TS

NOT MEASUREMENT
SENSITIVE

DOE–STD–1172-2003
December 2003

DOE STANDARD

SAFETY SOFTWARE QUALITY ASSURANCE FUNCTIONAL AREA QUALIFICATION STANDARD

DOE Defense Nuclear Facilities Technical Personnel

U.S. Department of Energy
Washington, D.C. 20585

AREA TRNG

This document has been reproduced directly from the best available copy.

**Available to DOE and DOE contractors from ES&H Technical Information Services, U.S. Department of Energy, (800) 473–4375,
fax: (301) 903-9823.**

Available to the public from the U.S. Department of Commerce, Technology Administration, National Technical Information Service, Springfield, VA 22161; (703) 605–6000.

APPROVAL

The Federal Technical Capability Panel consists of senior U.S. Department of Energy managers responsible for overseeing the Federal Technical Capability Program. This Panel is responsible for reviewing and approving the Qualification Standard for Department-wide application. Approval of this Qualification Standard by the Federal Technical Capability Panel is indicated by signature below.

Roy J. Schepens
Chairman
Federal Technical Capability Panel

INTENTIONALLY BLANK

TABLE OF CONTENTS

INTENTIONALLY BLANK

ACKNOWLEDGMENT

The Office of Environment, Safety, and Health is the Sponsor for the Safety Software Quality Assurance Functional Area Qualification Standard. The Sponsor is responsible for coordinating the development and/or review of the Functional Area Qualification Standard by subject matter experts to ensure that the technical content of the standard is accurate and adequate for Department-wide application for those involved with Safety Software Quality Assurance. The Sponsor, in coordination with the Federal Technical Capability Panel, is also responsible for ensuring that the Functional Area Qualification Standard is maintained current.

The following subject matter experts (SMEs) participated in the development and/or review of this Qualification Standard:

Ed Blackwood	DOE-Headquarters (EH), Team Lead
Sarbes Acharya	DOE-Headquarters (EH)
Bud Danielson	DOE-Headquarters (EH)
Pranab Guha	DOE-Headquarters (EH)
Darrell Huff	DOE-Headquarters (EH)
Subir Sen	DOE-Headquarters (EH)
Joe Arango	DOE-Headquarters (EM)
Rick Kendall	DOE-Headquarters (NA)
Dave Brown	Office of River Protection
Dana Bryson	Office of River Protection
John Swailes	Office of River Protection
Shiv Seth	Richland Operations Office
Bill Rowland	Savannah River Operations Office

INTENTIONALLY BLANK

U.S. DEPARTMENT OF ENERGY
FUNCTIONAL AREA QUALIFICATION STANDARD

Safety Software Quality Assurance

PURPOSE

DOE M 426.1-1, Federal Technical Capability Manual, commits the Department to continuously strive for technical excellence. The Technical Qualification Program, along with the supporting Technical Qualification Standards, complements the personnel processes that support the Department's drive for technical excellence. In support of this goal, the competency requirements defined in the Technical Qualification Standards should be aligned with and integrated into the recruitment and staffing processes for technical positions. The Technical Qualification Standards should form the primary basis for developing vacancy announcements, qualification requirements, crediting plans, interviewing questions, and other criteria associated with the recruitment, selection, and internal placement of technical personnel. Office of Personnel Management minimum qualifications standards will be greatly enhanced by application of appropriate materials from the technical Functional Area Qualification Standards.

The Technical Qualification Standards are not intended to replace the OPM Qualifications Standards nor other Departmental personnel standards, rules, plans, or processes. The primary purpose of the Technical Qualification Program is to ensure that employees have the requisite technical competency to support the mission of the Department. The Technical Qualification Program forms the basis for the development and assignment of DOE personnel responsible for ensuring the safe operation of defense nuclear facilities.

APPLICABILITY

The Safety Software Quality Assurance Functional Area Qualification Standard establishes common functional area competency requirements for Department of Energy personnel who provide assistance, direction, guidance, oversight, or evaluation of safety software that includes, but is not limited to safety software used for consequence analysis for potential accidents and design basis events, design for structures, systems and components, instrumentation and controls (I&C), and also other types of software, such as databases used for safety management functions. For ease of transportability of qualifications between DOE elements, Program and Field offices are expected to use this technical Functional Area Qualification Standard without modification or additions. Needed additional office/site/facility specific technical competencies should be handled separately. Satisfactory and documented attainment of the competency requirements contained in this technical Functional Area Qualification Standard ensures that personnel possess the requisite competence to fulfill their functional area duties and responsibilities. Office/Facility-Specific Qualification Standards supplement this technical Functional Area Qualification Standard and establish unique operational competency requirements at the Headquarters or Field element, site, or facility level.

IMPLEMENTATION

This technical Functional Area Qualification Standard identifies the minimum technical competency requirements for Department of Energy personnel. Although there are other competency requirements associated with the positions held by DOE personnel, this Functional Area Qualification Standard is limited to identifying the specific technical competencies. The competency statements define the expected knowledge and/or skill that an individual must meet. Each of the competency statements is further explained by a listing of supporting knowledge and/or skill statements.

The competencies identify a familiarity level, a working level, or an expert level of knowledge; or they require the individual to demonstrate the ability to perform a task or activity. These levels are defined as follows:

> **Familiarity level** is defined as basic knowledge of or exposure to the subject or process adequate to discuss the subject or process with individuals of greater knowledge.
>
> **Working level** is defined as the knowledge required to monitor and assess operations/activities, to apply standards of acceptable performance, and to reference appropriate materials and/or expert advice as required to ensure the safety of Departmental activities.
>
> **Expert level** is defined as a comprehensive, intensive knowledge of the subject or process sufficient to provide advice in the absence of procedural guidance.
>
> **Demonstrate the ability** is defined as the actual performance of a task or activity in accordance with policy, procedures, guidelines, and/or accepted industry or Department practices.

Headquarters and Field elements shall establish a program and process to ensure that DOE personnel possess the competencies required of their position. That includes the competencies identified in this technical Functional Area Qualification Standard. Documentation of the completion of the requirements of the Standard shall be included in the employee's training and qualification record.

Equivalencies should be used sparingly with the utmost rigor and scrutiny to maintain the spirit and intent of the TQP. Equivalencies may be granted for individual competencies based upon objective evidence of previous education, training, certification, or experience. Objective evidence includes a combination of transcripts, certifications, and, in some cases, a knowledge sampling through a written and/or oral examination. Equivalencies shall be granted in accordance with the Technical Qualification Program Plan of the office qualifying the individual. The supporting knowledge and/or skill statements, while not requirements, should be considered before granting equivalency for a competency.

Training shall be provided to employees in the Technical Qualification Program who do not meet the competencies contained in the technical Functional Area Qualification Standard. Training may include, but is not limited to, formal classroom and computer based courses, self-study, mentoring, on-the-job training, and special assignments. Departmental training will be based upon appropriate supporting knowledge and/or skill statements similar to the ones listed for each of the competency statements. Headquarters and Field elements should use the supporting knowledge and/or skill statements as a basis for evaluating the content of any training used to provide individuals with the requisite knowledge and/or skill required to meet the technical Functional Area Qualification Standard competency statements.

EVALUATION REQUIREMENTS

Attainment of the competencies listed in this technical Functional Area Qualification Standard should be documented by a qualifying official, immediate supervisor, or the team leader of personnel in accordance with the Technical Qualification Program Plan of the office qualifying the individual.

CONTINUING EDUCATION, TRAINING, AND PROFICIENCY

DOE personnel shall participate in continuing education and training as necessary to improve their performance and proficiency and ensure that they stay up-to-date on changing technology and new requirements. This may include courses and/or training provided by:

- Department of Energy
- Other government agencies
- Outside vendors
- Educational institutions

Beyond formal classroom or computer-based courses, continuing training may include

- Self Study
- Attendance at symposia, seminars, exhibitions
- Special assignments
- On-the-job experience

A description of suggested learning proficiency activities and the requirements for the continuing education and training program for Safety Software Quality Assurance personnel are included in Appendix A of this document.

DUTIES AND RESPONSIBILITIES

Safety Software Quality Assurance personnel implement the appropriate level of management effort and assume responsibility, accountability, and oversight for continued management process compliance within their respective program areas. Specifically they are to:

- Review and evaluate safety software plans and related processes to verify compliance with applicable regulations, standards, and DOE Orders.

- Verify that safety software plans and processes are developed based on hazard and risk assessments.

- Verify that safety software is developed, procured, verified, validated, used, and maintained consistent with nuclear safety and safeguards and security requirements.

- Verify that appropriate software quality assurance requirements are addressed in procurement documents.
- Assess safety software quality assurance programs, document results, and monitor resulting actions.

- Review and evaluate training and qualification programs for individuals who develop, use, or maintain safety software, as well as design, maintain, and implement SQA programs.

- Provide technical support with respect to safety software for activities such as accident and occurrence investigations.

- Serve as an organization's technical point-of-contact for safety software.

BACKGROUND AND EXPERIENCE

The preferred education and experience for Safety Software Quality Assurance personnel is defined in this section. The U. S. Office of Personnel Management's (OPM) Qualification Standards Handbook establishes minimum education, training, experience, or other relevant requirements applicable to a particular occupational series/grade level, as well as alternatives to meeting specified requirements. The preferred education and experience for Safety Software Quality Assurance personnel is:

- Education – Baccalaureate degree in engineering, science, or a related discipline; or meet the alternative requirements specified for engineers or scientists in the OPM Qualifications Standards Handbook. Baccalaureate degrees in other disciplines may also be appropriate based on the duties to be performed and considering the experience gained in performing related software development, maintenance, management, and quality assurance activities.

- Experience – Industry, military, federal, state, or directly related background that has provided specialized experience in software development, maintenance, management, and quality assurance activities. Specialized experience may be demonstrated through possession of the competencies outlined in this standard. In addition to this education and experience, certifications from other professional societies may serve as the basis for equivalency of competencies in portions of this standard.

REQUIRED TECHNICAL COMPETENCIES

The competencies contained in this Standard are in addition to and distinct from those competencies contained in the General Technical Base Qualification Standard. All Safety Software Quality Assurance personnel must satisfy the competency requirements of the General Technical Base Qualification Standard prior to or in parallel with the competency requirements contained in this Standard. Each of the competency statements defines the level of expected knowledge that an individual must posses to meet the intent of this Standard. The supporting knowledge, skills, and abilities statements further describe the intent of the competency statements.

Note: This section refers to NUREG/CR-6263, *High Integrity Software for Nuclear Power Plants*, in several of the competency statements and supporting knowledge, skills, and abilities. This NUREG was prepared for the Nuclear Regulatory Commission to aid the NRC in developing regulatory guidance for the commercial nuclear industry. It is used in this standard because it provides important insights on the software life cycle that are not available in industry standards. However, NUREG/CR-6263 is not a DOE Standard and should not be used as such. Copies of this NUREG are available at no charge to government agencies (but not government contractors). Send requests for copies from a government e-mail address to distribution@nrc.gov.

Note: When regulations or U.S. Department of Energy directives or other industry standards are referenced in the Qualification Standard, the most current version should be used.

Safety Software and System Relationship

1. Safety Software Quality Assurance personnel shall demonstrate a working level knowledge of the types of safety system software and safety design and analysis software, including custom software and commercial off-the-shelf software (COTS). This includes instrumentation and control software and firmware (e.g., human-machine interface software, and programmable logic controller software), and computer calculation and database program software used in the design and accident analyses of nuclear facilities.

Supporting Knowledge, Skills, and Abilities

a. Explain the characteristics, application, and limitations of instrumentation and control software and firmware (e.g., human-machine interface software, and programmable logic controller software), safety analysis and design software, and database program software used in the design, accident analyses, operation, and maintenance of nuclear facilities. This should include both custom and COTS safety software.

b. Given examples of safety and non-safety software, determine the controls that were applied to the safety software to distinguish it from non-safety software.

c. Describe the process for identifying safety software at a facility, based on the safety function as described in the facility Documented Safety Analysis.

2. Safety Software Quality Assurance personnel shall demonstrate a working level knowledge of the functional interfaces between safety system software components and the system-level design.

Supporting Knowledge, Skills, and Abilities

a. Identify how system-level requirements are established and then assigned to hardware, software, and human components of a digital instrumentation and control system.

b. Identify the typical requirements that define functional interfaces between safety system software components and the system-level design, as described in standards such as ANSI/IEEE 830, *IEEE Guide to Software Requirements Specifications* and IEEE 7-4.3.2, *Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations.*

c. Identify the specific records that must be maintained and the requirements for maintaining these records to document the development of safety system software.

d. Review a development project for safety system software. Explain how the functional interfaces between components and the system level design were established and controlled.

3. Safety Software Quality Assurance personnel shall demonstrate a working level knowledge of the relationships between the problems being addressed by safety analysis and design codes, the design requirements for the codes, and the components of the codes.

Supporting Knowledge, Skills, and Abilities

a. Identify how functional requirements and applicability of safety analysis and design computer codes are defined, documented, and controlled relative to modeling and data assumptions, design constraints, sizing and timing conditions, and input/output parameters.

b. Review a development project for safety analysis or design software. Explain how the problem being addressed by the software was translated into functional requirements, how the requirements were established and controlled, and how the code was reconciled with the original problem.

Software Engineering, Development, and Maintenance

4. Safety Software Quality Assurance personnel shall demonstrate a working level knowledge of the safety software life cycle processes described in IEEE 1074, *IEEE Standard for Developing Software Life Cycle Processes*.

Supporting Knowledge, Skills, and Abilities

a. Discuss the software life cycle processes such as the waterfall, modified waterfall, and spiral models.

b. Describe each phase of a typical software life cycle model such as the one described in IEEE 1074, *IEEE Standard for Developing Software Life Cycle Processes*. Explain the roles of quality assurance and configuration management in each phase.

c. Identify the types of audits and products associated with each life cycle process.

5. Safety Software Quality Assurance personnel shall demonstrate a working level knowledge of the safety software requirements specification concepts such as those described in ANSI/IEEE 830, *IEEE Guide to Software Requirements Specifications* and Section 3 of NUREG/CR-6263, *High Integrity Software for Nuclear Power Plants*.

Supporting Knowledge, Skills, and Abilities

a. Explain how software requirements specifications (SRS) are developed and used. Include in your explanation the essential role of SRS in the overall argument that software is safe.

b. Define and discuss the following SRS attributes as they relate to safety software quality:

- Completeness
- Unambiguity
- Consistency
- Verifiability
- Modifiability
- Traceability
- Readability

c. Describe the methods used to ensure the requirements specifications attributes are met.

d. Describe and give specific examples of:

- Functional requirements
- Performance requirements
- Design constraints
- Attributes
- External interfaces
- Input/output requirements
- Requirements Traceability Matrix

6. Safety Software Quality Assurance personnel shall demonstrate a familiarity level knowledge of the safety software design concepts as described in ANSI/IEEE 1016, *IEEE Recommended Practice for Software Design Descriptions* and Section 4 of NUREG/CR-6263, *High Integrity Software for Nuclear Power Plants*.

Supporting Knowledge, Skills, and Abilities

a. Discuss the following concepts as they relate to safety software quality:

- Modular design
- External interface
- Interfaces between both safety and non-safety components
- Interface integrity
- Data integrity, flow control
- Exception and error handling

7. Safety Software Quality Assurance personnel shall demonstrate a familiarity level knowledge of the safety software coding practices that ensure that software requirements specifications and design requirements are reflected in the source code.

Supporting Knowledge, Skills, and Abilities

a. Discuss the following concepts as they relate to safety software coding:

- Development environment
- Target environments and reusable components
- Data structure
- Logic structure
- Embedded comments

b. Discuss the following documents and describe how each supports safety software coding:

- Design Specifications
- Program Specifications
- Programming Standards
- System Design Document
- Programmers Manual
- Users Manual

8. Safety Software Quality Assurance personnel shall demonstrate a working level knowledge of the software verification and validation processes that ensure that the requirements specification, design, and coding of software adequately fulfill all intended safety functions. These processes are described in standards such as ANSI/IEEE 829, *IEEE Standard for Software Test Documentation*, ANSI/IEEE 1008, *IEEE Standard for Software Testing*, ANSI/IEEE 1012, *IEEE Standard for Software Verification and Validation Plans*, and Sections 6 – 8 of NUREG/CR-6263, *High Integrity Software for Nuclear Power Plants*.

<u>Supporting Knowledge, Skills, and Abilities</u>

a. Describe the following processes and documents as they relate to safety software quality:

- Verification of requirements
- Verification of design
- Verification of source code
- Unit testing
- Integration and system testing
- Verification and validation plan
- Verification and validation reports
- Verification and validation of tools
- Distinction between verification and validation activities
- Independent verification and validation

b. Describe methods for reviewing a verification and validation program.

c. Explain the differences in the verification and validation processes between custom and COTS safety software.

d. Explain the differences in the verification and validation processes between safety system software and firmware vs. safety analysis and design software.

e. Describe the controls used to assure that calculations performed using spreadsheets and other calculation programs are accurate. Identify the records that should be maintained to document the calculation process.

f. Conduct or review an assessment of the verification and validation processes applied to a software development project and/or to a program in the operation and maintenance life cycle phase. Describe the strengths and weaknesses you identify.

9. Safety Software Quality Assurance personnel shall demonstrate a working level knowledge of software safety analysis as described in documents such as IEEE 1228, *IEEE Standard for Software Safety Plans* and Section 9 of NUREG/CR-6263, *High Integrity Software for Nuclear Power Plants*.

Supporting Knowledge, Skills, and Abilities

a. Discuss the purpose and content of the following and relate the importance of each to safety software quality:

- Software safety plan
- Safety requirements analysis
- Software safety design analysis
- Software safety code analysis
- Software safety test analysis
- Software safety change analysis

b. Describe the process for incorporating the software safety analysis into the facility Documented Safety Analysis (DSA).

10. Safety Software Quality Assurance personnel shall demonstrate a working level knowledge of activities that ensure that safety software is properly maintained and continues to operate as intended as described in such documents as IEEE 1219, *IEEE Standard for Software Maintenance* and Section 10 of NUREG/CR-6263, *High Integrity Software for Nuclear Power Plants*.

Supporting Knowledge, Skills, and Abilities

a. Discuss the following concepts as they relate to safety software quality:

- Software maintainability
- Maintenance planning
- Performance monitoring

b. Conduct or review an assessment of software maintenance on a project or program to a standard such as IEEE 1219, *IEEE Standard for Software Maintenance.*

11. Safety Software Quality Assurance personnel shall demonstrate a working level knowledge of software configuration management processes that ensure the integrity of executable code during the entire life cycle of safety software as described in documents such as ANSI/IEEE 828, *Software Configuration Management Plans*, ANSI/IEEE 1042, *Guide to Software Configuration Management*, and Section 11 of NUREG/CR-6263, *High Integrity Software for Nuclear Power Plants*.

Supporting Knowledge, Skills, and Abilities

a. Discuss the following concepts as they relate to safety software quality and explain how each is applied:

- Software configuration management plan
- Configuration identification
- Configuration change control
- Configuration status accounting
- Configuration audits and reviews
- External interface control
- Subcontractor and vendor control
- Automated support for configuration management

b. Perform an assessment of a contractor's software configuration management plan to verify compliance with applicable software requirements.

Software Management and Quality Assurance

12. Safety Software Quality Assurance personnel shall demonstrate a working level knowledge of the elements of a successful software quality assurance program.

Supporting Knowledge, Skills, and Abilities

a. Discuss the purpose, scope and content of the following types of software management plans as they relate to safety software quality:

- Software Project Management Plan
- Software Development Plan
- Software Safety Plan
- Software Quality Assurance Plan
- Software Test Plan
- Software Verification and Validation Plan
- Software Configuration Management Plan
- Software Integration Plan
- Software Maintenance Plan
- Software Installation Plan
- Software Operations Plan
- Software Training Plan

b. Identify and describe safety software procurement methods, including supplier evaluation and source inspection processes.

c. Prepare or review a real or example quality assurance plan for a software development project. Identify the project strengths and weaknesses.

d. Describe the elements of an acceptable software quality assurance program for the development, use, and maintenance of safety software that meets the criteria in:

- 10 CFR 830, Nuclear Safety Management
- DOE Order 414.1A, *Quality Assurance*
- DOE Order 200.1, *Information Management Program*

and applicable industry standards, including, but not limited to:

- ASME NQA-1, *Quality Assurance Program Requirements for Nuclear Facilities*
- ANSI/IEEE 730.1, *IEEE Standard for Software Quality Assurance Plans*.
- Add ANSI/ANS-10.4-1987; R1998: *Guidelines for the Verification and Validation of Scientific and Engineering Computer Programs for the Nuclear Industry*
- ISO 9001 Quality Management Systems – Requirements
- SEI Capability Maturity Model

e. Perform an assessment of safety software quality, including procurement activities, using guidance such as IEEE 1028, *IEEE Standard for Software Reviews* and DOE G 414.1-1, Management and Independent Assessments.

INTENTIONALLY BLANK

APPENDIX A
CONTINUING EDUCATION, TRAINING, AND PROFICIENCY PROGRAM

The following list represents suggested continuing education, training, and other opportunities that are available for DOE personnel after completion of the competency requirements in this technical Functional Area Qualification Standard. It is extremely important that personnel involved with this program maintain their proficiency through continuing education, training, reading, or other activities such as workshops, seminars, and conferences. The list of suggested activities was developed by the Subject Matter Experts involved in the development of the Functional Area Qualification Standard and is not all-inclusive.

LIST OF CONTINUING EDUCATION, TRAINING, AND OTHER ACTIVITIES

Safety Software Quality Assurance personnel shall participate in an Office/Facility-specific continuing training and qualification program that includes the following elements:

1. Continuing technical education and/or training covering topics directly related to the safety software quality assurance area as determined appropriate by management. This may include courses/training provided by Department of Energy, other government agencies, outside vendors, or local educational institutions. Continuing training topics should also address identified weaknesses in the knowledge or skills of the individual personnel.

2. Active performance of the duties of a Safety Software Quality Assurance specialist at a Department of Energy facility for a minimum of 160 hours per year.

3. Attendance at seminars, symposia, or technical meetings related to the development, use, and maintenance of safety software.

4. Self-study of new regulations, requirements, or advances related to the development, use, and maintenance of safety software.

5. Documenting continuing professional development activities in Individual Development Plans.

INTENTIONALLY BLANK

CONCLUDING MATERIAL

Review Activity:
EM
NNSA
EH
NE
SC

Preparing Activity:
DOE-EH-22

Project Number:
TRNG-0040

Field and Operations Offices
CBFO
CH
ID
OH
OR
ORP
RFFO
RL
SR

Area and Site Offices
Argonne Area Office
Brookhaven Area Office
Fermi Area Office
Kansas City Site Office
Livermore Site Office
Los Alamos Site Office
Nevada Site Office
Pantex Site Office
Princeton Area Office
Savannah River Site Office
Sandia Site Office
Y-12 Site Office