U.S.NRC

United States Nuclear Regulatory Commission

Protecting People and the Environment

Feedback on the AREVA NP Priority Actuation and Control System (PACS) Design

Tung Truong
Instrumentation, Controls, and Electrical Engineering Branch 1
Division of Engineering
Office of New Reactors

September 2-3, 2009

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

Previous Issues

1. Classification of communication controller software as non-safety related on safety-related PACS board.
2. Testing of programmable logic device needed to be 100 percent of all possible combinations of inputs and internal states

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

Separation of Communication Controller

- Communication controller providing component commands from the non-safety control system is moved to a separate board.
- The communication controller board will be treated as an associated circuit per Regulatory Guide 1.75 and qualified as such.
- Acceptable path forward to address the independence issue regarding the communication controller.

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

100 Percent Combination Testing

- AREVA NP identified unique design aspects of the PACS module:
  - Use of infrastructure signals and not including them in the 100 percent combination testing
  - Handling the time delay aspects of certain signals during 100 percent combination testing (including invalid signal states less than minimum stability time)
  - Use and qualification of a test machine to automatically verify the test cases
  - Manual verification of a select set of test cases

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

Infrastructure Signals

- Infrastructure signals include status signals from components such as power supplies.
- Not including the infrastructure signals in the 100 percent combination testing is a path forward provided:
  - All infrastructure signals are specifically identified and justification is provided for not including the non-nominal state of the signals in 100 percent combination testing
  - The nominal state of the infrastructure signal is set in the 100 percent combination testing
  - The non-nominal state of the infrastructure signal is a result of a hardware single failure and the impact of the single failure is contained within the respective division

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

PACS Signal Time Delays

- AREVA NP discussed the sequence of test cases to (1) set internal states and (2) exercise the combinational logic and account for time delays
- Issuing a sequence of test cases and accounting for time delays is a path forward; however the following should be addressed:
  - Unless the output of the PACS module is locked at its previous output during the stabilization time, the output of the programmable device should be evaluated during stabilization time also to assess impact on potential downstream equipment.

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

Test Machine

- AREVA NP proposed to use a test machine/platform to automatically generate test vectors and expected outputs, compare the actual outputs to the expected, and generate reports.
- The staff does not have any issues with using an automated test machine to generate, execute, and document the test cases.
- AREVA NP proposed to qualify the test machine as a software tool described in Reg. Guide 1.152 and Standard Review Plan Appendix 7.1-D.

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

Manual Verification of Test Cases

- AREVA NP proposed to manually verify a subset of test cases based on selection criteria.
- Digital I&C Interim Staff Guidance No. 4 states that manual verification should be performed on all test cases.
- AREVA NP's basis for manually verifying a subset of test cases is the automated tool will perform verification better than manual means. Additionally, the automated tool is qualified.

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

Manual Verification of Test Cases (cont.)

- Software faults (potentially resulting in software common-cause failures when activated) enter the software development process at different phases.
- 100 percent combination testing addresses software faults entering the software implementation phase.
- Software faults may still enter the requirements and design phases – engineering design reviews to address these potential faults
- As devices become more complex, the greater the potential for software faults to enter at the requirements and design phases.

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

Manual Verification of Test Cases (cont.)

- ISG No. 4 sets objective criteria for a "simple digital device" as one that can be 100 percent combination tested with manual verification of all test cases.
- The staff does not intend to deviate from this criteria as it is important in assuring that simple digital devices are not susceptible to software common-cause failures.
- AREVA NP would need to perform manual verification on all test cases for the PACS design to be a viable option.
- Additionally, AREVA NP should describe their review and V&V efforts at the requirements and design phases.

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

Summary

- With the exception of the manual verification proposal, the PACS design presented to the staff in August is a viable path forward.

Questions?