INSPECTION PROCEDURE 52001

DIGITAL RETROFITS RECEIVING PRIOR APPROVAL

PROGRAM APPLICABILITY: 2515

SALP FUNCTIONAL AREA: MAINTENANCE (MAINT)

52001-01 INSPECTION OBJECTIVES

01.01 To ensure that digital systems previously 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 assess digital system failures, modifications, and maintenance issues for their affect on the system function, and for potential generic concern.

52001-02 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 maintaining 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 Safety Evaluation Report (SER) on the digital system.

e. Any licensing commitment documents concerning this modification.

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

02.02 Conduct of the Inspection

| The following are major topic areas to 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. Verify that the as-installed digital modification is in accordance with the SER, design drawings and licensee commitments.

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

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

e. Verify that the operators and technicians have been adequately trained, and have an understanding of the system commensurate with their responsibilities. Verify the training, qualifications and experience of the engineering staff or contractor personnel involved with the digital system.

f. Verify that post installation configuration management procedures and controls are in place, and are followed. This should include software and software media.

g. 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.

h. Verify that follow-up testing and post-installation testing were performed according to licensee commitments and manufacturer recommendations.

I. 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.

j. Verify that indication and/or annunciation for system bypass and failure, as specified in the SER is correctly installed and understood by the operators and technicians.

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

| l. Verify that the as-installed user interface is in accordance
| with the SER and design drawings.

52001-03 INSPECTION GUIDANCE

General Guidance

Future trends are toward increased use of computer based designs to encompass more plant instrumentation and controls (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 introduces 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.

Because of the complexity of digital systems, close coordination with NRR is recommended for a successful inspection. The regional inspector may consider NRR participation in the inspection. The inspector should concentrate on the plant-specific installation to confirm that the SER-approved design features have been properly implemented.

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. 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. Review the SER to identify specific licensee commitments or areas of concern flagged by the NRC reviewer. Verify that any changes made to the system since the issuance of the SER were adequately evaluated, and have not invalidated the SER conclusions.

b. During the verification that the modification is designed in accordance with the SER, design drawings and licensee commitments:

1. Verify that applicable 10 CFR Part 21 Notifications, Bulletins, Generic Letters, and Information Notices were correctly applied to the replacement 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 signs are posted limiting the use of radio equipment near the system, and that this policy is enforced.

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

6. Verify that the environmental conditions are consistent with those stated in the SER and with any special manufacturer requirements.

7. Verify that the shielding and grounding scheme is consistent with the SER and any applicable manufacturer recommendations.

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

c. During the verification of maintenance, surveillance, abnormal operating, emergency operating, and annunciator response procedures:

1. Verify that licensee commitments are incorporated in the procedures.

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

3. Verify that the system is tested in accordance with licensee commitments and that the post installation tests were adequate to ensure that the design basis was met. The tests should confirm correct trip outputs occur for the correct input logic combinations, and that safety functions are successfully accomplished.

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

5. Verify that the post installation testing included overall time response testing to demonstrate that the

actual system response times meet the requirements of the accident analysis.

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

7. Verify that any changes made to the system since the issuance of the SER were adequately evaluated, and have not invalidated the SER conclusions.

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

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

10. Verify that PCS, portable configurators or other computer interfacing test equipment are handled in accordance with the licensee commitments. This includes physical control, virus protection, password control, and personnel access.

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

12. Verify that cabinet ventilation devices are properly maintained.

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. In order to perform the verification that the operators and technicians have been adequately trained, it may require interviews with the personnel to insure they have an understanding of the system commensurate with their responsibilities.

f. If software has been revised and updated since the system installation, compare its handling to the configuration management plan, the SER, and any other QA documents that may govern. Place particular emphasis on the licensees actions to verify the correctness of the revised code.

g. 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.

h. No guidance provided.

I. Verify that setpoints or tuning parameters embedded in software are treated as any other setpoint, and the requirements for their control continue to be based upon the classification of the overall system. Appendix B to 10 CFR 50 will still apply to safety-related systems. 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.

j. No guidance provided.

k. 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.

l. No guidance provided.

52001-04 INSPECTION RESOURCE ESTIMATE

The estimated number of on-site inspection hours required to complete all inspection requirements is 35 hours (one week) 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 three weeks long. This would be one week preparation, one week onsite, and one week in-office. If extensive or unusual findings are identified during the on-site inspection, the inspector should consider lengthening the on-site inspection period as necessary to complete the required inspections. The inspector should be a knowledgeable I&C engineer familiar with digital equipment used in instrumentation systems.

52001-05 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 committed to them for application to the specific digital system. 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