CRAD - 4.2.4.1
Revision 3
October 24, 2003

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

October 24, 2003

TABLE OF CONTENTS

ACRONYMS

ANS	American Nuclear Society
ASME	American Society of Mechanical Engineers
CFR	Code of Federal Regulations
COTS	Commercial Off-the-Shelf
CRAD	Criteria Review and Approach Document
DSA	Documented Safety Analysis
DNFSB	Defense Nuclear Facilities Safety Board
DOE	U.S. Department of Energy
EH	Office of Environment, Safety and Health
I&C	Instrumentation and Controls
IEEE	Institute of Electrical and Electronics Engineers
IP	Implementation Plan
M&O	Management and Operating
NRC	Nuclear Regulatory Commission
PLC	Programmable Logic Controller
PSO	Program Secretarial Officer
QA	Quality Assurance
SAR	Safety Analysis Report
SC	Safety Class
SCADA	Supervisory Control and Data Acquisition
SCM	Software Configuration Management
SDD	Software Design Description
SRD	Software Requirement Description
SQA	Software Quality Assurance
SS	Safety-Significant
SSC	Structure, System, and Component
TSR	Technical Safety Requirement
UCNI	Unclassified Controlled Nuclear Information
USQ	Unreviewed Safety Question
USQD	Unreviewed Safety Question Determination
V&V	Verification and Validation

GLOSSARY

Acquired Software - Software that was neither developed nor modified by the Department of Energy (DOE) or its management and operating (M&O) contractor, and that was obtained from a source outside DOE.

Custom Software - Software that is developed or acquired and modified by DOE or its M&O contractor.

Nuclear Facility – A reactor or a nonreactor nuclear facility where an activity is conducted for, or on behalf of, DOE and includes any related area, structure, facility, or activity to the extent necessary to ensure proper implementation of the requirements established in the Code of Federal Regulations (CFR), part 10, section 830. [10 CFR 830]

Safety Analysis and Design Software – Computer software that is not part of a system, structure, or component (SSC), but is used in the safety classification, design, and analysis of nuclear facilities to:

- Ensure the proper accident analysis of nuclear facilities,
- Ensure the proper analysis and design of safety SSCs,
- Ensure the proper identification, maintenance, and operation of safety SSCs.

Safety-class structures, systems, and components (SC SSCs) - Structures, systems, or components, including portions of process systems, whose preventive and mitigative function is necessary to limit radioactive hazardous material exposure to the public, as determined from the safety analyses. [10 CFR 830]

Safety-significant structures, systems, and components (SS SSCs). Structures, systems, and components which are not designated as safety-class SSCs, but whose preventive or mitigative function is a major contributor to defense in depth and/or worker safety as determined from safety analyses. [DOE G 420.1]

Safety Software – as referenced and defined in this Implementation Plan, includes both safety system software and safety analysis and design software.

Safety SSCs – This term applies to both safety-class structures, systems, and components, and safety-significant structures, systems and components for a given facility. [10 CFR 830]

Safety System Software – Computer software and firmware that performs a safety system function as part of a SSC that has been functionally classified as SC or SS. This also includes computer software such as human-machine interface software, network interface software, programmable logic controller (PLC) programming language software, and safety management databases, that are not part of an SSC but whose operation or malfunction can directly affect SS and SC SSC function.

Software – Computer programs, operating systems, procedures, and associated documentation and data pertaining to the operation of a computer system. [Institute of Electrical and Electronics Engineers *(IEEE) Std. 610.12-1990, IEEE Standard Glossary of Software Engineering Terminology*]

Assessment Criteria and Guidelines for Determining the Adequacy of Software Used in the Safety Analysis and Design of Defense Nuclear Facilities

1.0 INTRODUCTION

This document contains software quality assurance (SQA) assessment criteria and guidelines for assessing the safety software currently in use in the safety analysis and design of structures, systems and components (SSCs) in Department of Energy (DOE) defense nuclear facilities. The criteria and guidelines fulfill Commitment 4.2.4.1 of the Implementation Plan (IP) for Defense Nuclear Facilities Safety Board (DNFSB) Recommendation 2002-1, *Quality Assurance for Safety Software at Department of Energy Defense Nuclear Facilities*.

Commitment 4.2.4 of the IP specifies three actions DOE will take to assess the processes in place to ensure that the safety software currently used in the analysis and design of defense nuclear facilities is adequate. Commitment 4.2.4.1 requires the Office of Environment, Safety and Health (EH) to develop and issue a Criteria Review and Approach Document (CRAD) for the identification, selection, and assessment of that safety software. Commitments 4.2.4.2 and 4.2.4.3 require the Program Secretarial Officers (PSOs) and Field Element Managers to develop a schedule and complete the assessments using this CRAD.

This document is organized as follows:

- The ***Background*** section describes the use of safety software in DOE defense nuclear facilities and the Board's concern about the safety of such facilities if faulty or unqualified software is used.
- The ***Assessment Guidelines*** section covers the purpose, scope, guiding principles, and assessment methodology for assessing the processes currently in use for ensuring the adequacy of safety analysis and design.
- The ***Criteria and Approach*** section presents the objectives, criteria, and approach for each of the following topical areas: (1) Software Requirement Description, (2) Software Design Description, (3) Software User Documentation (4) Software Verification and Validation, (5) Software Configuration Management, (6) Software Quality Assurance, (7) Software Procurements, (8) Software Problem Reporting and Corrective Action.
- The ***Report Format*** section provides a suggested report format.
- The ***References*** section lists selected references relevant to SQA.

2.0 BACKGROUND

The Defense Nuclear Facilities Safety Board (DNFSB) issued Recommendation 2002-1 on September 23, 2002. The Board stated in Recommendation 2002-1 that the robustness and reliability of many structures, systems, and components (SSCs) throughout DOE's defense nuclear complex depend on the quality of the software used to analyze and guide these decisions, the quality of the software used to design or develop controls, and proficiency in use of the software. In addition, software that performs safety-related functions in distributed control systems, supervisory control and data acquisition (SCADA) systems, and programmable logic controllers (PLCs) requires the same high quality needed to provide adequate protection for the public, workers, and the environment. Other types of software, such as databases used in safety management activities, can also serve important safety functions, and deserve a degree of quality assurance commensurate with their contribution to safety.

The Department completed its own analysis of the Board's Recommendation and evaluated the impact of potential safety software problems on safety systems that protect the public, workers, and the environment. The Department agreed that potential weaknesses in this type of software could negatively impact these safety systems. The Department accepted the Board's Recommendation and committed to developing an IP on November 21, 2002. DOE prepared and submitted an IP to the Board on March 13, 2003, that, when completed, will result in the following:

- Clear assignment of organizational roles, responsibilities, and authorities for safety software,
- Establishment of the infrastructure necessary to ensure an effective SQA program, including personnel with the appropriate skill and expertise,
- Implementation of processes to identify safety analysis and design codes and to ensure that they are subject to verification and validation (V&V) appropriate for the application,
- Establishment of requirements and guidance for a rigorous SQA process that will include the use of Federal agency or industry standards where practical, and
- A process that will track continuous improvements and initiatives in software technology.

The scope of the 2002-1 IP includes safety software at the Department's defense nuclear facilities. *Safety software*, as defined by the IP, includes both safety system software and safety analysis and design software. *Safety system software* is computer software and firmware that performs a safety system function as part of a SSC that has been functionally classified as Safety Class (SC) or Safety Significant (SS). This also includes computer software such as human-machine interface software, network interface software, PLC programming language software, and safety management databases that are not part of an SSC, but whose operation or malfunction can directly affect SS and SC SSC function. *Safety analysis and design software* is software that is not part of an SSC but is used in the safety classification, design, and analysis of nuclear facilities to ensure the proper accident analysis of nuclear facilities, ensure the proper analysis and design of safety SSCs, and ensure the proper identification, maintenance, and operation of safety SSCs.

3.0 ASSESSMENT GUIDELINES

3.1 Purpose and Scope

These guidelines and criteria provide a consistent overall framework for assessment of the processes that are currently in place to ensure that the software being used in the safety analysis and design of the SSCs in defense nuclear facilities is adequate. These reviews will be conducted only on software that is currently in use, not on software that was previously used as part of a safety analysis and design process.

Should an issue arise that questions the validity of software previously used to support design or development, it will be resolved using the Unreviewed Safety Question (USQ) process. Generic USQs will be used to the extent possible rather than multiple facilities developing separate USQ Determinations (USQDs) for the same problem.

Individual sites should tailor the scope of this assessment to suit the specific usage of analysis and design software in their safety systems. The types of safety analysis and design software that will be considered in the subject assessment are listed below.

- Custom software developed by DOE, its contractors, or subcontractors for use with SS or SC SSCs,
- Commercial off-the-shelf (COTS) software,
- Calculation software, such as spreadsheets and math programs (along with their associated user files), used to perform safety analysis and design calculations, and
- Database programs and associated user files used to maintain control of information that has nuclear safety implications.

3.2 Guiding Principles

The following principles should guide the conduct of the assessment. The assessment team leader, with assistance from the DOE site manager responsible for these assessments, should ensure that these guiding principles are incorporated in the tailoring process for assessments of safety analysis and design software applications. Therefore, each of these principles is not duplicated in the Objective and Criteria and Approach sections that follow.

- SQA assessments of analysis and design software should begin with a determination of all existing software to which this Criteria and Approach document applies. The team should request the facility staff to identify safety analysis and design software used in safety-related (SS and SC) SSCs as identified in the Documented Safety Analysis (DSA), the facility Safety Analysis Reports (SARs), and the Technical Safety Requirements (TSRs). The team should then draw a representative sample of safety analysis and design software, and the assessment should be limited to the representative sample to avoid unnecessary and excessive assessments.

- The team should review previous assessments, such as DNFSB Recommendation 2000-2 IP reviews and SQA reviews, to gather data as appropriate. This review will enable the team to understand previous assessments, analysis and design software qualification processes, associated requirements and performance criteria, assumptions concerning system operations, and the role of safety analysis and design software in operations.

- Review of SQA processes for existing safety analysis and design software should not involve a detailed software review. Rather, it should involve a review of the associated SQA process and documented evidence that the SQA standards were applied for software development, procurement, and use.

- Care should be taken to balance the effort invested during the assessment in verifying the SQA processes and its associated documentation against the demonstrated effect on improving software quality and safety and on eliminating the costly errors that result from misunderstood requirements.

- The team should review any lessons learned from past events associated with analysis and design software applications and include any additional attributes as appropriate in the site-specific Assessment Plan.

- The facility staff should assist the team with understanding the associated SQA process, provide documented evidence to the team that the appropriate SQA standards were applied to software development, procurement, or use, and provide a staff contact for further information.

- Procedures and records for analysis and design software V&V, testing, and maintenance will be evaluated to determine whether they are appropriate and are being used to verify that software requirements and performance criteria described in the software requirement documentation are satisfied.

- If the team identifies a condition that poses an imminent threat to personnel or facility safety, line management is notified immediately. Team personnel should immediately point out the imminent threat condition to their points of contact or the appropriate facility manager, and notify the assessment team leader as soon as practical.

- For design software, including COTS and proprietary software, it is not the intent of the assessment to evaluate individual codes. Instead, the assessment should verify that, for work activities using safety COTS and proprietary software, procurement and other software control processes are in place to ensure that the software used would be adequate.

3.3 Assessment Methodology

The team should address the following major activities:

- The team shall prepare an Assessment Plan using the CRAD and develop a question set with lines of inquiry and detailed attributes as appropriate for site-specific applications. The plan should include qualification requirements for team members, a listing of team members and their biographies, a plan for the pre-assessment visit, and guidance for preparing the report.

- The CRAD is prepared to address safety and analysis software applicable to both SC and SS SSCs as defined in the facility DSA, SAR, or TSR. Software classification should be consistent with SSC classification unless otherwise justified for case-specific application. The team should use facility-specific DSAs, SARs, and TSRs to select software within the scope.

- The team should review the applicable standards for assistance in developing the lines of inquiry and to determine their appropriateness for the analysis and design software under assessment. The

applicable standards may be obtained from the facility staff or EH. As part of Commitment 4.3.1 of the IP, EH will conduct a review to identify the industry and Federal agency standards that are applicable to SQA. The results of this review will be available to the team. The References section of this CRAD includes additional industry standards and guidelines.

- The team should select a representative sample of analysis and design software for the assessment and select a limited number of requirements and follow them down through each phase of the development process to evaluate the thoroughness of the process and to confirm that the code properly implements the requirements. The team should select the software based in part on its safety implications.
- The team will review existing SQA documentation for the software and evaluate the adequacy of the existing SQA processes that ensure adequacy of the existing analysis and design software used for safety SSCs.
- The team should use interview methods as well as informal discussions with program developers, users, and sponsors to supplement and complement the documented information.
- For analysis and design software used by DOE contractors and subcontractors, the team should evaluate the SQA program under which the software was developed, verified, validated, and controlled.
- For acquired software, the team should evaluate the procurement process and other programmatic controls used to ensure that the software was acceptable for use in the SC or SS application.
- V&V information for existing software may not be appropriately documented. For an *a posteriori* review, the Team must determine if any of the documentation, such as a problem statement, requirements specification, design specification, test plan, or test results is available. In situations where clearly identifiable formal documents do not exist, sufficient information may be contained in the program documentation for the level of V&V review selected. The *a posteriori* review may also take advantage of user experience. The team, however, should identify any software where an *a posteriori* V&V review may be warranted.

A suggested sequence for this assessment includes team selection, site-specific tailoring, preparation, pre-assessment visit, onsite assessment, and reporting.

Team Selection

Assessment team leader and team member selection processes should be consistent with the following guidance.

Team leader:
- Is appointed by the field element manager.
- Should be experienced in assessment techniques and leadership of teams.
- Should be a Federal employee.
- Should not be in the line organization of the facility for the software under assessment.
- Should document technical and lead capabilities in a short biographical sketch, which is included in the assessment report.

Team members:
- Should have demonstrated capability in performing technical assessments of safety analysis and design software.
- Should have as a group, working knowledge of hazard and safety analysis, safety classification of SSCs within defense nuclear facilities, software development practices, systems engineering, analysis and design software applications, and quality assurance practices.
- Can be Federal employees, site contractors, or subcontractor experts.
- Can be from any DOE field site or Headquarters office or their contractors or subcontractors.
- Should not have contractor line management responsibility for the software under assessment.
- Should be selected by the assessment team leader, in consultation with the DOE site manager.
- Should document technical capabilities in a short biographical sketch, which is included in the assessment report.

Tailoring

The assessment criteria and guidelines herein have not been developed for a specific analysis and design application. Therefore, in some cases it will be necessary to tailor the assessment criteria and guidelines to focus the assessment to address those aspects determined to be appropriate for the agreed-upon assessment scope. The tailoring process is intended to ensure that the assessments are conducted in accordance with the criteria and guidelines that are appropriate and applicable to each specific situation. The assessment criteria and guidelines in this CRAD are provided as a tool for use in developing specific criteria and guidelines. It is recognized that some of the criteria may not apply. This should be noted in the assessment report.

These assessment criteria and guidelines are intended to be flexible, and may be tailored to allow the most cost-effective use of resources in determining the adequacy of the safety analysis and design software currently used at defense nuclear facilities. The tailoring process may take into account considerations such as recently completed assessments, evaluations, studies, inspections, and other relevant factors. For each assessment, the tailoring performed and the associated rationale shall be agreed upon prior to the start of the assessment and documented in the assessment report.

The team should consider the level of modification to the software when evaluating the adequacy of the SQA processes. In general, acquired software, such as COTS, may not be modified by the user and can be viewed within the system as a “black box.” Custom software is completely modifiable, and may require

additional SQA processes over that of acquired software. Some acquired software can be configured specifically for its application or source code modified to meet application-specific requirements. In these instances, a higher level of SQA requirements should be expected.

Information for existing software may not be appropriately documented. The team should determine if any of the documentation, such as a problem statement, requirements specification, design specification, test plan, or test results is available. In situations where clearly identifiable formal documents do not exist, sufficient information may be contained in other documentation.

For software that has been in use for several years, the team should consider using an approach similar to the *a posteriori* review described in ANS 10.4. These approaches take advantage of available program development products and program staff as well as the experience of the users. The purpose of the *a posteriori* review is to determine if the system produces valid responses when used to analyze problems within a specific domain of applications. The level of *a posteriori* review may range from a simple demonstration that the program produces reasonable results for a representative sample of problems, to a rigorous verification of program requirements, design, coding, test coverage, and evaluation of test results. The team may consider using documented engineering judgments (including their bases) and test results to extrapolate the available existing information to establish functional and performance capabilities.

Preparation and Optional Pre-Assessment Site Visit

Information needed to understand the analysis and design functions, design, configuration management, level of modification, and other SQA requirements should be requested from the facility staff. This information should be reviewed to identify safety functions, software requirements, performance criteria, and additional details required for performing the assessment.

Based upon these documents, the team should develop lines of inquiry for interviews and observations during the onsite assessment.

The team leader, with the assistance of the DOE field office manager responsible for the assessment, should prepare a list of facility and software development staff to be interviewed. Lines of inquiry should be matched with the interview list and assigned to specific team members.

The team leader, DOE field office manager responsible for the assessment, and point of contact for the facility should have an active dialog during this time to gather additional information for the team and to clarify any issues.

Onsite Assessment

If appropriate, a short entrance meeting should be held by the assessment team leader. This meeting should include the facility staff, DOE field office personnel, and the team. The information should be limited to the topics covered in the assessment criteria. Suggested meeting content includes:

- Identification of the agreed-upon boundaries for the assessment
- Assessment schedule, including interviews
- Introduction of the team
- Overview of the use of the analysis and design software
- Points of contacts and escorts

- Any administrative support arrangements

Once the team has developed an understanding of the facility-specific conditions and layout, the team should conduct the interviews. During the onsite assessment, additional documentation may be requested and reviewed as appropriate. The interaction between the team, the DOE field office personnel, and facility staff should be frequent and informal.

Briefing and Reporting

After completion of the assessment, the team leader and site management should arrange a briefing with appropriate facility and DOE field management on the assessment results. The team leader will send the final report summarizing the results of the assessment to the field element manager. The report will state whether the assessment criteria were satisfied, and may contain areas for improvement and observations for consideration by the field office or contractor. Recommended actions may also be included.

4.0 CRITERIA AND APPROACH

The Criteria and Approach section is divided into the following topical areas:

- Software Requirement Description (SRD)
- Software Design Documentation (SDD)
- Software User Documentation
- Software V&V
- Software Configuration Management (SCM)
- Software Quality Assurance (SQA)
- Software Procurements
- Software Problem Reporting and Corrective Action

Each of these topical areas includes:

- ***Objective:*** Describes the assessment objective for the topical area and the intended contribution to the adequacy of the safety software.

- ***Criteria:*** Suggests characteristics of safety software that should be verified. Because application of standards at DOE sites varies, reference to specific standards for topical areas is not cited. Instead, generally used Federal agency and industry standards are listed in the References section of this document.

- ***Approach:*** Suggests information needed to assess the adequacy of the safety software in accordance with the criteria. The items in the *Approach* section are provided to guide the team; however, the team may choose to select another approach to meet assessment-specific needs.

Existing quality assurance (QA) or other requirements (e.g. procurement) for safety software may satisfy some of the objectives and criteria that follow. Previous reviews may also contain information relevant to this assessment that can be cited and used in this assessment. In such situations, this assessment should be limited to objectives and criteria not covered in previous assessments, and should not unnecessarily duplicate previous assessments.

A variety of software engineering methods may exist within various DOE field elements to meet applicable SQA requirements. These requirements should be commensurate with the risk associated with a software failure. Factors affecting this risk include the potential impact on safety or operation, complexity of computer program design, degree of standardization, state of the art, and comparison with previously proven computer programs.

For each of the eight topical areas that follow, the SQA standards and guidance being applied by the contractor should be documented in the assessment report along with the assessment team's judgment of their appropriateness for the specific software application, and the effectiveness of their implementation.

Simple, easily understood calculational software and tools, such as spreadsheets and mathematical utility software that are used in the analysis and design of SSCs, may not need to meet all aspects of the criteria if the designs using these computer programs are individually verified. Design verification

documentation should include design inputs, generated results from the calculational software program, and the computer-generated source listing, algorithms, equations, spreadsheet cell contents, and macros. However, frequent use of the software may justify applying the criteria in order to simplify the review as well as to ensure integrity of repeated use of the software. For multiple-use calculational software, configuration management of user-developed files is essential to maintaining the integrity of the results of its use.

Complex computer programs used in the safety analysis and design of SSCs should be developed and approved for use in accordance with these criteria unless software design verification and testing of the computer program (or parts thereof), independent of a specific application of the computer program, is not practical. In such cases, each application of the computer program must be design-verified and documented to ensure that the software will perform its intended function.

4.1 Software Requirements Description

Objective:

Analysis and design software functions, requirements, and their bases are defined and documented.

Criteria:

1. The functional and performance requirements for the analysis and design software are complete and detailed to perform software design.
2. The SRD is reviewed, controlled, and maintained.
3. Each requirement should be uniquely identified and defined such that it can be objectively verified and validated.

Approach:

Determine the existence of SRD documentation, either as a standalone document or embedded in another document, and ensure that it specifies, as applicable, the following:

- Functionality - the functions the software is to perform,
- Performance - the time-related issues of software operation such as speed, recovery time, and response time,
- Design constraints imposed on implementation-phase activities - any elements that will restrict design options,
- Attributes - non-time-related issues of software operation such as portability, acceptance criteria, access control, and maintainability, and
- External interfaces - interactions with people, hardware, and other software.

Determine whether the documents containing the SRD are controlled under configuration change control and document control processes. Verify that the SRD is reviewed and updated as necessary for completeness, consistency, and feasibility for developing a usable code.

Identify the standards and guidelines from applicable site/facility procedures, Federal, or industry standards that are applied to the development of the software. Determine their appropriateness and adequacy for the specific analysis and design software under assessment.

If the above requirements are not available, the perceived software requirements may be identified through available documentation and discussions with the program developer, users, and sponsor. These perceived requirements would then be used as the basis for other topical area assessment activities.

4.2 Software Design Description

Objective:

The SDD depicting the major components of the software design is defined and documented.

Criteria:

1. All software-related requirements are implemented in the design.
2. All design elements are traceable to the requirements.
3. The SDD is reviewed, controlled, and maintained.

Approach:

Review the appropriate documents, such as vendor specifications for analyzing and designing software, a description of the components and subcomponents of the software design, including databases and internal interfaces, etc. The design may be documented in a standalone document such as an SDD or embedded in other documents. The SDD should contain the information listed below:

- A description of the major safety components of the software design as they relate to the software requirements
- A technical description of the software with respect to control flow, control logic, mathematical model, and data structure and integrity
- A description of the allowable or prescribed ranges for inputs and outputs
- A description of error handling strategy and use of interrupt protocols
- The design should be described in a manner suitable for translating into computer codes

Determine whether the documents containing the software requirement description are controlled under configuration change control and document control processes. Verify that these documents are reviewed and updated as necessary for completeness, consistency, technical adequacy, and correctness.

In instances where the software the design is not available, the contractor may be able to construct a design summary on the basis of available program documentation, review of the source code (if applicable), and information from the facility staff. Care should be taken to ensure that such a design summary is consistent with the complexity and importance of the software to the safety functions.

4.3 Software User Documentation

Objective:

Software documentation is available to guide the user in installing, operating, managing, and maintaining the software.

Criterion:

1. The system requirements and constraints, installation procedures, and maintenance procedures such as database fine-tuning are clearly and accurately documented.
2. Any operational data system requirements and limitations are clearly and accurately documented.
3. Documentation exists to aid the users in the correct operation of the software and to provide assistance for error conditions.
4. Appropriate software design and coding documentation to assist in any future software modifications is defined and documented.

Approach:

The team will review the user's manual and related documents. These documents may exist either as a standalone document or embedded in other documents. The user documentation should contain:

- User instructions that contain an introduction, a description of the user's interaction with the software, and a description of any required training necessary to use the software
- Input and output specifications appropriate for the function being performed
- A description of error messages or other indications as a result of improper input or system problems and user response
- Information for obtaining user and maintenance support
- A description of system requirements and limitations such as operating system versions, minimum disk and memory requirements, and any known incompatibilities with other software
- A description of any system requirements or limitations for operational data, such as file sizes
- Recommendations for routine database maintenance and instructions for performing this maintenance
- Design diagrams, structure or flow charts, pseudo code, and source code listings necessary for performing future modifications of custom software

4.4 Software Verification and Validation

Objective:

The software V&V process is defined and performed, and related documentation is maintained to ensure that (a) the software adequately and correctly performs all intended functions, and (b) the software does not perform any unintended function.

Criteria:

1. All analysis and design software requirements and design have been verified and validated for correct operation using testing, observation, or inspection techniques.

2. Relevant abnormal conditions have been evaluated for mitigating unintended functions through testing, observation, or inspection techniques.

.

Approach:

Review the software V&V documentation, either as a standalone document or embedded in another document, to determine if:

- The tasks and criteria are documented for verifying the software in each development phase and validating it at completion,
- The hardware and software configurations pertaining to the software V&V are specified,
- Traceability to both software requirements and design exists,
- Results of the V&V activities, including test plans, test results, and reviews are documented,
- A summary of the status of the software's completeness is documented,
- Changes to software are subjected to appropriate V&V,
- V&V is complete, and all unintended conditions are dispositioned before software is approved for use and,
- V&V is performed by individuals or organizations that are sufficiently independent.

4.5 Software Configuration Management

Objective:

The SCM process and related documentation for safety analysis and design software, including calculational software, are defined, maintained, and controlled.

Criteria:

1. All software components and products to be managed are identified.
2. For those components and products, procedures exist to manage the modification and installation of new versions.
3. Procedures for modifications to those components and products are followed.

Approach:

Review appropriate documents, such as applicable procedures related to software change control, to determine if a SCM process exists and is effective. This determination is made based on the following actions.

- Verify the existence of an SCM plan, either in standalone form or embedded in another document
- Verify that a configuration baseline is defined and that it is being adequately controlled
- Verify that configuration items such as operating systems, source code components, any associated runtime libraries, acquired software executables, custom-developed source code files, users' documentation, documents containing software requirements, software design, software V&V procedures, test plans, and procedures have been identified and placed under configuration control
- Review procedures governing change management, including installation of new versions of the software components and new releases of acquired software

- Review software change packages and work packages to ensure that (1) possible impacts of software modifications are evaluated before changes are made, (2) various software system products are examined for consistency after changes are made, and (3) software is tested according to established standards after changes have been made
- Verify by sampling that documentation affected by software changes accurately reflects all safety-related changes that have been made to the software
- Interview a sample of cognizant line, engineering, and QA managers and other personnel to verify their understanding of the change control process and commitment to manage changes affecting design, safety basis, and software changes in a formal, disciplined, and auditable manner.

4.6 Software Quality Assurance

Objective:

SQA activities are evaluated for applicability to the analysis and design software, defined to the appropriate level of rigor, and implemented.

Criteria:

1. SQA activities and software practices for requirements management, software design, software configuration management, procurement controls, V&V (including reviews and testing), and documentation have been evaluated and established at the appropriate level for proper applicability to the analysis and design software under assessment.
2. SQA activities have been effectively implemented.

Approach:

Determine if an appropriate SQA plan exists, either as a standalone document or embedded in another document, as well as related procedures, QA assessment reports, test reports, problem reports, corrective actions, supplier control, and training. Determine the effectiveness of the SQA program by reviewing the SQA plan. The assessment may also include interviewing managers, engineers, and software users. The SQA plan should identify:

- The software products to which it applies,
- The organizations responsible for maintaining software quality, along with their tasks and responsibilities,
- Required documentation: SRD, SDD, software user documentation, SCM plan, and software V&V plans and results,
- Standards, conventions, techniques, or methodologies that guide software development, as well as methods to ensure compliance to the same,
- Methods for error reporting and developing corrective actions, and
- Provisions for controlling software supplier activities for meeting established requirements.

4.7 Software Procurements

Objective:

Vendor-supplied software, either COTS software, custom-developed or modified, requires the appropriate levels of QA commensurate with the level of risk introduced by their use.

Criteria:

1. Procurement documents for acquisition of software programs identify the quality requirements appropriate for the level of risk introduced by their use.
2. Acquired software is verified to meet the identified quality requirements.

Approach:

Vendors that supply COTS and other software are evaluated to ensure that they develop software under an appropriate QA program and are capable of providing software that satisfies the specific requirements. The volume of commercial use for vendor software, especially with COTS software, should be considered in determining the adequacy of the vendor's QA program. The assessment of software procurements shall include the following:

- Determine the existence of acquired software QA requirements. These requirements may be embedded in the DOE contractor's or subcontractor's procurement requirements, SRD, SDD, or an SQA plan.
- Review the methods the site uses to verify that vender software meets the specified QA requirements, and determine if these methods accomplish those requirements. These methods may be included in an SQA plan or software test plan.
- Review evidence that the vendor software was evaluated for the appropriate level of quality. This evidence may be included in test results, a test summary, vendor site visit reports, or vendor QA program assessment reports.

4.8 Software Problem Reporting and Corrective Action

Objective:

Formal procedures for software problem reporting and corrective action for software errors and failures are established, maintained, and controlled.

Criteria:

1. Practices and procedures for reporting, tracking, and resolving problems or issues identified in both software items and software development and maintenance processes are documented and implemented.
2. Organizational responsibilities for reporting issues, approving changes, and performing corrective actions are identified and effective.

Approach:

Review documents and interview facility staff responsible for problem reporting and notification to determine if:

- A formal procedure exists for software problem reporting and corrective action development that addresses software errors, failures, and resolutions
- Corrections and changes are executed according to established change control procedures
- The problems that impact the software's operation are promptly reported to affected organizations
- Corrections and changes are evaluated for impact and approved before being implemented
- Corrections and changes are verified for correct operation and to ensure that no side effects were introduced before being implemented
- Preventive measures and corrective actions are provided to affected organizations in a timely manner commensurate with the impact of the original defect
- The organizations responsible for problem reporting and resolution are defined

5.0 REPORT FORMAT

The report is intended for cognizant facility managers and DOE line management, and should include the following sections. The report must conform to security requirements, undergo classification review if needed, and should not contain classified information or Unclassified Controlled Nuclear Information (UCNI).

1. **Title Page (Cover).** The cover and title page should contain state the name of the site and dates of assessment.

2. **Signature Page.** A signature page should be signed by all team members, signifying their agreement to the report content and conclusions drawn in the areas to which they were assigned. In the event all team member signatures cannot be obtained due to logistical considerations, the team leader should gain members' concurrence and sign for them.

3. **Table of Contents.** The table of contents should identify all sections and subsections of the report, illustrations, charts, and appendices.

4. **Acronyms.**

5. I**ntroduction.** The introduction should provide information and background regarding the site, system, team composition, methodology, and any definitions applicable to the review.

6. **Tailoring.** Identify any tailoring of the criteria and guidelines provide in this CRAD. State the basis for the tailoring.

7. **Assessment Results.** State whether the assessment criteria are satisfied and describe any exceptions. Summarize areas needing improvement, and include a qualitative conclusion regarding the software's ability to perform its intended functions in its current condition. Recommended actions may also be included. Note any topical areas that were not assessed and any limitations to the qualitative conclusions. A detailed discussion of results in each topical area that was assessed should be included as a separate attachment or appendix.

8. **Lessons Learned.** Identify lessons learned that may be applied to future reviews.

9. **Detailed Results.** In each topical area assessed, include sufficient detail to enable a knowledgeable individual to understand the specific results. As specified in the IP, assessment results needing correction will be tracked either locally or in DOE-wide systems.
   The suggested format for this section is as follows:
   - Is the criterion met? [Yes/No]
   - How the review was conducted [Include lists of documents reviewed, including any system software documentation and QA, and titles of persons interviewed]
   - Software quality-related issues or concerns
   - Areas needing improvement
   - Recommended changes to criteria and guidance

10. **Documents and References.** Title, number, revision, and issue date as applicable.

11. **SQA Data (if applicable)**

12. **Biographies of Team Members**

6.0 REFERENCES

1. 10 CFR 830.120, *Nuclear Safety Management,* Quality Assurance Requirements

2. ANSI/ANS 10.4-1987 (R1998), Section 11, *V&V for Existing Programs, Guidelines for the Verification and Validation of Scientific and Engineering Computer Programs for the Nuclear Industry*

3. ASME NQA-1a-1999, Subpart 2.7, *Quality Assurance Requirements for Computer Software for Nuclear Facility Applications with Addenda (1999)*

4. DNFSB Recommendation 2002-1, *Quality Assurance for Safety-Related Software*

5. DNFSB/TECH-25, *Quality Assurance for Safety-Related Software at Department of Energy Defense Nuclear Facilities*

6. DOE G 200.1-1, *DOE Guidelines for Software Engineering Methodology*

7. DOE G 420.1-1, *Nonreactor Nuclear Safety Design Criteria and Explosives Safety Criteria Guide for use with DOE O 420.1,* Facility Safety

8. DOE-STD-3009-94, Change Notice 2, April 2002, *Preparation Guide for U.S. Department of Energy Nonreactor Nuclear Facility Documented Safety Analyses*

9. IEEE Std. 1012, *Standard for Software Verification and Validation*

10. IEEE Std. 1028, *Standard for Software Reviews*

11. IEEE Std. 1219, *Standard for Software Maintenance*

12. IEEE Std. 1228, *Standard for Software Safety Plans*

13. IEEE Std. 610.12-1990, *IEEE Standard Glossary of Software Engineering Terminology*

14. IEEE Std. 730, *Standard for Software Quality Assurance Plans*

15. IEEE Std. 828, *Standard for Software Configuration Management Plans*

16. IEEE Std. 829, *Standard for Software Test Documentation*

17. IP 2002-1, *Implementation Plan for Defense Nuclear Facilities Safety Board Recommendation 2002-1,* Quality Assurance for Safety Software at Department of Energy Defense Nuclear Facilities, March 13, 2003

18. IP 2000-2, *Implementation Plan for Defense Nuclear Facilities Safety Board Recommendation 2000-2, Configuration Management, Vital Safety Systems,* October 31, 2000.