TS

NOT MEASUREMENT SENSITIVE

DOE-STD-1172-2011
March 2011

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 is available on the
Department of Energy
Technical Standards Program
Web Site at
http://www.hss.energy.gov/nuclearsafety/techstds/

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 Functional Area Qualification Standard for Department-wide application. Approval of this Qualification Standard by the Federal Technical Capability Panel is indicated by signature below.

Karen L. Boardman, Chairperson
Federal Technical Capability Panel

INTENTIONALLY BLANK

TABLE OF CONTENTS

INTENTIONALLY BLANK

ACKNOWLEDGMENT

The U.S. Department of Energy, Office of Health, Safety and Security (HSS) is the Champion and Sponsor for the Safety Software Quality Assurance (SSQA) Functional Area Qualification Standard (FAQS). The Sponsor is responsible for coordinating the development and/or review of the SSQA FAQS by subject matter experts to ensure that the technical content of the FAQS is accurate and adequate for Department-wide application for those involved in the SSQA Program. The Sponsor, in coordination with the Federal Technical Capability Panel, is also responsible for ensuring that this FAQS is maintained current.

The following individuals participated in the development and/or review of this FAQS:

- Subir Sen, HS-23 (Team Leader)
- Shiv Seth, HS-64
- Cliff Ashley, EM-RL
- Pranab Guha, HS-22
- Robert Blyth, DOE-ID
- Sherry Hardgrave, NNSA Y-12
- Teresa Perry, SC ORO
- Donna Riggs, SC ORO (Alternate)
- Anton Tran, NA-173
- Charles Thayer, HS-23 (Support)

INTENTIONALLY BLANK

U.S. DEPARTMENT OF ENERGY
FUNCTIONAL AREA QUALIFICATION STANDARD

Safety Software Quality Assurance

PURPOSE

DOE Order (O) 426.1, *Federal Technical Capability*, commits the Department to continuously strive for technical excellence. The Technical Qualification Program (TQP), 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 this FAQS should be aligned with and integrated into the recruitment and staffing processes for technical positions. This FAQS should form the primary basis for developing vacancy announcements, qualification requirements, crediting plans, interview questions, and other criteria associated with the recruitment, selection, and internal placement of personnel performing SSQA duties. The U.S. Office of Personnel Management (OPM) minimum qualifications standards will be greatly enhanced by application of appropriate materials from the technical FAQS.

The technical qualification standards are not intended to replace the OPM qualifications standards or other departmental personnel standards, rules, plans, or processes. The primary purpose of the TQP is to ensure that employees have the requisite technical competency to support the mission of the Department. The TQP forms the basis for the development and assignment of DOE personnel responsible for ensuring the safe operation of defense nuclear facilities.

APPLICABILITY

The SSQA FAQS establishes common functional area competency requirements for DOE personnel who provide assistance, or direction, guidance, oversight, or evaluation of safety software that includes: safety system software; safety and hazard analysis software and design software; and safety management and administrative controls software as defined in DOE O 414.1C, *Quality Assurance*. The Order identifies that DOE G 414.1-4, *Safety Software Guide for use with 10 CFR 830 Subpart A, Quality Assurance Requirements, and DOE O 414.1C, Quality Assurance* "provides acceptable implementation strategies and appropriate standards for these work activities." The Order further requires ASME NQA-1-2000, *Quality Assurance Requirements for Nuclear Facility Applications*, or other national or international consensus standards that provide an equivalent level of quality assurance requirements as NQA-1-2000, must be used to implement these work activities.

Knowledge of ASME NQA-1-2000 and DOE G 414.1-4 is important to SSQA personnel in performing their duties and responsibilities. For ease of transportability of qualifications between DOE elements, program and field offices are expected to use this technical FAQS without modification. Needed additional office-/site-/facility-specific technical competencies should be handled separately. Satisfactory and documented attainment of the competency requirements contained in this technical FAQS (see the Federal Technical Capability Program [FTCP] Directives and Standards page at http://www.hss.energy.gov/deprep/ftcp/directives/directives.asp for an example of the SSQA FAQS qualification card) ensures that personnel possess the minimum requisite competence to

fulfill their functional area duties and responsibilities common to the DOE complex. Additionally, office-/site-/facility-specific qualification standards supplement this technical FAQS and establish unique operational competency requirements at the Headquarters or field element, site, or facility level.

It should be noted that the competencies of management and leadership, general technical knowledge, regulations, administrative capability, and assessment and oversight are all embodied in the competencies listed in this standard. All of these factors have a bearing on safety. Although the focus of this standard is technical competence, competencies such as good communication, recognized credibility, ability to listen and process information, and the ability to guide an effort to get it right the first time are recognized as important aspects of safety.

IMPLEMENTATION

This SSQA FAQS identifies the minimum technical competency requirements for DOE personnel who have a responsibility for safety software. Although there may be other competency requirements associated with the positions held by DOE personnel, this technical FAQS is limited to identifying the specific technical competencies required throughout all defense nuclear facilities. The competency requirements define the expected knowledge and/or skill that an individual must meet. Each of the competency requirements is further described by a listing of supporting knowledge, and/or skill statements. The supporting knowledge and/or skill statements for each competency requirement are provided to challenge the employee in the breadth and depth of his/her understanding of the subject matter. In selected competencies, expected knowledge, and/or skill have been designated as “mandatory performance activities.” The mandatory performance activities are not optional.

The term “must” denotes a mandatory requirement, “should” denotes a recommended practice that is not required, and “may” denotes an option in this standard.

The competencies identify a familiarity level, a working level, or an expert level of knowledge; or they require the candidate 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 recognize the need to seek and obtain appropriate expert advice (e.g., technical, legal, safety) or consult appropriate reference materials required to ensure the safety of DOE 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 DOE practices.

Headquarters and field elements must establish a program and process to ensure that DOE personnel possess the competencies required of their position, including the competencies identified in this technical FAQS. Documentation of the completion of the requirements in the SSQA FAQS must be included in the employee's training and qualification record. Satisfactory

attainment of the competency requirements contained in this technical FAQS may be documented using the example SSQA FAQS qualification card that can be obtained from the Federal Technical Capability Program Directives and Standards page at http://www.hss.energy.gov/deprep/ftcp/directives/directives.asp.

Equivalencies should be used sparingly and 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 must be granted in accordance with the TQP plan of the site/office/Headquarters organization qualifying the individual. The supporting knowledge and/or skill statements and mandatory performance activities should be considered when granting equivalency for a competency.

Training must be provided to employees in the TQP who do not meet the competencies contained in this technical FAQS. 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 requirements. 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 SSQA FAQS competency requirements.

EVALUATION REQUIREMENTS

Attainment of the competencies listed in this technical FAQS must be documented in accordance with the TQP plan of the site/office/Headquarters organization qualifying the individual and the requirements in DOE M 360.1-1B, *Federal Employee Training Manual*, and DOE O 426.1.

Unless stated otherwise within the TQP plan, attainment of the competencies listed in the SSQA FAQS should be evaluated and documented by either a qualifying official or immediate supervisor, using any one or a combination of the following methods: (Note: if the immediate supervisor is not an SSQA engineer, it is expected that the supervisor consult with a qualified SSQA engineer.)

- Satisfactory completion of a written examination
- Satisfactory completion of an oral examination
- Satisfactory accomplishment of an observed task or activity directly related to a competency
- Documented evaluation of equivalencies without a written examination

Field element managers/Headquarters program managers must qualify candidates as possessing the basic technical knowledge, technical discipline competency, and position-specific knowledge, skills, and abilities required for their positions. Final qualification should be performed using one or a combination of the following methods:

- Satisfactory completion of a comprehensive written examination. The minimum passing grade should be 80 percent.

- Satisfactory completion of an oral examination by a qualified Senior Technical Safety Manager (STSM) or a qualification board of technically qualified personnel that includes at least one qualified STSM.
- Satisfactory completion of a walkthrough of a facility with a qualifying official for the purpose of verifying a candidate's knowledge and practical skills of selected key elements.

Guidance for oral interviews and written exams is contained in DOE-HDBK-1205-97, *DOE Handbook: Guide to Good Practices for the Design, Development, and Implementation of Examinations*, and DOE-HDBK-1080-97, *DOE Handbook: Guide to Good Practices for Oral Examinations*.

For oral examinations and walkthroughs, qualifying officials or board members should ask critical questions intended to integrate identified learning objectives during qualification. Field element managers/Headquarters program managers or designees should develop formal guidance for oral examinations and walkthroughs that includes:

- Standards for qualification
- Use of technical advisors by a board
- Questioning procedures or protocol
- Pass/fail criteria
- Board deliberations and voting authorization procedures
- Documentation process

INITIAL QUALIFICATION AND TRAINING

Qualification of SSQA personnel must be conducted in accordance with the requirements of DOE O 426.1.

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

- DOE
- 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 SSQA personnel are included in appendix A of this document.

DUTIES AND RESPONSIBILITIES

The following are the typical duties and responsibilities expected of personnel assigned to the SSQA functional area:

1 Support the DOE senior manager responsible for developing and implementing the DOE SSQA program consistent with DOE O 414.1C and other customer requirements.

2 Serve as a resource to DOE management and technical point of contact for SSQA activities.

3. Review safety and quality assurance documentation to ensure safety software is properly identified, evaluated and controlled.

4. Verify that safety software is developed, procured, verified, validated, used and maintained consistent with DOE O 414.1C.

5. Review and evaluate training and qualification programs for DOE and contractor personnel who develop, procure, verify, validate, use, or maintain safety software, or design, maintain, and implement SSQA programs.

6. Verify that DOE and the contractor's software quality assurance (SQA) programs, plans and processes are developed based on assessments of hazards and risks, and that these elements comply with DOE Orders and applicable requirements.

7. Develop and implement plans that monitor and evaluate DOE and contractor implementation of SSQA programs and processes, verifying adequacy, implementation effectiveness, and compliance with applicable DOE directives and requirements.

8. Lead/perform reviews, surveillances, and assessments of SSQA programs, plans and procedures and other oversight activities, document results, prepare reports, and monitor resulting actions.

9. Interface with DOE Headquarters and field elements, regulators, and stakeholders to ensure the effective implementation of DOE SSQA programs.

10. Verify all safety software is identified and graded in accordance with DOE O 414.1C and other applicable requirements.

11. Monitor contractor organization to ensure reportable occurrences involving safety software to ensure that lessons learned are captured and disseminated to appropriate organizations and individuals and that implementation of corrective actions is effective.

Position-specific duties and responsibilities for SSQA personnel are contained in their office/facility-specific qualification standard or position description.

BACKGROUND AND EXPERIENCE

The U.S. Office of Personnel Management's 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 SSQA personnel is:

1. Education:

   Baccalaureate degree in engineering, science, computer science, information technology 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.

2. Experience:

   Commercial, industrial, military, Federal, state, or other directly related experience that has provided specialized experience in software development, management, and quality assurance activities. Specialized experience can be demonstrated through possession of the competencies outlined in this FAQS.

   In addition to this education and experience, certifications from other professional societies such as National Lead Auditor Certification (e.g., ASME NQA-1 and ASQ), ASQ Certified Quality Engineer (CQE), ASQ Certified Software Quality Engineer (CSQE), ASQ Certified Manager of Quality (CMQ) or Institute of Electrical and Electronics Engineers (IEEE) Certification 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 DOE-STD-1146, *DOE Standard: General Technical Base Qualification Standard*. All SSQA 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 requirements is further described by a listing of supporting knowledge and/or skill statements that describe the intent of the competency statements. In selected competencies, expected knowledge and/or skills have been designated as "mandatory performance activities." In these competencies, the actions are not optional.

Note: When regulations, DOE directives, or other industry standards are referenced in the FAQS, the most recent revision should be used. It is recognized that some SSQA personnel may oversee facilities that utilize predecessor documents to those identified. In those cases, such documents should be included in local qualification standards via the TQP.

I. Software Management and Quality Assurance

1. **Safety software quality assurance personnel must demonstrate a working level knowledge of DOE quality assurance policy, programs, and processes contained in:**
   - **DOE O 414.1C, *Quality Assurance***
   - **10 CFR 830, Subpart A, "Quality Assurance"**

   Supporting Knowledge and/or Skills

   a. Discuss the purpose and interrelationships of DOE O 414.1C, and 10 CFR 830, Subpart A.

   b. Discuss the DOE and contractor requirements and responsibilities for development, review, approval, and implementation of a quality assurance program (QAP).

   c. Discuss and give an example of how the safety software inventory requirements specified in DOE O 414.1C can be met.

   d. Discuss the purpose, benefits, and restrictions of the graded approach in the implementation of DOE quality assurance requirements.

   e. Discuss the implementation of a software quality assurance program such as described in DOE G 414.1-4, *Safety Software Guide for use with 10 CFR 830 Subpart A, Quality Assurance Requirements, and DOE O 414.1C, Quality Assurance*.

   f. Discuss and give examples of how national or international consensus standards can be used in the development and implementation of work processes to provide an equivalent level of quality assurance requirements.

2. **Safety software quality assurance personnel must demonstrate a working level knowledge of the elements of a successful software quality assurance program.**

Supporting Knowledge and/or Skills

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

- Software project management plan
- Software risk 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 procurement and supplier management plan
- Software problem reporting and corrective action plan
- Software integration plan
- Software maintenance plan
- Software installation plan
- Software operations plan
- Software training plan
- Software retirement plan

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

c. Using the references below, describe the various elements of an acceptable safety software quality assurance program for the development, use, grading, and maintenance of safety software.

- 10 CFR 830, “Nuclear Safety Management”
- DOE O 414.1C, *Quality Assurance*
- DOE G 414.1-4, *Safety Software Guide for use with 10 CFR 830 Subpart A, Quality Assurance Requirements, and DOE O 414.1C, Quality Assurance*
- DOE O 200.1A, *Information Technology Management*
- ASME NQA-1-2000, *Quality Assurance Requirements for Nuclear Facility Applications,* including Part I, Part II Subpart 2.7 and Part IV Subpart 4.1
- IEEE 730.1, *IEEE Standard for Software Quality Assurance Plans*

II. Safety Software and System Relationship

3. **Safety software quality assurance personnel must demonstrate a working level knowledge of the types of safety software and grading levels.**

Supporting Knowledge and/or Skills

a. Explain the general characteristics, application, and safety significance of safety software including: safety system software; safety and hazard analysis software and

design software; safety management and administration controls software.

b. Given examples of safety software, identify the grading levels, and the applicable SQA work activities associated with the safety software (such as defined in DOE G 414.1-4, *Safety Software Guide for use with 10 CFR 830 Subpart A, Quality Assurance Requirements, and DOE O 414.1C, Quality Assurance*).

c. Describe the process for identifying safety software.

d. Describe the function of the following safety software types (such as defined in DOE G 414.1-4) and applications and provide an example of each:

- Custom developed
- Configurable
- Acquired
- Utility calculations
- Commercial design and analysis

e. Differentiate between real time and non-real time software.

4. **Safety software quality assurance personnel must demonstrate a familiarity level knowledge of the functional interfaces between safety system software and the system-level design.**

Supporting Knowledge and/or Skills

a. Identify how safety system-level requirements are established and then assigned to hardware, software, and human components.

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

c. Explain with an example how the functional interfaces between components and the system-level design are established and how the safety system software controls the safety functions of the subsystems, components, and interfaces.

5. **Safety software quality assurance personnel must demonstrate a familiarity level knowledge of the safety and engineering scenarios that are modeled by software.**

Supporting Knowledge and/or Skills

a. Explain with an example the sequence of steps that are typically followed in the development process of a safety analysis or design code such as the mathematical model and the associated computational model.

b. Identify and discuss with an example safety analysis scenarios appropriate to simulate with safety software.

c. Identify and discuss with an example appropriate uses of design software to assist with safety-related design decisions.

6. **Safety software quality assurance personnel must demonstrate a familiarity level knowledge of the relationships between nuclear hazards and the control and protection functions being addressed by safety management and administrative controls software.**

Supporting Knowledge and/or Skills

a. Identify how the software functional requirements of safety management and administrative controls software are defined, documented, and controlled relative to nuclear hazard controls and protection, risk management, and design constraints.

b. Given the scope of safety management and administrative controls software, explain how the radiological hazard controls and protection being addressed by the software were translated into software functional requirements, and how the software supports nuclear hazards risk management functions.

7. **Safety software quality assurance personnel must demonstrate a familiarity level knowledge of the purpose, features, and contents of the DOE safety software Central Registry.**

Supporting Knowledge and/or Skills

a. Discuss the purpose of the safety software Central Registry, and identify the current codes in the Central Registry.

b. Discuss the intent and use of the following documents as they relate to the codes in the safety software Central Registry:

- Code gap analysis report
- Code guidance report

c. Using DOE G 414.1-4, *Safety Software Guide for use with 10 CFR 830 Subpart A, Quality Assurance Requirements, and DOE O 414.1C, Quality Assurance,* as a reference, describe the SQA requirements that are applicable to the Central Registry codes and the SQA activities the DOE users need to perform for the Central Registry codes.

III. Software Engineering, Development, and Maintenance

8. **Safety software quality assurance personnel must demonstrate a working level knowledge of the software life-cycle processes.**

Supporting Knowledge and/or Skills

a. Discuss the differences between various life-cycle models such as waterfall, spiral, incremental, and evolutionary, and, how they relate to the software development process.

b. Describe each phase, associated SQA work activities, and products of a typical software life-cycle model such as the one described in DOE G 414-1-4, *Safety Software Guide for use with 10 CFR 830 Subpart A, Quality Assurance*

Requirements, and DOE O 414.1C, Quality Assurance and IEEE 1074, *IEEE Standard for Developing a Software Project Life Cycle Process*. Explain the roles of quality assurance, configuration management, and verification and validation in each phase.

9. **Safety software quality assurance personnel must demonstrate a working level knowledge of software requirements identification and management.**

Supporting Knowledge and/or Skills

a. Explain how software requirements specifications (SRS) are developed and used throughout the software life cycle.

b. Define and discuss the SRS attributes as they relate to safety software such as described in DOE G 414-1-4, *Safety Software Guide for use with 10 CFR 830 Subpart A, Quality Assurance Requirements, and DOE O 414.1C, Quality Assurance* and IEEE 830, *IEEE Recommended Practice for Software Requirements Specifications.*

c. Describe the purpose, scope, and content of SRS and requirements traceability matrix and describe the methods to ensure that all elements of the SRS are addressed.

d. Describe and give specific examples of the following software requirements such as described in DOE G 414.1-4:

- Functional
- Performance
- Access control
- Interface with safety requirements
- Installation considerations
- Design constraints

10. **Safety software quality assurance personnel must demonstrate a familiarity level knowledge of the safety software design concepts.**

Supporting Knowledge and/or Skills

a. Discuss the following software design concepts as they relate to safety software such as described in part in IEEE 1016, *IEEE Recommended Practice for Software Design Descriptions*:

- Modular design
- External interface
- Interfaces between both safety and non-safety components
- Interface integrity
- Data integrity
- Flow control
- Exception and error handling
- Simplicity
- Decoupling
- Isolation

- Software failure mode analyses

11. **Safety software quality assurance personnel must demonstrate a familiarity level knowledge of the safety software design and implementation practices.**

Supporting Knowledge and/or Skills

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
- Peer reviews

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

- Design specifications
- Program specifications
- Coding standards
- System design document
- Programmers manual
- Users manual

12. **Safety software quality assurance personnel must demonstrate a working level knowledge of the safety software verification and validation processes that ensure software will adequately fulfill all intended safety functions.**

Supporting Knowledge and/or Skills

a. Describe the following processes and documents as they relate to safety software verification and validation such as described in IEEE 1012, *IEEE Standard for Software Verification and Validation*:

- Validation of requirements
- Verification and validation of design
- Verification and validation of source code
- Unit/component testing
- Integration testing
- System testing
- Verification and validation test cases
- Verification and validation reports
- Verification and validation of tools
- Independent verification and validation
- Acceptance testing
- Installation and checkout testing

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

c. Use an example of a safety analysis or design code to explain the following:

- How verification primarily is the process of determining that the computational model represents the underlying mathematical model/solution.
- How validation is the process of determining that the model accurately represents the physical phenomenon/feature being modeled (predictive capability) from the perspective of its intended use.

d. Explain the differences in the verification and validation processes for various types and applications safety software.

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

f. Describe the relationships between test procedures, test cases, expected results, test data, and actual results.

13. **Safety software quality assurance personnel must demonstrate a familiarity level knowledge of software safety analysis.**

Supporting Knowledge and/or Skills

a. Discuss the purpose and content of the following and relate the importance of each to software safety analysis, such as described in DOE G 414-1-4, *Safety Software Guide for use with 10 CFR 830 Subpart A, Quality Assurance Requirements, and DOE O 414.1C, Quality Assurance* and IEEE 1228, *IEEE Standard for Software Safety Plans.*

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

14. **Safety software quality assurance personnel must demonstrate a familiarity level knowledge of activities that ensure that safety software will be properly maintained and will continue to operate as intended.**

Supporting Knowledge and/or Skills

a. Discuss the following concepts as they relate to safety software maintenance and operation such as described in IEEE 1219, *IEEE Standard for Software Maintenance*:

- Software maintainability
- Maintenance planning
- Performance monitoring
- Preventative maintenance

15. **Safety software quality assurance personnel must demonstrate a working level knowledge of software configuration management.**

Supporting Knowledge and/or Skills

a. Discuss the following concepts as they relate to safety software configuration management such as described in IEEE 828, *IEEE Standard for Software Configuration Management Plans* and explain how each is applied:

- Software configuration management plan
- Configuration identification
- Configuration change control
- Configuration status accounting
- Configuration audits and reviews
- Subcontractor and vendor control
- Software configuration management tools, including source code control tools

b. Review and evaluate an unreviewed safety question (USQ) determination associated with software including any proposed change or potential inadequacy.

c. Discuss the process of problem reporting and corrective actions and its implementation related to software configuration management.

IV. Safety Software Assessments

16. **Safety software quality assurance personnel must demonstrate the ability to perform an assessment of safety software quality using appropriate DOE directives and standards and industry standards.**

Mandatory Performance Activities

a. Participate in and document one or more SQA assessments that demonstrate the ability to adequately assess SQA work activities selected from the following as described in DOE O 414.1C, *Quality Assurance* and DOE G 414.1-4, *Safety Software Guide for use with 10 CFR 830 Subpart A, Quality Assurance Requirements, and DOE O 414.1C, Quality Assurance*

- Software project management and quality planning
- Software risk management
- Software configuration management.
- Procurement and supplier management
- Software requirements identification and management
- Software design and implementation
- Software safety
- Verification and validation
- Problem reporting and corrective action
- Training of personnel in the design, development, testing, use, and evaluation of safety software.

b. Safety software quality assurance personnel must demonstrate through an assessment the ability to evaluate safety software in relation to the safety basis, and explain how any changes that may affect the safety software function are controlled. The following are examples of activities that may demonstrate this ability:

- Identify and discuss the safety function of safety software related to the prevention or mitigation of hazards or accidents identified in the safety basis documentation. Additionally, identify the facility equipment and/or system by walking down with a cognizant system engineer.
- Review the function of safety software that controls a safety function as defined in a technical safety requirement (TSR) or an administrative control, including the technical basis for the control.
- Review permanent or temporary changes made to a safety system digital instrumentation and control (I&C) that involve changes to safety software configuration and implementation; evaluate how those changes were processed through the facility's USQ procedures; review how any changes made to the safety software were documented and review verified; and how any changes to the safety basis documentation or facility procedures were implemented. Summarize the review activity along with any observations and insights gained.
- Identify some of the major input parameters of a safety software and summarize how they are being controlled to prevent any undesired changes.

APPENDIX A
CONTINUING EDUCATION, TRAINING AND PROFICIENCY PROGRAM

The following list represents suggested continuing education, training, and other activities that are available for DOE personnel after completion of the competency requirements in this FAQS. 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 FAQS and is not all-inclusive.

LIST OF CONTINUING EDUCATION, TRAINING, AND OTHER ACTIVITIES

It is suggested that participation in the following activities support the maintenance of proficiency in the SSQA functional area after completion of competencies in the standard and the requirements of the Technical Qualification Program:

1. Continuing technical education and/or training covering topics directly related to the SQA area as determined appropriate by management. This may include courses/training provided by DOE, other government agencies, outside vendors, or local educational institutions.

2. Training covering topics that address identified deficiencies in the knowledge and/or skills of SSQA personnel.

3. Training in areas added to the SSQA FAQS since initial qualification.

4. Attend seminars, workshops, symposia, or technical meetings related to SQA.

5. Engage in self-study of new regulations, requirements, or advances related to SQA.

6. Participation in activities required to maintain QA related certification, such as:

    - Lead Auditor Certification (e.g., ASME NQA-1 and ASQ)
    - ASQ Certified Quality Engineer (CQE)
    - ASQ Certified Software Quality Engineer (CSQE)
    - ASQ Certified Manager of Quality (CMQ)

7. Training in the scope and application of DOE’s overall QA requirements of 10 CFR 830 Subpart A and DOE Order 414.1C as they relate to software used in nuclear activities.

8. Specific continuing training requirements must be documented in individual development plans.

9. Participation in activities such as: SSQA-related audits, assessments, surveillances, and operational readiness reviews.

RESOURCES:

Department of Energy
Office of Health, Safety and Security
Software Quality Assurance
http://www.hss.doe.gov/nuclearsafety/qa

Institute of Electrical and Electronics Engineers, Inc. (IEEE)
3 Park Avenue, 17th Floor
New York, New York 10016-5997
http://www.computer.org/portal/site/ieeecs/index.jsp

American Society for Quality (ASQ)
600 North Plankinton Avenue
Milwaukee, WI 53203
http://www.asq.org/

Software Engineering Institute (SEI)
4500 Fifth Avenue
Pittsburgh, PA 15213-2612
http://www.sei.cmu.edu/

APPENDIX B
REFERENCES AND RESOURCE DOCUMENTS

This appendix provides a list of reference documents as well as several pertinent standards and reports. The identified resource materials are not intended to be all inclusive, but do provide significant information for self-study.

10 CFR 830, Subpart A, “Quality Assurance Requirements”
10 CFR 830, Subpart B, “Safety Basis Requirements”
DOE G 414.1-4, *Safety Software Guide for use with 10 CFR 830 Subpart A, Quality Assurance Requirements, and DOE O 414.1C, Quality Assurance*
DOE O 200.1A, *Information Technology Management*
DOE O 414.1C, *Quality Assurance*
DOE O 420.1B, chg 1, *Facility Safety*
DOE O 430.1B, chg 1, *Real Property Asset Management*

ASME NQA-1-2000, *Quality Assurance Program Requirements for Nuclear Facility Applications:*
Part I, *Requirements for Quality Assurance Programs for Nuclear Facilities*
Part II, *Subpart 2.7, Quality Assurance Requirements for Computer Software for Nuclear Facility Operations*
Part IV, *Subpart 4.1, Application Appendix—Guide on Quality Assurance Requirements for Software.*
ASME V&V 10-2006, *Guide for Verification and Validation in Computational Solid Mechanics*

IEEE 7-4.3.2, *Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations*
IEEE 730.1, *IEEE Guide for Software Quality Assurance Planning*
IEEE 828, *IEEE Standard for Software Configuration Management Plans*
IEEE 829, *IEEE Standard for Software Test Documentation*
IEEE 830, *IEEE Recommended Practice for Software Requirements Specifications*
IEEE 1008, *IEEE Standard for Software Unit Testing*
IEEE 1012, *IEEE Standard for Software Verification and Validation*
IEEE 1016, *IEEE Recommended Practice for Software Design Descriptions*
IEEE 1028, *IEEE Standard for Software Reviews*
IEEE 1042, *IEEE Guide to Software Configuration Management*
IEEE 1074, *IEEE Standard for Developing a Software Project Life Cycle Process*
IEEE 1219, *IEEE Standard for Software Maintenance*
IEEE 1228, *IEEE Standard for Software Safety Plans*
IEEE/EIA 12207.2-1997 *Industry Implementation of International Standard ISO/IEC 12207: 1995: Information Technology—Software Life Cycle Processes—Implementation Considerations,* IEEE and EIA, 1998.

ISO/IEC 15288, *System Life Cycle Processes*

NUREG/CR 6263, *High Integrity Software for Nuclear Power Plants*

Regulatory Guide 1.152*, Criteria for Digital Computers in Safety Systems of Nuclear Power Plants*

Software Engineering Institute (SEI) Capability Maturity Model Integration

Christensen, Mark J., and Richard H. Thayer, *The Project Manager's Guide to Software Engineering's Best Practices*, Institute of Electrical and Electronics Engineers (IEEE) Computer Society Press, 2001.

Herrmann, Debra S., *Software Safety and Reliability: Techniques, Approaches, and Standards of Key Industrial Sectors (Practitioners),* IEEE Computer Society, 2000.

Leveson, Nancy, Safeware: *System Safety and Computers*, Addison Wesley, 1995.

Pressman, Roger S., *Software Engineering: A Practitioner's Approach*, McGraw Hill, 1992.

CONCLUDING MATERIAL

Review Activity:	Field and Operations Offices	Preparing Activity:
HSS	CBFO	HS-23
NNSA	CH	
EM	ID	**Project Number:**
NE	OH	TRNG-0054
SC	OR	
CTA/CNS	ORP	
CTA/CDNS	RL	
	SR	

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