

QUALITY ASSURANCE FOR SAFETY-RELATED SOFTWARE AT DEFENSE NUCLEAR FACILITIES

Thomas D. Burns, Jr.
Matt Forsbacka
Charles R. Martin
DNFSB, 625 Indiana Ave.
Washington, DC 20004
(202) 694-7000

Confidence in safe operation of Department of Energy (DOE) defense nuclear facilities is highly dependent on the underlying quality of the computer codes used to determine which controls are important to safety, as well as those codes used to operate specific safety-related controls. Software quality assurance (SQA), as considered here, is a process for the systematic development, testing, documentation, maintenance, and execution of such software.

Deficiencies in computer software used in support of both safety analyses and machine control at DOE sites have been identified. Instances of phenomenological modeling deficiencies in the computer software for safety analyses have also been noted. In addition, there have been problems with local implementation and use of codes resulting from a lack of guidance and training of safety analysts on the use of codes for performing safety analysis pursuant to authorization of facility operation. These problems are symptomatic of underlying deficiencies in the infrastructure supporting SQA at DOE.

Given the current problems with SQA at DOE described above, unclear ownership for these problems within DOE, and concerns about the need for a research program to improve the understanding of phenomenology and develop code benchmarks, it is clear that corrective actions should be pursued.

Achieving a productive SQA infrastructure will require the coordination of various departmental entities that perform SQA related functions. Furthermore, an effective approach for addressing SQA issues should include, but not be limited to, the following actions:

- ! Assess the adequacy of accident analysis codes in the following areas: model fidelity and appropriateness for various accidents, approximate level of SQA, confidence in local installation at sites using the codes, and ease of use (including user interface, user documentation, and guidance on input parameters). Consolidate the best codes into a standard Atool-box@ to be certified under an a posteriori verification and validation program for use in DOE safety basis analyses.
- ! Develop and institute a short but intensive training program, including best practices and other guidance for safety analysts who use such codes in the performance of safety analysis, emergency preparedness, or other safety-related activities.

- ! Consider a modest program of experimental research designed to validate calculations used to develop the safety basis for defense nuclear facilities.
- ! Develop a Website to (1) promulgate lessons learned from the application of codes in safety analyses; (2) share benchmark data and test problems; (3) permit rapid communication of code problems and fixes; (4) share databases needed for execution of these codes, such as meteorological and population data; and (5) provide a forum for discussion of common problems.
- ! Identify a core group of safety analysis experts to advise on the above actions and assist in resolving future technical issues.
- ! Verify that the principles comprising an acceptable set of SQA standards flow down and are implemented in safety-related control systems.