond fuel load
- ITAAC 2.5.02.12 [Index No. 551] includes maintenance which potentially will not be implemented until after fuel load.
 - Closure based on implementation of maintenance extends through the life of the plant.

Conclusions for Process-Based DI&C ITAAC

- ITAAC Completion must be based on rigorous processes and not implementation.
 - ICNs and Principle Closure Documents focused on the process to meet verbatim ITAAC language
- Closure timing of Process-Based DI&C ITAAC should be after some degree of implementation to ensure processes are rigorous.
- NRC may inspect implementation of the processes prior to and after ITAAC completion.



Back-Up Slides

Digital I&C Process ITAAC

ITAAC #	Design Commitment	Inspection, Test, Analysis	Acceptance Criteria
2.5.01.04	<p>4. The DAS hardware and any software are developed using a planned design process which provides for specific design documentation and reviews during the following life cycle stages:</p> <ul style="list-style-type: none"> a) Development phase for hardware and any software b) System test phase c) Installation phase <p>The planned design process also provides for the use of commercial off-the- shelf hardware and software.</p>	<p>Inspection will be performed of the process used to design the hardware and any software.</p>	<p>A report exists and concludes that the process defines the organizational responsibilities, activities, and configuration management controls for the following:</p> <ul style="list-style-type: none"> a) Documentation and review of hardware and any software. b) Performance of tests and the documentation of test results during the system test phase. c) Performance of tests and inspections during the installation phase. <p>The process also defines requirements for the use of commercial off-the-shelf hardware and software.</p>
2.5.02.11	<p>11. The PMS hardware and software is developed using a planned design process which provides for specific design documentation and reviews during the following life cycle stages:</p> <ul style="list-style-type: none"> a) Not used b) System definition phase c) Hardware and software development phase, consisting of hardware and software design and implementation d) System integration and test phase e) Installation phase 	<p>Inspection will be performed of the process used to design the hardware and software.</p>	<p>A report exists and concludes that the process defines the organizational responsibilities, activities, and configuration management controls for the following:</p> <ul style="list-style-type: none"> a) Not used. b) Specification of functional requirements. c) Documentation and review of hardware and software. d) Performance of system tests and the documentation of system test results, including a response time test performed under maximum CPU loading to demonstrate that the PMS can fulfill its response time criteria. e) Performance of installation tests and inspections.

Digital I&C Process ITAAC

ITAAC #	Design Commitment	Inspection, Test, Analysis	Acceptance Criteria
2.5.02.12	<p>12. The PMS software is designed, tested, installed, and maintained using a process which incorporates a graded approach according to the relative importance of the software to safety and specifies requirements for:</p> <ul style="list-style-type: none"> a) Software management including documentation requirements, standards, review requirements, and procedures for problem reporting and corrective action. b) Software configuration management including historical records of software and control of software changes. c) Verification and validation including requirements for reviewer independence. 	<p>Inspection will be performed of the process used to design, test, install, and maintain the PMS software.</p>	<p>A report exists and concludes that the process establishes a method for classifying the PMS software elements according to their relative importance to safety and specifies requirements for software assigned to each safety classification. The report also concludes that requirements are provided for the following software development functions:</p> <ul style="list-style-type: none"> a) Software management including documentation requirements, standards, review requirements, and procedures for problem reporting and corrective action. Software management requirements may be documented in the software quality assurance plan, software management plan, software development plan, software safety plan, and software operation and maintenance plan; or these requirements may be combined into a single software management plan. b) Software configuration management including historical records of software and control of software changes. Software configuration management requirements are provided in the software configuration management plan. c) Verification and validation including requirements for reviewer independence. Verification and validation requirements are provided in the verification and validation plan.

Digital I&C Process ITAAC

ITAAC #	Design Commitment	Inspection, Test, Analysis	Acceptance Criteria
2.5.02.13 (Closed)	<p>13. The use of commercial grade computer hardware and software items in the PMS is accomplished through a process that specifies requirements for:</p> <ul style="list-style-type: none"> a) Review of supplier design control, configuration management, problem reporting, and change control. b) Review of product performance. c) Receipt acceptance of the commercial grade item. d) Acceptance based on equipment qualification and software validation in the integrated system. 	<p>Inspection will be performed of the process defined to use commercial grade components in the application.</p>	<p>A report exists and concludes that the process has requirements for:</p> <ul style="list-style-type: none"> a) Review of supplier design control, configuration management, problem reporting, and change control. b) Review of product performance. c) Receipt acceptance of the commercial grade item. d) Acceptance based on equipment qualification and software validation in the integrated system.
2.5.02.14	<p>14. The Component Interface Module (CIM) is developed using a planned design process which provides for specific design documentation and reviews.</p> <p>(Design Acceptance Criteria)</p>	<p>An inspection and or an audit will be performed of the processes used to design the hardware, development software, qualification and testing.</p>	<p>A report exists and concludes that CIM meets the below listed life cycle stages. Life cycle stages:</p> <ul style="list-style-type: none"> a. Design requirements phase, may be referred to as conceptual or project definition phase b. System definition phase c. Hardware and software development phase, consisting of hardware and software design and implementation d. System integration and test phase e. Installation phase

“Process Based” Digital I&C ITAAC Closure

Sarah DiTommaso & Brian Bedford

Westinghouse Electric Company

Background

- Technologies with Digital I&C systems, including **AP1000**[®] contain “process-based” ITAAC covering I&C system development.
- Several previous Construction Inspection Program public meetings have discussed these types of ITAAC, but haven’t specifically addressed ITAAC Closure documentation and timing.
- Relevant aspects of previous discussions included the relationship between *Definition* and *Implementation* of the process as they relate to ITAAC performance, NRC Inspection, and ITAAC Closure.

Purpose

- **AP1000** Licensees have begun preparations for closure of the 1st process-based DI&C ITAAC.
- Continue Previous CIP public meeting discussions on this generic DI&C topic, focusing specifically on ITAAC Closure, based on this recent experience.

ITAAC No.	Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
2.5.02.13	<p>13. The use of commercial grade computer hardware and software items in the PMS is accomplished through a process that specifies requirements for:</p> <p>a) Review of supplier design control, configuration management, problem reporting, and change control.</p> <p>b) Review of product performance.</p> <p>c) Receipt acceptance of the commercial grade item.</p> <p>d) Acceptance based on equipment qualification and software validation in the integrated system.</p>	<p>Inspection will be performed of the process defined to use commercial grade components in the application.</p>	<p>A report exists and concludes that the process has requirements for:</p> <p>a) Review of supplier design control, configuration management, problem reporting, and change control.</p> <p>b) Review of product performance.</p> <p>c) Receipt acceptance of the commercial grade item.</p> <p>d) Acceptance based on equipment qualification and software validation in the integrated system.</p>

AP1000 ITAAC 2.5.02.13 Closure Overview

- Principal Closure Document for the ITAAC is a report that summarizes a review/inspection of the PMS Commercial Grade Dedication (CGD) Process.
- The report provides:
 - Overview description of the CGD Process
 - Applicable regulatory and industry guidance
 - List of applicable Procedures and Commercial Dedication Instructions, and explanation of how each is used to implement the CGD process.
 - Explanation of how each aspect of the Design Commitment is met by the defined CGD process.
- Preparations for ITAAC closure included reviews of process implementation & outputs to confirm each part of the process has been exercised and implemented successfully.
 - This activity is performed separate from the summary report



General Conclusions for Process-Based DI&C ITAAC

- The balance between process *definition* and *implementation* affects the timing of ITAAC Closure:
 - Some degree of implementation of the process is prudent, in order to demonstrate the robustness and effectiveness of the process.
 - Waiting until the process has been fully implemented is impractical, and results in unnecessarily delaying ITAAC closure until late in construction – exacerbating the Surge.
- **AP1000** conclusion: Process-based DI&C ITAAC should be closed based on a process that has been exercised.
 - ITAAC Closure documentation is process ***definition***
 - Closure timing is after each aspect of the defined process has experienced a sufficient degree of implementation.

ITAAC Maintenance Considerations

- The balance between process *definition* and *implementation* also has implications for ITAAC Maintenance.
- The thresholds in NEI 08-01/RG 1.215 determine when ITAAC Post-Closure Notification is necessary.
- The following *would* likely trip a notification threshold:
 - A significant change to the process itself
 - A material deficiency identified in the process
- The following *would not* likely trip a notification threshold, because the ITAAC is about the process definition:
 - Continued implementation of the process following ITAAC closure
 - A deficiency identified where the process was not implemented properly. (*The deficiency must be corrected, but the process is still complete and valid.*)