U.S.NRC

United States Nuclear Regulatory Commission

Protecting People and the Environment

Pre- Review of Basic Software Program Manual Draft Sections

Instrumentation, Controls and Electrical Engineering Branch 1 (ICE1)

Royce Beacom

January 20, 2010

Purpose

The purpose of this presentation is to :

- Provide feedback on the staff’s pre-review of the two plans of the basic software SPM – Software Management Plan and Software V&V Plan.

- Consideration of these issues going forward in the development of the remaining plans of both SPMs.

Background

- Consider the issues raised by the staff in the attachment (ML103420426) of the December 20, 2010 letter.

- These were taken from staff guidance on the subject of Software Program Reviews:
  - 7 Regulatory Guides endorse 9 IEEE standards
    - BTP 7-14 provides guidance taken from these and other standards, NUREGs etc

Software Program Manuals
Pre-Review

- Independence of the Organizations
  - The SMP should ensure that the quality assurance organization, the software safety organization and the software V&V organization maintain independence from the development organization. In particular, the plan should ensure that these assurance organizations *not report* to the development organization, *and* not be subject to the financial control of the development organization. - BTP 7-14.
- Can the Design Section Manager assume the role of Project Manager and still maintain this?

Software Program Manuals Pre-Review

- Terminology used should be per IEEE 610.12, IEEE Standard Glossary of Software Engineering Terminology or BTP 7-14 with exceptions noted:
  - Examples: Verification, Validation, Requirements Traceability Matrix, Qualified, etc

Software Program Manuals
Pre-Review

➢ The requirements identification in the Project Plan, as identified in the RG 1.173/ IEEE Std 1074, is identified as the “input information” and should include the following:

- The input information as well as the life cycle activity and output information, *must* identify applicable regulatory requirements, design bases and related guidance. – RG 1.173
- The input information shall address regulatory approvals, required certifications etc. The project standards shall include requirements, design, coding, test and documentation standards. – IEEE 1074
- The statement on the Project Plan; that it shall include, “Requirements top-level laws and regulations, codes, and customer requirements” needs to be significantly expanded and revised.”

➢ Software Quality Metrics:

- Further discussion on this topic is normally part of the Software QA plan. But as IEEE 1074 identifies, metrics shall be defined as part of establishment of the project environment (Project Plan).
  - There is no mention of initial identification of metrics and methodology in the project plan per IEEE stds 1061, Methodology of Metrics, and phase based metric characteristics per IEEE 7-4.3.2, Section 5.3.1.1.

Software Program Manuals
Pre-Review

➢ Software Project Risk Management

– The Analysis of Risks is also part of the Establishment of the Project Enviornment (Project Plan) – IEEE 1074

– IEEE 7-4.3.2 identifies seven steps in the scope of project risk management.

– In the SMP, the statement: “Identified risks and issues associated with any anomalies that arise from the V&V activities of each phase are maintained in the Problem List.” Use of the “Problem List” that is contains many different issues needs to be evaluated. This could be an issue of future audits.

Software Program Manuals Pre-Review

- ➢ Examples of Issues to be further addressed in the SV&VP:

– All topics to be addressed for each V&V activity per IEEE 1012-1998 as endorsed by RG 1.168.

– The types of software safety analyses, identified by BTP 7-14, to be completed for each phase of the software life cycle.

Software Program Manuals Pre-Review

- ➢ Examples of Implementing Processes :

- – The MHI “augmented” quality program for systems important to safety. (Ex: O-VDU, Alarms, SPDS, SSA etc.)

- – Identification of the actual lower level software plans, procedures, manuals, etc. that will be used to implement the planning and later phase activities.

- – Addressing hardware attributes throughout various planning activities.

- – Checklists are not included as attachments to the SPM. Merely stating the checklist meets the regulatory guide is not sufficient evidence of conformance.

Software Program Manuals Pre-Review

- Examples of issue with Software Tools:

– The SMP states “The MELTAC Engineering Tool is used to generate safety application software for the MELTAC.” It also states, “per the MELCO QAP for non-safety items, qualification and configuration control processes are identified.”

– This simple statement, without addressing the V&V of the output of the tool by procedure, would require the engineering tool to be safety related per IEEE Std 7-4.3.2. This standard identifies two methods to determine the tools are suitable for use

– The SMP also states “the tool itself is non-safety software.” The MELTAC TR says the engineering tool is “called MELENS.” The Safety I&C TR says “The Engineering Tool is a personnel computer.” All discriptions should be the same. Both the software, and the pc that it is loaded on, should have a particular process for qualification and configuration control other than “a QAP for non-safety items.”