Insights from Assessments of Safety Software Quality Assurance

S. Seth, C. Ashley, D. Brown

U.S. Department of Energy Richland Operations Office, P.O. Box 550, MS: A6-39, Richland, WA 99352
shivaji_s_seth@rl.gov

[The views expressed are solely those of the authors and no endorsement by the U.S. Department of Energy is intended.]

INTRODUCTION

This paper summarizes the results and insights from a set of comprehensive assessments of safety software quality assurance (SQA) conducted at the Department of Energy's (DOE's) Hanford Site. The assessments were conducted jointly by the DOE Richland Operations Office and the Office of River Protection during February through August 2004. They covered the SQA requirements, processes, and procedures of four DOE prime contractor and selected subcontractor organizations. The safety software included nuclear facility digital instrumentation and control (I&C) software, safety analysis and design computer codes, databases, spreadsheets, and other software with nuclear safety implications. The primary driver for the assessments was the DOE Implementation Plan for Defense Nuclear Facilities Safety Board Recommendation 2002-1 [1].

ASSESSMENT APPROACH

The SQA assessments were based on a relatively large sample of about 50 safety software applications, including 12 I&C applications. These were selected based on several factors, such as software type, complexity, vintage, usage, and safety significance. All I&C software and close to half of the other software was custom; the remaining software was commercial off-the-shelf. Assessments were performed using contractual requirements and DOE criteria and guidelines [2, 3]. They entailed extensive document reviews, facility visits and interviews.

RESULTS AND INSIGHTS

The assessments resulted in a combined total of about 30 findings and 25 observations. Findings identified specific non-compliances with applicable SQA requirements. The following discussion focuses on a few of the insights that would be of broader interest.

Definition and Scope of Safety Software

The assessments covered a broader range of safety software than would be included by the definition of safety software in DOE's Implementation Plan and guidelines. While the latter focused on nuclear facility safety system software and safety analysis and design software, the scope of Hanford assessments was based on DOE's QA Rule [4], whose requirements apply "in a graded approach to those facilities, activities, and areas that have the potential to cause radiological harm" [5]. The QA Rule is implemented through DOE contractors' QA program descriptions and procedures typically using consensus standards, such as NQA-1 [6]. Using requirements with broader applicability, the assessments identified significant SQA issues in important safety, health and environmental applications, such as radioactive plume dispersion during emergencies, radiological dose assessments, and contaminated ground water modeling. On the other hand, categorizing software (e.g., delineating safety analysis or safety system software from other software with safety implications) to exclude or relax SQA requirements may not have exposed the identified deficiencies. There did not appear to exist adequate technical basis and cost-benefit analysis to support categorization of safety software. This is similar to a conclusion of an extensive study of SQA standards [7].

Management of Legacy Software

For legacy safety software that was developed without the benefit of present-day SQA standards, the assessments found that processes to bring such software into conformance with current requirements generally were lacking or inadequate; and several software applications did not have software management plans. Typically, the qualification of legacy software involves documenting its functional requirements; defining critical features; evaluating the adequacy of design, test and user documentation; and determining the need for further testing using a graded approach. A software management plan based on such a process ensures that adequate management controls are defined and applied.

Flow-down of SQA Requirements

The assessments identified some significant issues when work involving safety software was subcontracted or performed through staff augmentation. For example, in certain instances where technical services were procured, standards or appropriate clauses to ensure adequate SQA were not included in the contract. As a result, analyses

were completed without the necessary software validation testing or without the assurance that the correct software version was used. Another issue concerned subcontractors and affiliated organizations whose work agreements required certain SQA standards, but they did not have adequate procedures implementing those SQA requirements, or they followed different standards that were used in their own organization.

Software Verification and Validation (V&V)

The review of V&V processes of software modifications showed that in several instances there were no clear criteria and process for determining the significance of changes and applying a higher degree of rigor. The additional rigor for significant software changes could include an appropriate test plan, test cases, regression testing, selective retesting, more detailed test documentation, and independent V&V. Furthermore, the independence of V&V was found to be weak in small organizations or where knowledge of a legacy software application was generally limited to one individual. The assessments found cases where management or independent reviews had not identified incorrect or insufficient software validation.

Software Use, Maintenance and Problem Reporting

For certain safety software applications, the responsible organizations had allowed expiration of maintenance (including problem reporting) agreements with vendors. In such instances, there was little assurance that users would be notified of software errors and revisions. More generally, the assessments found that processes for reporting software errors to suppliers and for acting upon errors reported by suppliers were ad hoc. Also, the records of software use (user logs) generally were not adequately maintained. A proper use record aids traceability between software version and specific application, and is important in tracing impacts of a software error or misapplication.

CONCLUSION

The assessments indicated that high level requirements documents of DOE prime contractors, such as QA program descriptions, recognize and often require the use of SQA standards [6] for safety software applications. This is consistent with the growth in importance and awareness of SQA standards. However, the assessments show that significant weaknesses exist in implementing SQA requirements. It appears that enhanced implementing procedures and more widespread SQA training is needed. Furthermore, it is critical that organizations responsible for safety software conduct comprehensive and rigorous self-assessments to identify SQA deficiencies. The assessments reported here are already having a positive impact at Hanford as progress continues on corrective actions.

REFERENCES

1. U.S. Department of Energy, "Quality assurance for Safety Software at Department of Energy Defense Nuclear Facilities: Implementation Plan for Defense Nuclear Facilities Safety Board Recommendation 2002-1," (2003).
2. U.S. Department of Energy, "Criteria and Guidelines for the Assessment of Safety System Software and Firmware at Defense Nuclear Facilities," CRAD – 4.2.3.1, Rev. 3 (2003).
3. U.S. Department of Energy, "Assessment Criteria and Guidelines for Determining the Adequacy of Software used in the Safety Analysis and Design of Defense Nuclear Facilities," CRAD – 4.2.4.1, Rev. 3 (2003).
4. U.S. Government, "Nuclear Safety Management Quality Assurance Requirements," *Code of Federal Regulations,* Title 10, Part 830, Subpart A.
5. U.S. Department of Energy Office of Enforcement and Investigation, "Enforcement of 10 CFR 830.120 (Quality Assurance Rule) for Facilities Below Hazard Category III," *Enforcement Guidance Supplement 99-01,* (1999).
6. The American Society of Mechanical Engineers, "Quality Assurance Requirements for Computer Software for Nuclear Facility Applications," ASME NQA-1, Subpart 2.7 (2000 or earlier versions).
7. S. Seth et al., "High Integrity Software for Nuclear Power Plants: Candidate Guidelines, Technical Basis and Research Needs," NUREG/CR-6263, U.S. Nuclear Regulatory Commission (1995).