OPERATING EXPERIENCE SMART SAMPLE (OpESS) 2023/01

DIGITAL INSTRUMENTATION AND CONTROLS

CORNERSTONE: INITIATING EVENTS
MITIGATING SYSTEMS
BARRIER INTEGRITY

APPLICABILITY:

- This voluntary OpESS applies to all licensed operating commercial nuclear reactors.
- This OpESS supplements and supports informing sample selection for Inspection Procedures (IP) 71111.18, 71111.24, 71111.21M, 71111.21N.03, 71111.21N.04, 71130.10, and 71152.

OpESS 2023/01-01 OBJECTIVES

01.01 Provide support to baseline inspection activities in the area of digital instrumentation and controls (I&C) systems and modifications.

01.02 Provide examples where deficiencies may be present in digital I&C equipment in order to inform the inspection of design, modification, and maintenance activities.

OpESS 2023/01-02 BACKGROUND

02.01 Digital Instrumentation and Controls Implementation

Digital technology offers significant operational and maintenance benefits for I&C systems of nuclear power plants (NPPs). Digital I&C systems consist of both hardware components and logic elements (e.g., software). Hardware components in digital I&C systems are susceptible to failures similar to those considered for analog systems. In this guidance, the term “software” refers to software, firmware, and logic developed from software-based development systems (e.g., hardware description language programmed devices).

The application of digital technology to the design and configuration of NPP safety and important to safety systems requires careful consideration of NRC guidance pertaining to safety system architecture, failure modes and effect analysis, and the application of defense-in-depth principles.

02.02 Operating Experience

Past digital I&C related audit and inspection activities have identified licensee issues with establishing and maintaining the design control, maintenance, and testing of digital

I&C equipment. In some cases, issues identified were associated with reviewing changes to verify that a license amendment was not necessary.

Examples of licensee performance issues include:

Shearon Harris Nuclear Power Plant, March 2013

The licensee performed a review but erroneously concluded that the change could be implemented without performing a formal 10 CFR 50.59 evaluation and without obtaining a license amendment. Specifically, in the spring of 2012, Shearon Harris failed to perform a 10 CFR 50.59 evaluation that was sufficient to demonstrate that a license amendment was not required prior to replacing the original solid state protection system (SSPS) circuit boards with boards using complex programmable logic device (CPLD) technology. The violation was due in part to the licensee's misinterpretation of the Nuclear Energy Institute (NEI) 01-01 guidance. With the replacement of the SSPS boards, the licensee implemented a change that did not adequately evaluate and document that they did not create the possibility of a software common-cause failure (CCF) in the reactor protection system (RPS) and engineered safety features actuation systems (ESFAS) that had not previously been evaluated in the Updated Final Safety Analysis Report (UFSAR). The licensee failed to recognize that the software used in the replacement boards had the potential to adversely affect the design functions of the SSPS.

The results of the inspection can be viewed in Inspection Report (IR) 05000400/2013002 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML13120A340) and IR 05000400/2013009 (ML13224A290).

Susquehanna Steam Electric Station, August 2011 and November 2012

The licensee experienced numerous reactor trips and downpowers during the implementation of their digital Integrated Control System (ICS), a digital feedwater and level control system. One instance occurred when Unit 2 automatically scrammed from 100 percent power due to a main turbine trip. The main turbine trip occurred during the performance of the quarterly functional test of the feedwater/main turbine trip system associated with reactor vessel water level channels. The test was being performed for the first time since the 2011 upgrade of the Unit 2 feedwater level control system with a digital ICS. As part of the test, operations personnel transferred the reactor water level input signal from average level to narrow range 'B' biased as required by the procedure. The main turbine and feedwater trip system design uses three narrow range reactor water level channels in a two-out-of-three trip logic. When the first narrow range reactor water level channel ('2A') was tested, an unexpected automatic main turbine trip occurred. The direct cause was an incorrectly terminated internal jumper. The wiring anomaly in the ICS Level 8 turbine trip logic circuitry resulted in one of the Level 8 trip logic contacts being jumpered out of the channel trip circuitry, causing a Unit 2 main Turbine Trip from the initiation of one single channel instead of the designed two-out-of-three channel logic.

This event is captured in Licensee Event Report 2011-003-00 (ML112920131). The results of this inspection can be viewed in IR 05000388/2011004 (ML113120409) and 05000388/2011005 (ML12045A383).

Another instance was documented for the failure to evaluate operating experience for the ICS when Unit 2 lost control of reactor vessel level on November 9, 2012, requiring insertion of a manual scram. The cause of the loss of level control was the lockup of one of the two ICS network switches due to a data storm, a condition which had been described in various operating experience communications from April 2007 through September 2012.

The results of this inspection can be viewed in Inspection Report (IR) 05000388/2013011 (ML13322B321).

Summary

The examples of digital I&C equipment performances above are provided to support the need for inspectors to conduct baseline inspection activities in the areas of digital I&C equipment design, maintenance, and testing.

OpESS 2023/01-03 INSPECTION GUIDANCE

The following inspection guidance may be applied, as appropriate, to support baseline inspection activities. Inspector judgment should be used when determining the extent to which the OpESS should be used to inform inspection activities under the applicable baseline IPs.

03.01 Design Control

The recommended inspection activity described below supports IP 71111.21M, "Comprehensive Engineering Team Inspection (CETI)."

a. General

1. Review conditions or deficiencies affecting digital I&C and verify that corrective actions are prompt and correct the condition adverse to quality.

2. Verify that the licensee identifies the cause of the conditions or deficiencies associated with significant condition adverse to quality affecting digital I&C equipment and takes sufficient corrective measures to prevent repetition.

3. Verify that the digital component has the ability to perform its safety functions, as-designed and as-built, by reviewing qualification testing, post-maintenance testing, and in-service testing.

4. Verify that the Quality Assurance (QA) program, and equipment qualification (environmental, seismic, and electromagnetic interference (EMI)/radio frequency interference (RFI)) requirements are met.

b. Design

1. If preventative maintenance and/or testing is performed by a licensee's vendor, how is the licensee providing oversight of the vendor?

(a) Verify that applicable administrative or regulatory requirements are specified in procurement documents/vendor contracts/work orders and comply with digital I&C equipment functions.

2. Verify adequate diversity and defense in depth against common-cause failure reviews have been performed.

3. Review procedures, work orders, surveillance testing, and maintenance testing for deviations from acceptance criteria and vendor manuals.

4. Setpoints (Regulatory Guide (RG) 1.105, “Setpoints for Safety-Related Instrumentation”)

   (a) Verify that instrumentation to monitor variables and systems over their anticipated ranges for accident conditions is appropriate to ensure adequate safety (General Design Criteria (GDC) 13, “Instrumentation and Control”).

   (b) Verify protection systems be designed to initiate operation of appropriate systems to ensure that specified acceptable fuel design limits are not exceeded (GDC 20, “Protection System Functions”).

   (c) Verify maintenance of instrument channels implementing these setpoints ensures they are functioning as required and consistent with plant technical specifications.

c. For critical equipment failing to perform a critical safety function, such as reactivity control, core heat removal, reactor coolant inventory, containment isolation, and containment integrity.

   1. Review the Requirements Traceability Matrix (RTM) from licensee’s initial change package and review how that function was tested during design, installation, and testing. Note: smaller modifications would not have an RTM.

   2. If equipment fails due to EMI/RFI, verify proper level of analysis for digital equipment. See RG 1.180, “Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems.”

   3. If a failure of equipment due to human factors is suspected discuss with license the difference in human actions to be taken before and after the modifications. This also applies to information being provided to the personnel and whether it changed after the modification.

03.02 Testing and Maintenance of Equipment Important to Risk

The recommended inspection activity described below supports IP 71111.24, “Testing and Maintenance of Equipment Important to Risk.”

a. Review Plans for Maintenance and Testing

   1. Verify maintenance and testing procedures are updated, and correctly reflect the system attributes to be verified.

      (a) Review the licensee’s maintenance and testing procedures, vendor guidance, and applicable industry standards to ensure they correctly reflect system attributes and met licensing commitments.

(b) Verify test procedures include or reference test objectives, test requirements, applicable prerequisites, and acceptance criteria contained in the applicable technical documents.

(c) Review procedures, calculations, and design documents to verify that setpoints and related uncertainty terms have been adequately evaluated and included in maintenance activities and procedures.

(d) Ensure maintenance and testing frequency is determined based on equipment type and expected use.

(e) Verify deviations from guidance or vendor recommendations have technical justification. Verify assumptions in justification remain valid.

(f) Verify that electrostatic discharge (ESD) precautions and considerations have been incorporated into procedures and are followed.

2. Assess the implementation of the technical specifications (TS), applicable licensee standards, vendor recommendations in the maintenance, and testing and calibration procedures.

3. Verify if the licensee implemented procedures for ensuring that stored parts will be correctly handled (e.g., ensuring stored chips with embedded software are the correct revision).

4. Review the licensee's plans for repair activities.

(a) Determine if the licensee intends to repair specific boards, or if boards will be returned to the vendor for repair.

(b) Review the licensee's test equipment calibration, the frequency of board testing, and oversight of vendors.

5. Review training documents and interview personnel to verify that operators, technicians, and system engineers had been adequately trained and understand the system commensurate with their responsibilities and maintenance activity.

b. Equipment Maintenance and Testing Activities

1. Observe real-time maintenance, testing, and post-maintenance testing; conduct interviews of maintenance and test personnel to verify qualifications.

2. Review testing conditions to ensure the conditions are similar to how they will be used and properly challenge the critical functions.

3. Verify that cabinet ventilation devices are properly maintained.

4. If the licensee will be performing board-level repair activities, verify that the vendor manuals and drawings contain adequate detail and that maintenance personnel involved in board repair have been trained. If the licensee will be using vendor repair activities, verify that an adequate supply of spare boards is available on site.

5. 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 volatile and non-volatile memory.

6. Is the device a critical digital asset (CDA)? Assess whether the cybersecurity controls specified in the licensee's cybersecurity plan were appropriately applied and remain adequate for the CDA.

7. Verify that the licensee performed ongoing monitoring and assessment (OM&A) activities at a prescribed frequency to verify that the cybersecurity controls implemented on CDAs remain in place.

8. Verify that the licensee performs vulnerability assessments or scans as described in their cybersecurity procedures.

c. If preventative maintenance and/or testing is performed by licensee's vendor, how is the licensee providing oversight of the vendor?

1. Verify that any applicable administrative or regulatory requirements are specified in procurement documents/vendor contracts/work orders and comply with the digital I&C equipment functions.

2. Verify that appropriate facility personnel, including contractors, are aware of cybersecurity requirements, and receive the training necessary to perform their assigned duties, and responsibilities.

d. Verify that the licensee ensures that personal relied upon to maintain equipment are familiar with the equipment operation and requirements.

03.03 Plant Modifications

The recommended inspection activity described below supports IP 71111.18, "Plant Modifications."

a. Temporary and Permanent Modifications

1. Review what guidance was used for the 50.59 screening and evaluation process. NEI 96-07 Appendix D, "Supplemental Guidance for Application of 10 CFR 50.59 to Digital Modifications" endorsed by RG 1.187 provides one method. If NEI 96-07 Appendix D was not used, determine what guidance was used.

2. Verify that an adequate 50.59 evaluation was performed to determine whether a license amendment is required.

3. Review and verify that a cybersecurity screening was performed to determine the classification of the digital I&C asset.

4. Review the cybersecurity screening to ensure that the digital asset is appropriately classified (e.g., CDA or Non-CDA).

5. Verify that a digital asset classified as a Non-CDA is accurately classified in accordance with NEI 10-04, "Identifying Systems and Assets Subject to the Cyber Security Rule."

6. Verify that the modification included an EMI/RFI review.

7. Determine if the modification is an analog to digital modification?

   (a) If so, ensure likelihood of a failure has not increased or is addressed.

   (b) Ensure the 50.59 screening addresses CCF if two pieces of equipment are the same type and perform the same function.

8. Review the RTM for large modifications to see the key safety functions and how they were tested in the modification.

9. Review if digital modification impacts the cornerstones and ensure it does not adversely affect them.

10. Determine if the modification affects the control room or critical systems that require an evaluation by other technical disciplines (e.g., structural, mechanical, human factors, etc.).

11. Verify functional areas affected by the modification have had an opportunity to evaluate the design prior to installation (e.g., fire protection, design engineering, system engineering, emergency preparedness, operations, etc.).

b. Permanent Modifications Only

1. Verify that the licensee is implementing the required cybersecurity controls on CDAs in accordance with NEI 13-10, “Cyber Security Control Assessments.”

2. Reference NEI 08-09, “Cyber Security Plan for Nuclear Power Reactors,” section 3.1.6 to verify that if the license is implementing alternate security controls for a CDA per section 3.1.6 of the licensee’s cybersecurity plan, and that such alternate controls provide at least the same protection as the required security controls.

3. Verify that the licensee performs an analysis and documents their justification demonstrating that any cybersecurity controls the licensee decided not to implement are not necessary.

4. Verify that defense-in-depth protective strategies have been implemented, documented, and are maintained per the licensee’s cybersecurity plan to ensure the capability to detect, delay, respond to, and recover from cyberattacks on CDAs.

5. Verify that the licensee has established a program per the licensee’s cybersecurity plan to ensure that CDAs are continuously protected from cyberattacks including implementing any necessary measures to address new vulnerabilities.

6. Verify that the licensee is controlling physical access to the CDAs independent of the physical access controls for the facility.

7. Verify that only qualified and authorized individuals obtain access to CDAs and individuals that are authorized to modify CDA configurations are trained and qualified to perform the modifications.

8. Verify that the licensee updated affected procedures and review how the licensee ensures that all affected procedures have been correctly updated.

9. 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, verify that the process is underway, and is properly planned and proceeding in a timely manner.

03.04 Cybersecurity

The recommended inspection activity described below supports IP 71130.10, "Cybersecurity."

a. Verify that the licensee has performed an adequate security impact analysis prior to making changes to critical systems and CDAs to manage the cyber risk resulting from the changes.

b. Verify that the licensee has implemented appropriate supply chain and services acquisition controls for new and/or replacement CDAs.

c. Verify documentation for any technical security controls (Appendix B of RG 5.71, "Cyber Security Programs for Nuclear Facilities," or Appendix D of NEI 08-09) implemented in the design of a CDA that will be used by the licensee to fulfill requirements in accordance with the licensee's CSP.

d. Verify the following applicable information is documented by the licensee for acquired CDAs:

1. secure configuration, installation, and operation of the CDA;

2. effective use and maintenance of security features/functions;

3. known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions;

4. user-accessible security features/functions and how to effectively use those security features/functions;

5. methods for user interaction with CDA, which enables individuals to use the system in a more secure manner; and

6. user responsibilities in maintaining the security of the CDA.

03.05 Commercial Grade Dedication

The recommended inspection activity described below supports 71111.21N.03, "Commercial Grade Dedication."

Guidance from RG 1.250, "Dedication of Commercial Grade Digital Instrumentation and Control Items for Use in Nuclear Power Plants," and EPRI TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," should be considered when performing the inspection activity.

a. Verify that a technical evaluation has been performed to establish the digital component's safety function, performance requirements, component functional classification, and application requirements.

b. Verify whether a failure modes and effects analysis exist for the digital component that identifies possible failure modes.

c. Verify that critical characteristics, i.e., important design, material, and performance characteristics, have been identified and the basis for selection of the critical characteristics should be consistent with the information from items a and b above.

d. Verify that appropriate verification method(s) for each critical characteristic have been identified. In smaller modifications this would involve testing of system parameters such as flow, level, or recording.

e. Verify that acceptance criteria for the verification method used is consistent with the plant-specific application of the digital component.

03.06 Age-Related Degradation

The recommended inspection activity described below supports IP 71111.21N.04, "Age-Related Degradation."

a. Verify that engineering performance and maintenance activities to address age-related degradation for structures and components (SCs) are conducted in a manner that provides reasonable assurance of the safe operation of the plant.

b. Determine the intended safety function credited to address age-related degradation.

c. Verify age-related degradation for plant SCs are appropriately identified, addressed, and corrected.

d. Review FSAR, vendor documents, health reports, maintenance/surveillance testing, and engineering evaluations.

e. Review 10 CFR Part 21 reports, site specific functional failures, performance indicators, and corrective actions for digital I&C components and systems.

03.07 Problem Identification and Resolution

The recommended inspection activity described below supports IP 71152, "Problem Identification and Resolution," and IP 71111.21M, "Comprehensive Engineering Team Inspection," as applicable.

a. For selected items related to digital I&C in the Corrective Action Program (CAP), assess the following items.

1. Verify issues are identified, prioritized, and adequately evaluated per the licensee's corrective action program (CAP) and associated procedures.

2. Verify corrective actions are taken in a timely manner per the licensee's CAP and associated procedures.

b. For operating experience reviews of digital I&C systems and components, assess the following items.

1. Verify that conditions discussed in the operating experience either are not applicable or have been adequately addressed to ensure that digital I&C equipment functions are maintained.

2. Verify any corrective actions are taken in a timely manner per licensee procedures.

3. Verify that for conditions affecting digital I&C equipment, the extent of condition is reviewed when applicable.

OpESS 2023/01-04 REFERENCES

These references may include pre-decisional information contained on NRC internal websites. Once the agency has formally evaluated an operating experience issue and has determined that it meets the criteria for agency action, the NRC communicates the issue to the public and the industry through one or more appropriate methods (e.g., generic communication, rulemaking public comment periods, etc.)

04.01 Inspection Manual Chapters and Procedures

IP 71111.18, “Plant Modifications”

IP 71111.21M, “Comprehensive Engineering Team Inspection”

IP 71111.21N.03, “Commercial Grade Dedication”

IP 71111.21N.04, “Age-Related Degradation”

IP 71111.24, “Testing and Maintenance of Equipment Important to Risk”

IP 71130.10, “Cybersecurity”

IP 71152, “Problem Identification and Resolution”

04.02 Correspondence

Information Notice 2019-04, “Effective Cyber Security Practices to Protect Digital Assets of Byproduct Materials Licensees,” (ML18044A350)

04.03 Other Reference Material

Institute of Electrical and Electronics Engineers (IEEE) 100, “The Authoritative Dictionary of IEEE Standards Terms,” IEEE, Piscataway, NJ

IEEE Std 279-1968, “Proposed IEEE Criteria for Nuclear Power Plant Protection Systems,” Piscataway, NJ

IEEE Std 279-1971, “Criteria for Protection Systems for Nuclear Power Generating Stations,” Piscataway, NJ

IEEE Std 379-2000, “IEEE Standard Application of the Single Failure Criterion to Nuclear Power Generating Station Safety Systems,” Piscataway, NJ

IEEE Std 603-1991, “IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations,” Piscataway, NJ

IEEE Std 603-1991 Correction Sheet, “Standard Criteria for Safety Systems for Nuclear Power Generating Stations,” January 30, 1995

U.S. NRC Regulatory Guide (RG) 1.62, “Manual Initiation of Protective Actions,” Revision 1

NUREG-0493, “A Defense in Depth and Diversity Assessment of the RESAR414 Integrated Protection System”

RG 1.30, “QA Requirements for the Installation, Inspection, and Testing of Instrumentation and Electric Equipment”

RG 1.53, “Application of the Single Failure Criterion to Safety Systems”

RG 1.152, “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants”

RG 5.71, “Cyber Security Programs for Nuclear Facilities”

RG 1.187, “Guidance for Implementation of 10 CFR 50.59, Changes, Tests, and Experiments”

NUREG-0800, Section 7.1-T, “Regulatory Requirements, Acceptance Criteria, and Guidelines for Instrumentation and Control Systems Important to Safety”

NUREG-0800, Section 7.7, “Control Systems”

NUREG-0800, Section 7.8, “Diverse Instrumentation and Control Systems”

NUREG-0800, Section 13.6.6, “Cyber Security Plan”

NUREG-0800, Chapter 15, “Transient and Accident Analysis”

NUREG-0800, Chapter 18, “Human Factors Engineering”

NUREG-0800, Appendix 7.0-A, “Review Process for Digital Instrumentation and Control Systems”

NUREG-0800, BTP 7-17, “Guidance on Self Test and Surveillance Test Provisions”

NUREG-0800, BTP 7-19, “Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based I&C Systems”

NUREG-0800, BTP 7-21, “Guidance on Digital Computer Real-Time Performance”

NUREG-1764, “Guidance for the Review of Changes to Human Actions,” Revision 1

SECY-91-0292, “Digital Computer Systems for Advanced Light Water Reactors,” September 16, 1991

NUREG/CR-7007, “Diversity Strategies for Nuclear Power Plant Instrumentation and Control Systems”

NUREG/CR-6303, “Method for Performing Diversity and Defense in Depth Analyses of Reactor Protection Systems”

SECY-93-087, “Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light Water Reactor (ALWR) Designs,” April 2, 1993

SRM-SECY-93-087, “Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light Water Reactor (ALWR) Designs,” July 21, 1993

SECY-18-0090, “Plan for Addressing Common Cause Failure in Digital Instrumentation and Controls,” September 12, 2018

U.S. NRC Generic Letter (GL) 85-06, “Quality Assurance Guidance for ATWS Equipment That is Not Safety Related,” April 16, 1985

U.S. NRC Regulatory Issue Summary (RIS) 2002-22, Supplement 1, “Clarification on Endorsement of Nuclear Energy Institute Guidance in Designing Digital Upgrades in Instrumentation and Control Systems,” May 31, 2018

NEI 01-01/EPRI TR-102348, “Guideline on Licensing of Digital Upgrades”

Nuclear Energy Institute, NEI 96-07, Appendix D, Supplemental Guidance for Application of 10 CFR 50.59 to Digital Modifications,” Revision 1, May 2020

OpESS 2023/01-05 REPORTING RESULTS/TIME CHARGES/ADDITIONAL ISSUES

If information from this OpESS is used to inform a baseline inspection sample, reference the OpESS number in the scope section of the report.

In addition, if any findings or violations are identified in conjunction with this OpESS, include a statement similar to the following in the description section of the finding write-up:

> “This finding was identified in connection with a review of Operating Experience Smart Sample (OpESS) 2023/01.”

Inspection time for this OpESS is to be charged to the normal baseline procedure under which it is being used and the level of effort is expected to be within normal baseline inspection sample resource estimates.

OpESS 2023/01-06 CONTACTS

For technical support regarding the performance of this OpESS and emergent issues, contact: Shiattin Makor (RIV/DORS/EB2) at 817-200-1507 or shiattin.makor@nrc.gov, or Julie Winslow (NRR/DRO/IOEB) at 301-415-0593 or julie.winslow@nrc.gov.

Appendix A – Table of regulatory and licensing basis for various components and inspection procedures

OpESS Sections	Inspection Procedure	Technical Area	Regulatory Guide	Standard or Industry Document
03.01	IP 71111.21M	Criteria for Safety Systems	RG 1.153, Rev. 1	IEEE Std 603-1991
03.01	IP 71111.21M	Criteria for Safety Systems - Bypass. & Inoperable Indication	RG 1.47, Rev. 1	N/A
03.01	IP 71111.21M	Criteria for Safety Systems - Manual Initiation	RG 1.62, Rev. 1	N/A
03.01	IP 71111.21M	Criteria for Safety Systems - Independence	RG 1.75, Rev. 3	IEEE Std 384-1992
03.01	IP 71111.21M	Criteria for Safety Systems - Single-Failure Criterion	RG 1.53, Rev. 2	IEEE Std 379-2000
03.02	IP 71111.24	Criteria for Safety Systems - Periodic Testing of Actuation Functions	RG 1.22, Rev. 0	N/A
03.02	IP 71111.24	Criteria for Safety Systems - Periodic Testing of Electric Power	RG 1.118, Rev. 3	ANSI/IEEE Std 338-1987
03.01 03.02	IP 71111.21M IP 71111.24	Criteria for Safety Systems - QA Installation, Inspection and Testing	RG 1.30, Rev. 0	IEEE Std 336-1971
03.04	IP 71130.10	Criteria for Safety System Programmable Digital Devices	RG 1.152, Rev. 4 and DG-1374 (Rev 4 of 1.152) NEI 08-09	IEEE Std 7-4.3.2-2003
03.04	IP 71130.10	Digital Development and Reliability – Verification and Validation	RG 1.168, Rev. 2 NEI 08-09	IEEE Std 1012-2004 and IEEE Std 1028-2008

OpESS Sections	Inspection Procedure	Technical Area	Regulatory Guide	Standard or Industry Document
03.04	IP 71130.10	Digital Development and Reliability – Configuration Management	RG 1.169, Rev. 1 NEI 08-09	IEEE Std 828-2005
03.04	IP 71130.10	Digital Development and Reliability - Software Test Documentation	RG 1.170, Rev. 1 NEI 08-09	IEEE Std 829-2008
03.04	IP 71130.10	Digital Development and Reliability - Software Unit Testing	RG 1.171, Rev. 1 NEI 08-09	ANSI/IEEE Std 1008-1987
03.04	IP 71130.10	Digital Development and Reliability - Software Requirements Specification	RG 1.172, Rev. 1 NEI 08-09	IEEE Std 830-1998
03.04	IP 71130.10	Digital Development and Reliability - Software Life Cycle Processes	RG 1.173, Rev. 1 NEI 08-09	IEEE Std 1074-2006
03.01	IP 71111.21M	Equipment Qualification - (Harsh Environment)	RG 1.89, Rev. 1 and DG-1361 (Rev 2 of 1.89)	IEEE Std 323-1974 (Soon: IEC/IEEE Std. 60780-323)
03.01	IP 71111.21M	Equipment Qualification - Seismic	RG 1.100, Rev. 4	IEEE Std 344-2013, IEEE Std C37.98-2013, and ASME QME-1-2017
03.01	IP 71111.21M	Equipment Qualification - EMI/RFI	RG 1.180, Rev. 2	IEEE Std 1050-2004, IEEE Std C62.41.1-2002, IEEE Std C62.41.2-2002, IEEE Std C62.45-2002, MIL-STD-461G, IEC 61000-3, IEC 61000-4, IEC 61000-6
03.01	IP 71111.21M	Equipment Qualification - Computer Based I&C (Mild Environment)	RG 1.209, Rev. 0	IEEE Std 323-2003

OpESS Sections	Inspection Procedure	Technical Area	Regulatory Guide	Standard or Industry Document
03.05	IP 71111.21N.03	Commercial Grade Dedication	RG 1.164, Rev. 0	EPRI 3002002982, Revision 1 to EPRI NP-5652 and TR-102260
03.05	IP 71111.21N.03	Commercial Grade Dedication - Digital Equipment	SE dated 7/17/97	EPRI TR-106439
03.05	IP 71111.21N.03	Commercial Grade Dedication - PLC	SE dated 1/9/98	EPRI TR-107330
03.05	IP 71111.21N.03	Commercial Grade Dedication - SIL Certification	RG 1.250, Rev. 0	NEI 17-06, Rev. 1
03.05	IP 71111.21N.03	Commercial Grade Dedication – Design and Analysis Programs	RG 1.231, Rev. 0	EPRI TR-1025243, Rev. 1
03.01	IP 71111.21M	Accident Monitoring Instrumentation	RG 1.97, Rev. 5	IEEE Std 497-2016
03.01 03.02	IP 71111.21M IP 71111.24	Setpoints	RG 1.105, Rev. 4	ANSI/ISA 67.04.01-2018 (endorsed) and RP 67.04.02 ("contains useful information")
03.01 03.02	IP 71111.21M IP 71111.24	Instrument Sensing Lines	RG 1.151, Rev. 2	ANSI/ISA-67.02.01-2014 and IEEE Std 622-1987
03.04	IP 71130.10	Cyber Security - Programs	RG 5.71, Rev. 1 NEI 08-09	N/A
03.04	IP 71130.10	Cyber Security - Event Notifications	RG 5.83, Rev. 0 NEI 08-09	N/A
03.03	IP 71111.18	10 CFR 50.59	RIS-02-2002, Supplement 1	NEI 01-01

Attachment 1: Revision History for OpESS 20xx-01

Commitment Tracking Number	Accession Number Issue Date Change Notice	Description of Change	Description of Training Required and Completion Date	Comment Resolution and Closed Feedback Form Accession Number (Pre-Decisional Non-Public Information)
	ML23235A248 02/12/24 CN 24-007	Initial issuance to provide support for initial baseline inspection activities in the area of digital instrumentation and controls.		ML23237B248