

NRC INSPECTION MANUAL

EICB

INSPECTION PROCEDURE 52003

DIGITAL INSTRUMENTATION AND CONTROL MODIFICATION INSPECTION

PROGRAM APPLICABILITY: 2515

52003-01 INSPECTION OBJECTIVES

01.01 To ensure that digital instrumentation and control (digital I&C) systems that have been reviewed by the NRC staff are installed, operated, and maintained according to the safety evaluation, and in accordance with the manufacturer's design and operating recommendations (as appropriate), and licensee commitments.

01.02 To ensure that the licensee has properly considered the guidance for effective system design in the upgrade, and has satisfied the plant specific licensing basis.

52003-02 INSPECTION REQUIREMENTS AND GUIDANCE

02.01 Advance Preparation. Be familiar with the licensee's administrative programs for designing, installing, testing, and maintaining modifications. The following documents may be reviewed throughout the course of the inspection if available. Many will be reviewed during the amendment request, and will be discussed in the staff's Safety Evaluation Report (SER); but knowledge of these documents will still be required to conduct the inspection.

- a. Updated Final Safety Analysis Report (UFSAR).
- b. Technical Specifications (TS).
- c. The licensee's Quality Assurance Program (for both hardware and software).
- d. Final Installation Report.
- e. Final Test Reports.
- f. Installation Test reports.
- g. Site Acceptance Test (SAT) Plans and Reports.
- h. Site Installation Documentation.
- i. Completed Test Procedures.
- j. Summary of SAT and Acceptance Test Results.

- k. Verification and Validation (V&V) Problem Reports.
- l. V&V Report on Test Plans and Procedures.
- m. V&V Report on Installation Test.
- n. Software Design Requirements Traceability Database (RTD).
- o. Software Design Documents (SDD).
- p. System/Subsystem Design Documents.
- q. Software Test Plan (STP).
- r. Software Configuration Management (CM) Document.
- s. Software Development Capability Maturity Model (or equivalent) Certification Reports and Procedures.

02.02 Inspection Plan. Develop a site-specific inspection plan to select and review the activities associated with the major phases of the digital I&C modification. The site-specific inspection plan should include a sample of inspection requirements outlined below. The emphasis on inspection activities should be based on the overall scope, the safety and/or risk significance of the activities, the licensee's historical performance in that area, and industry experience. Additional emphasis may be considered for those licensee activities that include new or different management controls, or are being managed/controlled in a different manner, or implemented with new techniques.

- a. Digital I&C modification inspections involve four major areas of effort: developing an understanding of the modification design; documentation verification; review of testing, operations, and training; and a review of plans for maintenance and repair efforts.
- b. NRR will conduct an evaluation of the proposed license amendment as part of the normal review process. This will include a review of the design and capabilities of the modification. Regional inspectors will perform documentation and functionality reviews after the system leaves the vendor. While regional inspectors will need to review specific documentation to gain familiarity with the system, inspectors should not duplicate NRR review efforts.
- c. Any operating experience related to similar digital I&C modifications is an excellent resource for assistance in development of the inspection plan, and should be reviewed in order to provide insight into previously identified issues. NRR should be contacted to gain additional insight in a particular inspection area that may be similar to past reviews/inspections.
- d. The inspection should be conducted by inspector(s) who are knowledgeable in the areas of digital I&C and operations. Additionally, environmental conditions and cyber security will need to be verified to meet the requirements of the SER. Therefore, it may be appropriate to include/consult inspector(s) knowledgeable in these areas. However, all inspectors should be familiar with digital equipment. Specific technical support from NRR may be required and should be coordinated through the NRR project manager.

02.03 Design Review. Review the documentation required to gain a working knowledge of the digital I&C modification. The intent is for inspectors to be familiar with the system;

not to duplicate previous NRR review efforts. The following are major areas that should be considered for review by the inspector(s):

- a. Review the necessary documentation, and determine the full scope of the digital I&C upgrade. This review should include the staff's SER, any licensing commitment documents concerning the modification, manufacturer literature on the hardware and software being installed, and applicable drawings and schematics. To facilitate developing a familiarity with the modification, regional management may authorize inspection visits to vendor facilities.
 1. Determine the project scope including architecture, input consolidations, whether multiple trains are affected, whether the system supplies or receives inputs from other systems, isolation and interface devices, affected indicators, and the credited function of the system.
 2. Review the design specification to verify that the architecture, inputs, process, timing and outputs for the system are adequately detailed. The timing should include an analysis of the sampling rate and processor execution time to show that digital control systems requirements are met.
 3. Review the process used to minimize the probability of incorrect translation of the system basis to hardware and software requirements.
- b. Review the licensee's proposed schedule for implementation, and evaluate it against the shutdown risk analysis for conducting the modification. Review the licensee's plan, to include whether the modification will be implemented in conjunction with a complete core offload.
- c. Verify that any change to the human-system interface design reflects current human factors principles including compatibility with the remainder of the control room or local control stations.

02.04 Documentation Verification. Conduct selected reviews of the following areas, consistent with the safety significance and inspection resources:

- a. Verify that the as-installed digital modification is in accordance with the NRC SER, design drawings, and licensee commitments.
 1. Verify that applicable 10 CFR 21 Notifications, Bulletins, Generic Letters, and Information Notices were correctly applied to the system.
 2. Determine the effectiveness of the licensee and vendor interface during system development, system installation, and system modification (i.e. active, no real interface, black box, etc.)
 3. Verify that relevant manufacturer recommendations have been correctly incorporated, and that there is a system in place to track manufacturer recommendations.
 4. Verify that the environmental conditions are consistent with those stated in the SER, manufacturer recommendations, and applicable industry standards under all conditions (including testing).

5. Verify that the shielding and grounding scheme is consistent with the SER, manufacturer recommendations, and applicable industry standards.
 6. Verify that the cable routing scheme (how cables are mixed, how cables are run, bus terminations, etc.) is consistent with the SER, manufacturer recommendations, and applicable industry standards.
 7. Verify that cyber-security designs are incorporated in accordance with the SER.
 8. Verify that software/hardware for individual devices that are part of the network are consistent with the SER, manufacturer recommendations, and applicable industry standards. Verify that software life cycles are consistent for independent devices and the host device.
- b. Verify that surveillance, abnormal operating, emergency operating and annunciator response procedures have been updated, and correctly reflect the new system attributes.
1. Verify that the licensee updated affected procedures. Review how the licensee ensures that all affected procedures have been correctly updated.
 2. Verify that the digital systems self-test incorporates a return to normal procedure to provide the safety function in the event of an accident while the system is in self test. Determine if the analysis of the sampling rate and processor execution time show that there is sufficient margin, such that accident analysis requirements are still met.
 3. Verify that calibration procedures meet the TS, applicable licensee standards, and vendor recommendations.
 4. Verify that the calibration and surveillance procedures provide complete loop testing, or that there is adequate overlap of the separate sections to ensure complete testing.
 5. Assess the applicability of reactivity control during the performance of a surveillance to ensure that only licensed operators will manipulate equipment that affects reactivity.
 6. Verify that surveillance procedures have instructions for returning the system to 'normal' if conditions require terminating the surveillance prior to completion.
 7. Determine how any personal computers, portable configurators, or other interface test equipment are controlled (i.e. physical protection, virus protection, password control, and personnel access). Evaluate the adequacy of this control for security, and that it is sufficiently self-checking to minimize the introduction of errors.
 8. Verify that electro-static discharge (ESD) and electromagnetic interference/radio frequency interference (EMI/RFI) precautions and

considerations have been incorporated into relevant procedures and are followed.

- c. Verify that plant drawings, the UFSAR, and other relevant documentation have been updated to reflect the replacement system. In those cases where the update to the UFSAR and other relevant documentation has not been completed, ensure that the process is underway, and is properly planned and proceeding in a timely manner.
- d. Verify the adequacy and quality of the power and grounding system for the modification. The power quality and grounding review should address the following:
 - 1. Grounding: Determine if there are any special grounding requirements from the vendor or due to plant conditions (i.e. age, potential of ground, floating versus non-floating) that should have precipitated an additional grounding review by the licensee.
 - 2. Power Requirements: Determine if the licensee considered battery loading profiles, maximum inverter loads, and inrush currents.
 - 3. Power Quality (voltage, frequency, harmonic distortion): Evaluate voltage/frequency fluctuations and total harmonic distortion against the manufacturer's specification. Was harmonic distortion measured before and after installation to ensure this digital upgrade does not create additional problems?
 - 4. Power Quality Impact of the Digital System: Determine if the post-installation effects of the digital system were considered for their effects on other instrumentation powered from the same source, and vice versa (e.g. clocks and switching circuits can create their own harmonics).

02.05 Review of Testing, Operations, and Training. Conduct selected inspections and reviews of the following areas, consistent with the safety significance and inspection resources:

- a. Become familiar with the license amendment request (LAR), V&V plans and final report, RTD, STP, SDD, all Requests for Additional Information, and the NRC SER. Review the software test plan in accordance with BTP 7-14, Section B.3.1.12, and determine if the software test plan is sufficiently detailed to provide site acceptance tests, installation tests, and startup tests for the proposed digital system. Review the procedures for the SAT, installation test, and start-up tests; and review the final V&V reports on these test procedures.
 - 1. Determine if the SAT will adequately test the licensee (not vendor) system specification, and that the test procedures are sufficiently detailed, clear, and unambiguous to allow site personnel to perform this test.
 - 2. Determine if the installation test will adequately demonstrate that the system, as installed, will meet the all system requirements, and all plant specific requirements listed in the SER; and that the test procedures are sufficiently detailed, clear, and unambiguous to allow site personnel to perform this test.

3. Determine if the start-up testing will demonstrate that the system will meet all operational requirements, and that the test procedures are sufficiently detailed, clear, and unambiguous to allow site personnel to perform this test.
 4. Determine if appropriate levels of V&V have been applied to these test plans and procedures.
- b. Review the Operations Manuals in accordance with BTP 7-14, Section B.3.3.7, and determine if the manuals are sufficiently detailed, clear, and unambiguous to allow site operational and maintenance personnel to understand and operate the software and the system.
 - c. Review the Software Training Plan in accordance with BTP 7-14, Section B.3.1.7, and determine if the plan provides adequate software training, appropriate for the level of maintenance being planned for licensee personnel. Review the Software Training Manuals in accordance with BTP 7-14, Section B.3.3.9, and determine if the manuals are sufficiently detailed and understandable to provide training of operations and maintenance personnel, based upon the level of maintenance planned for site staff.
 - d. Verify that the operators, technicians, and system engineers have been adequately trained, and have an understanding of the system commensurate with their responsibilities. In order to perform the verification that the operators, technicians, and system engineers have been adequately trained, interviews with the personnel may be required to ensure they have an understanding of the system commensurate with their responsibilities. If the licensee intends to use vendor support to maintain the system, review what controls the licensee exercises over the vendor with respect to design control, access, and software configuration.
 - e. Review any hardware and software failures that have occurred to determine if they were properly resolved or if there are system weaknesses that require correction.
 1. Verify that the system failure information is trended and that trends are properly used to predict system performance and reliability.
 2. Sample LERs and/or surveillance and/or repair orders related to the system to determine if any trending indicators have been missed by the licensee, or if there are larger generic implications on reliability.
 - f. Inspect the installation environment and verify that the licensee-specified environmental parameters accurately reflect the installation environment. The review should address the following:
 1. Did the licensee specify the environmental qualification parameters (i.e. temperature, humidity, radiation, seismic, surge withstand, and EMI/RFI) when purchasing the system?
 2. Did the licensee credit previous operating history for the digital equipment under review? Did the licensee consider commercial or nuclear experience? Were the applications similar? Was documentation available to confirm acceptable equipment performance?

3. If vendor testing was performed to verify the resulting qualification, did the licensee specifically review these tests for applicability to the installation environments?
 4. Were testing anomalies, testing configuration, and test results specifically reviewed by the licensee? Is appropriate supporting documentation, and level of licensee involvement with the testing demonstrated?
 5. Are the environmental parameters consistent with the licensing bases?
- g. Verify that setpoints and related uncertainty terms have been adequately evaluated and revised to reflect the new system, and have been accurately installed in the software. Request the licensee to download the current system setpoints and coefficients to a selected sample and compare these to the system requirements documentation.
 - h. Verify that proper indication and/or annunciation for system bypass and failure is functional during installation or startup.

02.06 Review of Plans for Maintenance and Repair. Identify and review the licensee's plans for repair efforts. Perform selective inspections, consistent with the safety significance and inspection resources, of the following areas:

- a. Review maintenance and repair procedures to verify they have been updated, and correctly reflect the new system attributes.
 1. Determine if the licensee intends to repair specific boards, or if boards will be returned to the vendor for repair. If the licensee will be performing board repair activities, verify that the vendor manuals and drawings contain adequate details and that maintenance personnel involved in board repair have been trained and certified. Inspectors should also review the licensee's test equipment, and the frequency of board testing. If the licensee will be using vendor repair activities, verify that an adequate supply of spare boards is available on site. Batteries embedded in the system should be on a periodic replacement schedule, if recommended by the battery manufacturer. This includes batteries used for battery backed random access memory (RAM).
 2. Verify that ESD precautions and considerations have been incorporated into relevant procedures, and are followed.
 3. Verify that cabinet ventilation devices are properly maintained.
- b. Verify that the handling and storage requirements of spare system parts are consistent with manufacturer and licensee requirements (periodic power-up, battery life, etc.). Determine if the licensee implemented any special procedures for ensuring that stored parts will be correctly handled (such as ensuring stored chips with embedded software are the correct revision).

52003-03 DOCUMENTATION

Based on its unique nature, this inspection procedure may be documented outside the requirements of Inspection Manual Chapter 0612. The report should provide sufficient information regarding what items were inspected and the results of those reviews. Any commitments that were not met by the licensee should be clearly annotated in the inspection report.

52003-04 RESOURCE ESTIMATE

The resource estimate for inspectors is typically 240 hours of offsite preparation and review, to determine acceptability of plans and procedures; and 100 hours of onsite activities, in order to complete the required inspections. Onsite inspection activities will likely need to be scheduled to coincide with plant milestones, which may occur over a several week period.

52003-05 REFERENCES

References for this inspection procedure are extensive and are listed in Appendix A. Some of the documents listed are for the inspector's information only, and are not considered regulatory requirements unless the licensee has formally committed to implementing any of these documents. Verify that any documents reviewed are the latest endorsed references. Contact the Instrumentation and Control Branch in NRR for an electronic collection (compact disk) of the appropriate references for the modification being reviewed.

52003-06 COMPLETION STATUS

This inspection procedure shall be conducted to demonstrate that the modification is implemented in a safe manner. Satisfactory reviews of documentation verification; testing, operations, and training; and plans for maintenance and repair will constitute completion of this procedure in the RPS.

END

Appendices:

- A List of References
- B Revision History for IP 52003

APPENDIX A
LIST OF REFERENCES

References that an inspector should be familiar with:

Regulatory Guide 1.152, "Criteria for Programmable Digital Computer System Software in Safety-Related Systems of Nuclear Power Plants"

Regulatory Guide 1.170, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"

Regulatory Guide 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"

Regulatory Guide 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"

NUREG-0700, Rev. 1, "Human-System Interface Design Review Guideline"

NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants", Chapter 7, Instrumentation and Controls

NUREG CR-6101, "Software Reliability and Safety in Nuclear Reactor Protection Systems"

ANSI/IEEE Std. 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations, Institute of Electrical and Electronic Engineers"

ANSI/IEEE Std. 1012-1986, "IEEE Standard for Software Verification and Validation Plans"

IEEE 829-1983, "Software Test Documentation"

IEEE 1008-1987, "IEEE Standard for Software Unit Testing"

IEEE 1074-1991, "Standard for Developing Software Life Cycle Processes"

Additional references that may be useful to an inspector:

Regulatory Guide 1.22, "Periodic Testing System Actuation Functions"

Regulatory Guide 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant"

Regulatory Guide 1.53, "Application of the Single Failure Criterion to Nuclear Power Plant Systems"

Regulatory Guide 1.75, "Physical Independence of Electrical Systems"

Regulatory Guide 1.97, "Instrumentation for Light-Water Cooled Nuclear Power Plants To Assess Plant and Environs Conditions During and Following an Accident"

Regulatory Guide 1.100, "Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants"

Regulatory Guide 1.118, "Periodic Testing of Electric Power and Protection Systems"

Generic Letter 83-28, "Required Actions Based on Generic Implications of Salem ATWS Event"

IN83-83, "Use of Portable Radio Transmitters Inside Nuclear Power Plants"

NUREG-0493, "A Defense-in-Depth and Diversity Assessment of the RESAR-414 Integrated Protection System"

NUREG-0711, "Human Factors Engineering Program Review Model"

NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants", Chapter 13.2, Training, and Chapter 13.5, Plant Procedures

NUREG-0800, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants", Chapter 18, Human Factors Engineering

NUREG CR-3270, "Investigation of Electro-magnetic Interference (EMI) Levels in Commercial Nuclear Power Plants"

NUREG/CR-4640, "Handbook of Software Quality Assurance Techniques Applicable to the Nuclear Industry"

NUREG/CR-6303 "Method for Performing Defense-In-Depth and Diversity Analyses of the Reactor Protection System"

ANSI/IEEE-ANS-7-4.3.2-1993, "Application Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations"

IEEE 279-1971, "Criteria for Protection Systems for Nuclear Power Generating Stations"

IEEE 323-1974, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations"

IEEE 338-1977, "IEEE Standard Criteria for Periodic Testing of Nuclear Power Generating Station Safety Systems"

IEEE 344-1975, "IEEE Recommended Practices for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations"

IEEE 379-1977, "Application of the Single Failure Criterion to Nuclear Power Generating Station Class 1E Systems"

IEEE 384-1977, "Criteria for Independence of Class 1E Equipment and Circuits"

IEEE 472-1974, "Guide for Surge Withstand Capability Tests"

IEEE 518-1982, "Guide for the Installation of Electrical Equipment to Minimize Electrical Noise Inputs to Controllers from External Sources"

IEEE 730-1989, "Software Quality Assurance Plans"

IEEE 828-1983, "Software Configuration Management Plans"

IEEE 830-1984 "Guide to Software Requirements Specifications"

IEEE 1016-1987 "Recommended Practice for Software Design Descriptions"

IEEE 1028-1988 "Standard for Software Reviews and Audits"

IEEE 1050-1989, "IEEE Guide for Instrumentation and Control Equipment Grounding in Generating Stations"

IEEE 1228-1991 "Standard for Software Safety Plans"

IEC 880, "Software for Computers in Safety Systems of Nuclear Power Stations"

ASME NQA-2a-1990, Part 2.7, "Quality Assurance Requirements of Computer Systems for Nuclear Facility Applications, American Society of Mechanical Engineers"

MIL-STD-461(A, B, C), "Electro-magnetic Emission and "Susceptibility Requirements for the Control of Electro-magnetic Interference"

MIL-STD-462, "Electro-magnetic Interference Characteristics Measurement"

SAMA PMC 33.1-1978, "Electro-magnetic Susceptibility of Process Control Instrumentations"

EPRI Report TR-102323 "Guide to Electromagnetic Interference (EMI) Susceptibility Testing for Digital Safety Equipment in Nuclear Power Plants"

MIL-STD-1399, "Interface Standard for Shipboard Systems, DC Magnetic Field Environments"

IEEE 12207, "Standard for Information Technology – Software Lifecycle Processes"

MIL-STD-498, "Software Development and Documentation"

APPENDIX B

Revision History For IP 52003

Commitment Tracking Number	Issue Date	Description of Change	Training Needed	Training Completion Date	Comment Resolution Accession Number
NA	10/31/08 CN 08-031	<p>Conducted 4 year commitment search and found none.</p> <p>New inspection procedure (IP) which combines the previous IP 52001, "Digital Retrofits Receiving Prior Approval" and IP 52002, "Digital Retrofits Not Receiving Prior Approval."</p>	No	N/A	ML082200119