U.S.NRC

United States Nuclear Regulatory Commission

Protecting People and the Environment

Feedback on Self-Testing and Diagnostics Credited Towards Replacement of Standard Surveillance

Office of New Reactors
Division of Engineering
Instrumentation, Controls and Electrical Engineering Branch 1
(ICE1)
Royce Beacom

July 20, 2011

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Regulations

- 10 CFR Part 50 Appendix A, General Design Criterion (GDC) 21, "Protection System Reliability and Testability," requires in part that the protection system be designed for high functional reliability and in-service testability commensurate with the safety functions to be performed.

- 10 CFR Part 50 Appendix B, Criterion XII, "Control of Measuring and Test Equipment," requires in part that measures be established to assure that measuring and testing devices used in activities affecting quality are properly controlled, calibrated, and adjusted at specified periods to maintain accuracy within necessary limits.

Self-Testing and Diagnostics Background

- Branch Technical Position (BTP) 7-17, "Guidance on Self-Test and Surveillance Test Provisions," provides the staff guidance for this subject on computer-based instrumentation and control (I&C) systems.
- If automatic test features are proposed to be credited with performing surveillance test functions, it is important that equipment, hardware and software, used to perform the tests are qualified and provisions are be made to confirm the execution of the automatic tests during plant operation.
- In Chapter 1 of the US-APWR DCD, conformance to this BTP was identified with "no exceptions noted."

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Self-Testing and Diagnostics
BTP 7-17 Acceptance Criteria

- "The safety classification and quality of the hardware and software used to perform periodic testing should be equivalent to that of the tested system."
  - MHI has some aspects of self testing and diagnostics built into the safety system software meet this criteria. Staff finds these safety aspects acceptable.
- "Commercial digital computer-based equipment used to perform periodic testing should be appropriately qualified for its function."
  - However, MHI additionally uses non-safety equipment for periodic testing and has not demonstrated this criterion.

Self-Testing and Diagnostics
One BTP 7-14 Acceptance Criterion

- On software tools, BTP 7-14, Guidance of Software Reviews, states "The SCMP should include a description of the process used to maintain and track purchased items, such as software tools used to make the final product. A qualification procedure should be provided, and a method of tracking tool history, bug lists, and errata sheets should enable the applicant/licensee to track."
  - (MHI's MELTAC technical report) The Memory Integrity Check is proposed to be done with the Engineering Tool on the Safety System CPU modules. Although not clearly identified in Software Program Manual, this tool appears to be a non-safety item with no additional controls or qualifications applied.

Self-Testing and Diagnostics
BTP 7-17 Acceptance Criteria

- "If automatic test features are credited with performing surveillance test functions, provisions should be made to confirm the execution of the automatic tests during plant operation."

  - The automated non-safety CHANNEL CHECK is being proposed to replace the operator implemented CHANNEL CHECK . A means of confirming the execution of this check during operation needs to be identified. CHANNEL CALIBRATION is not done during plant operation, therefore it cannot be used to confirm operation of the automatic test.

  - There is no sufficient information on the docket how or why the CHANNEL CHECK is implemented in the PCMS. (This should be identified in the FMEA, per IEEE Std 352, as a safety to non-safety system interaction)

Self-Testing and Diagnostics Summary

- The staff guidance states that testing of safety system software should be conducted by hardware and software with classification and quality equivalent of those of the safety system.
- Staff guidance presents that the software tools used to develop, test and assist in the V&V of Safety Related Software should be validated and qualified.
- Once the tools and their quality are properly identified, the effectiveness (i.e., reliability) of these software tests vs. others already implemented in the software and the standard surveillances, would have to be presented.
- The staff will follow with RAIs on this subject.