INSPECTION PROCEDURE 52002

DIGITAL RETROFITS NOT RECEIVING PRIOR APPROVAL

PROGRAM APPLICABILITY: 2515

SALP FUNCTIONAL AREA: MAINTENANCE (MAINT)

52002-01 OBJECTIVES

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

01.02 To ensure that the licensee has properly addressed the regulatory requirements of 10 CFR 50.59 regarding the existence of an unreviewed safety question for the digital upgrade.

01.03 To assess digital system failures, modifications, and maintenance issues for their affect on the system function, and for potential generic concerns.

52002-02 INSPECTION REQUIREMENTS

02.01 Advance Preparation. Review the following applicable documents before the start of the inspections. Be familiar with the licensee's administrative programs for designing, installing, testing, and maintain modifications; also be familiar with the type of digital system being installed.

a. Final Safety Analysis Report (FSAR).

b. Technical Specifications (TS).

c. Descriptions of the proposed modifications.

d. The 10 CFR 50.59 evaluation for the digital system modifications.

e. Any licensing commitment documents concerning this modification.

f. Licensee Software Quality Assurance Program.

g. Manufacturer literature on the vendor hardware and software being installed.

02.02 Conduct of the Inspection

The following are major topic areas that should be considered for review by the inspector. The list is not all inclusive, and should be interpreted as potential major focal points of the inspection.

a. Determine the full scope of the digital I&C system upgrade.

b. Review the 10 CFR 50.59 analysis performed by the licensee to address the existence of an unreviewed safety question.

c. Verify that the modification is designed in accordance with the plant licensing design basis, and that the post-modification testing performed by the licensee adequately demonstrates that the digital system's installed configuration meets the design basis.

d. Verify that plant drawings, the Safety Analysis Report, and other relevant documentation has been updated to reflect the replacement system.

e. Verify that maintenance, surveillance, abnormal operating, emergency operating and annunciator response procedures have been updated, and correctly reflect the new system attributes.

f. Verify that the as-installed system is consistent with design drawings.

g. Verify that the operators, technicians, and system engineers have been adequately trained, and have an understanding of the system commensurate with their responsibilities.

h. 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.

I. Inspect the installation environment and verify that the licensee specified environmental parameters accurately reflect the installation environment.

j. Verify that the EMI/RFI qualifications of the digital equipment are sufficient to ensure proper operation in the actual EMI/RFI environment in which it will be used.

k. Verify the adequacy and quality of the power and grounding system for the modification.

l. Review the software quality control, configuration management, and general software quality documentation for proper demonstration of compliance with the requirements of 10 CFR Part 50, Appendix B.

m. 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.

n. Verify that proper indication and/or annunciation is provided for system bypass and failure.

o. Verify that the handling and storage requirements of spare system parts are consistent with manufacturer and licensee requirements (periodic power-up, battery life, etc.).

p. Verify that any change to the human-system interface design reflects stat-of-the-art human factors principles including compatibility with the remainder of the control room or local control stations.

52002-03 INSPECTION GUIDANCE

General Guidance

Future trends are toward increased use of computer based designs to encompass more plant instrumentation and control (I&C) functions and to ensure that the latest I&C requirements are met. An important consideration for these applications is computer architectural designs that permit easy change or addition, thus minimizing equipment obsolescence. These trends affect safety system functions in many applications in nuclear power plants.

With the proper hardware and software design, the use of digital systems in instrument control can provide excellent functional performance while allowing for rapid, minimum impact changes in instrument function when needed. Incorporating new computer based technology within safety-related system nuclear power plants can introduce a positive potential for improving overall system performance, while at the same time creating a potential for introducing new system failure modes within the computer software architecture.

Software presents a unique problem in that software failures do not follow the traditional failure profiles, i.e., the bathtub curve, associated with analog or mechanical systems. Since there is no component wear or manufacturing tolerance, any potential failures in the software are present at installation, and are identical in each channel into which identical software is used. For this reason, review of the development process, in addition to an inspection of the end result of that development process is necessary to assure that the software being used will perform the intended function.

This inspection procedure applies in cases where a digital upgrade has been installed under the requirements of 10 CFR 50.59 without prior NRC staff approval. Therefore, the inspector will verify (1) that the digital system design issues have been properly addressed by the licensee, (2) that the requirements of 10 CFR 50.59 for the existence of an unreviewed safety question have been properly addressed, and (3) that system failures and modifications have been

properly addressed and implemented. Guidance contained in Generic Letter 95-02, "Use of NUMAC/EPRI Report TR-102348 `Guidance on Licensing Digital Upgrades' in determining the acceptability of performing analog-to-digital replacements under 10 CFR 50.59", dated April 26, 1995 can be used in performing these determinations.

Because of the complexity of digital systems, close coordination with NRR is recommended for a successful inspection. The inspector should contact NRR for advice and recommendations on issues and concerns as appropriate.

Specific Guidance

03.01 Advanced Preparation. No guidance provided.

03.02 Conduct of the inspection

a. This review should include drawings, schematics, and licensee review documents.

   1. Describe 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. Compare the 10 CFR 50.59 analysis for consistency against licensee procedures for such evaluations. When reviewing the 10 CFR 50.59 determination of no unreviewed safety question, ensure that the determination was appropriate for this plant-specific digital upgrade. Was common mode software failure and its consequences considered? Was the determination made using EPRI TR-102348 as a guide?

   1. Examine the internal system architecture and its interconnections with external systems. Did the licensee perform a review of possible single failures that may affect more portions of the system than analyzed for the original system?

   2. Determine what method the licensee uses to determine when the hardware and/or software is not working.

3. What are the possible hazards that would influence the system hardware, software and interfaces in such a way as to cause incorrect or unsafe operation? Are there defenses against these hazards?

4. Are there errors that a user or maintainer could make that could disable or cause a malfunction, and if so, what defenses against these hazards are in place?

5. Verify that any changes made to the system since the 50.59 evaluation were adequately evaluated, and have not invalidated the conclusions of that 50.59 evaluation.

c. During the verification that the modification is designed in accordance with the plant licensing design basis and that the post-modification testing demonstrates this:

1. Verify that the licensee analyzed the affect of the system replacement on related issues such as Regulatory Guide 1.97, Station Blackout (10 CFR 50.63), Anticipated Transients Without Scram (10 CFR 50.62), 10 CFR 50 Appendix R, and the Safety Parameter Display System to ensure consistency with the plant licensing basis.

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. Determine if there are any test units or data loggers connected to the system for extended periods of time (e.g., monitoring, troubleshooting, etc.)? In what modes and how are they connected? Are they connected through qualified isolation devices?

5. Determine what post installation testing was performed following the modification. Did the digital system vendor perform a site acceptance test, and if so, did the licensee review and approve the test plan and procedure, and review the results of the test?

6. Verify that post installation test was adequate to prove that the design basis was met. Did all correct trip outputs occur for the correct input logic combinations? Were all safety functions and combinations tested?

7. Verify that local and remote alarms indicating degraded conditions were tested during the post installation testing.

8. Verify that the post installation testing include overall time response testing to demonstrate that the actual

system response times meet the requirements of the accident analysis.

9. Verify that system outputs fail safe on loss of power for those digital systems that provide inputs to safety related functions.

d. In those cases where the update to the Safety Analysis Report and other relevant documentation has not been completed, insure that the process is underway, and is properly planned and proceeding in a timely manner.

e. During the procedures review:

1. Verify that the licensee updated affected procedures. How did the licensee ensure 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. Did 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 technical specifications, 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 insure complete testing.

5. Determine if the licensee intends to repair specific boards, or will be returning the boards to the vendor for repair. If the licensee will be performing board repair activities, verify that the vendor manuals and drawings contain adequate details. 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 RAM.

6. 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.

7. Determine how any PCS, portable configurators, or other computer interface test equipment are controlled, i.e., physical protection, virus protection, password control, and personnel access. Is this control adequate for security and is it sufficiently self-checking to minimize the introduction of errors?

8. Verify that applicable 10 CFR Part 21 Notifications, Bulletins, Generic Letters, and Information Notices were correctly applied to the replacement system.

9. Verify that relevant manufacturer recommendations have been correctly incorporated and that there is a system in place to track manufacturer recommendations.

10. Verify that electro-static discharge (ESD) precautions and considerations have been incorporated into relevant procedures and are followed.

11. Verify that EMI/RFI precautions are incorporated into procedures and followed.

12. Verify that cabinet ventilation devices are properly maintained.

f. During the review of the as-installed system for consistency with the design drawings:

1. Verify that signs are posted limiting the use of radio equipment near the system, and that this policy is enforced.

2. Verify that there are no radio and/or microwave sources nearby that may affect the system.

3. Verify that the cable routing scheme (how cables are mixed, how cables are run, etc.) is consistent with the 50.59 evaluation and any applicable manufacturer recommendations.

4. Verify that there are procedures to insure that the software loaded into the system is actually the intended software, and any corruption during initial download or during surveillance can be detected.

g. 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 insure they have an understanding of the system commensurate with their responsibilities. If the licensee does not intend to maintain the system, what control does the licensee exercise over the vendor with respect to design control, access, and software configuration?

h. During the hardware and software failures review:

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.

I. The environmental qualifications review should address the following:

1. Did the licensee specify the environmental qualification parameters, e.g., 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. Was vendor testing 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?

j. The EMI/RFI qualifications review should address the following:

1. Was factory EMI/RFI testing performed on the system? What standards were used by the vendor? What frequency ranges and signal strengths were covered in the testing?

2. Did the licensee specify that EMI/RFI qualification was needed? What was the specification and how was it developed?

3. 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?

4. Did the licensee perform any field measurements of EMI/RFI at the installation location, or reference EPRI Report TR-102323? Did the licensee consider whether the installed system would create an EMI concern for other systems?

5. Do the licensee specified EMI parameters accurately reflect the installation environment?

6. Are radio and/or radio telephone restrictions at the installed area followed and enforced?

7. Was a microwave and/or radar susceptibility study performed (e.g., microwave dish for communicating to

field relays, ship traffic, local military base)? Is one necessary for this installation?

8. Was electrostatic discharge considered in the specification and the licensee's review? Are procedural restrictions in place to minimize these effects?

9. Was electrostatic discharge analyzed by the vendor? Is an adequate analysis and/or testing for electrostatic discharge provided?

k. The power quality and grounding review should address the following:

1. How did the licensee treat grounding? Are there 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?

2. Were the power requirements of the system analyzed by the licensee? Did the licensee consider battery loading profiles, maximum inverter loads, and inrush currents?

3. Were power quality requirements analyzed by the licensee i.e., total harmonic distortion, voltage and frequency fluctuations? Are they within the manufacturer's specification? Was harmonic distortion measured before and after installation to insure this digital upgrade does not create additional problems?

4. Were the post-installation power quality affects of the digital system considered for its affects on other instrumentation powered from the same source (e.g., clocks and switching circuits can create their own harmonics)?

l. The software review should address the following:

1. Has the licensee identified any software errors/failures, hardware errors/failures, and incorrect design assumptions used for the system (during or post installation)? How did the licensee disposition these error/failures?

2. Did the licensee or the vendor perform verification & validation (V&V) on the software?

3. If the vendor performed the V&V, did the licensee review this V&V? Was adequate documentation provided by the licensee in support of this review?

4. Did the software used in the test equipment undergo a V&V process? How does the licensee know that intended and unintended errors will not be introduced via software errors in the test equipment?

5. What software standards did the licensee use for the V&V? Did the licensee make a comparison to ANSI 7.4-3-2-1993? Can the licensee demonstrate that the software V&V meets the ANSI 7.4-3-2-1993 guidance?

6. Did the licensee review software errors found by the V&V process? How did the licensee treat these errors? How did the licensee know that all the errors were corrected for the plant-specific application?

7. Did the licensee verify that "generic" values used in the software code are applicable to their plant? How did the licensee confirm that the system was set-up correctly for their plant?

8. Is there any inactive code in the system, i.e., code still found in memory but not used for the plant-specific application? How does the licensee know that it cannot or will not be reactivated erroneously or through subsequent revisions thereby creating unintended functions?

9. Has software been revised and updated since the system installation? If so, was the update handled in accordance with the configuration management plan, and any other QA documents that may govern? What licensee actions were performed to verify the correctness of the revised code?

10. Who is the software librarian? How does the licensee ensure that revised code is correct (correct values, correct revision), and ensure post-installation configuration control? What assures that what was programmed is actually installed in the system, and that it performs to specification? If the system's software is loaded from magnetic media, are original and backup media properly labeled and controlled, and are magnetic media stored correctly?

m. To verify the system setpoints, request the licensee to download the current system setpoints and coefficients to a selected sample and compare these to the system requirements documentation.

n. No guidance provided.

o. No guidance provided.

52002-04 INSPECTION RESOURCE ESTIMATE

The estimated number of onsite inspection hours required to complete all inspection requirements is typically 70 hours (two weeks) for one inspector. This estimate is for broad resource planning, and is not intended as a quota or standard for judging inspector performance. The inspection is normally four weeks long. This would be one week preparation, one week onsite, one week in-

office, and a final week onsite. If extensive or unusual findings are identified during the onsite inspection, the inspector should consider lengthening the onsite inspection period as necessary to complete the required inspections. The inspector should be an knowledgeable I&C engineer familiar with digital equipment used in instrumentation systems.

52002-05 REFERENCES

References for this inspection procedure are extensive and are listed in an Appendix to this IP. Some of the following documents are listed for the inspector's information only, and are not considered regulatory requirements unless the licensee has formally committed to implementing any of these documents for application to digital systems. The inspector may wish to review these documents to become familiar with digital instrumentation issues.

END

Appendix:

List of References

APPENDIX

LIST OF REFERENCES

10 C.F.R. Part 50, Appendix A, GDC 2

10 C.F.R. Part 50, Appendix A, GDC 4

10 C.F.R. Part 50, Appendix A, GDC 17

10 C.F.R. Part 50, Appendix A, GDC 19

10 C.F.R. Part 50, Appendix A, GDC 20

10 C.F.R. Part 50, Appendix A. GDC 21

10 C.F.R. Part 50, Appendix A, GDC 22

10 C.F.R. Part 50, Appendix A, GDC 23

10 C.F.R. Part 50, Appendix A, GDC 24

10 C.F.R. Part 50, Appendix A, GDC 25

10 C.F.R. Part 50, Appendix B

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"

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

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

Generic Letter 95-02, "Use of NUMARC/EPRI Report TR-102348, 'Guideline on Licensing Digital Upgrades', in determining the

acceptability of performing analog-to-digital replacements under 10 CFR 50.59"

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-0700, Rev. 1, "Human-System Interface Design Review Guideline"
|
| 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 7, Instrumentation and Controls

| 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"

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

IEEE Standard 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 Standard 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 829-1983, "Software Test Documentation"

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

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"

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

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,"

END