CRAD - 4.2.3.1
Revision 3
October 24, 2003

U. S. Department of Energy

# Criteria and Guidelines For the Assessment of Safety System Software and Firmware at Defense Nuclear Facilities

October 24, 2003

# TABLE OF CONTENTS

ACRONYMS ..... ii
GLOSSARY ..... iii
1.0 INTRODUCTION ..... 1
2.0 BACKGROUND ..... 2
3.0 ASSESSMENT GUIDELINES ..... 3
3.1 Purpose and Scope ..... 3
3.2 Guiding Principles ..... 3
3.3 Assessment Methodology ..... 5
4.0 CRITERIA AND APPROACH ..... 9
4.1 Software Requirement Description ..... 10
4.2 Software Design Description ..... 11
4.3 Software Verification and Validation ..... 12
4.4 Software User Documentation ..... 13
4.5 Software Configuration Management ..... 14
4.6 Software Quality Assurance ..... 15
4.7 Software Procurement ..... 16
4.8 Software Problem Reporting and Corrective Action ..... 17
5.0 REPORT FORMAT ..... 18
6.0 REFERENCES ..... 20

# 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.

**Firmware** - The combination of a hardware device and computer instructions and data that resides as read-only software on that device. [IEEE Std. 610.12-1990, *IEEE Standard Glossary of Software Engineering Terminology*]

**I&C Software** - Software used for instrumentation and controls (I&C), including embedded microprocessors, distributed control systems, supervisory control and data acquisition systems (SCADAs), programmable logic controllers (PLCs), and other related software.

**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 CFR, part 10, section 830. [10 CFR 830]

**Safety Analysis and Design Software** - Software that is not a part of a structure, system, 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,
- the proper analysis and design of safety SSCs,
- 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 [10 CFR 830]. As a general rule of thumb, safety-significant SSC designations based on worker safety are limited to those systems, structures, or components whose failure is estimated to result in a prompt worker fatality or serious injuries (e.g., loss of eye, loss of limb) or significant radiological or chemical exposure to workers. [DOE G 420.1-1]

**Safety Software** - As referenced and defined in the Implementation Plan for the DNFSB Recommendation 2002-1, includes both safety system software and safety analysis and design software.

**Safety SSCs** - This term applies both to safety-class structures, systems, and components, and to 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*]

**Criteria and Guidelines**
**For the Assessment of Safety System Software and Firmware**
**At Defense Nuclear Facilities**

# 1.0 INTRODUCTION

This document contains software qualification assessment criteria and guidelines for assessing the safety system software used for instrumentation and controls (I&C) at Department of Energy (DOE) defense nuclear facilities. The criteria and guidelines fulfill Commitment 4.2.3.1 of the DOE Implementation Plan (IP) for Defense Nuclear Facilities Safety Board (DNFSB or Board) Recommendation 2002-1, *Quality Assurance for Safety Software at Department of Energy Defense Nuclear Facilities*.

Commitment 4.2.3 of the IP specifies three actions DOE will take to assess the processes in place to ensure that the safety software currently used in instrumentation and controls at defense nuclear facilities is adequate. Commitment 4.2.3.1 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 the safety system software. Commitments 4.2.3.2 and 4.2.3.3 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 software.
- The ***Criteria and Approach*** section presents the objective, criteria, approach, and tailoring for the following topical areas: (1) Software Requirement Description, (2) Software Design Description, (3) Software Verification and Validation, (4) Software User Documentation, (5) Software Configuration Management, (6) Software Quality Assurance, (7) Software Procurement, and (8) Software Problem Reporting and Corrective Action.
- The ***Report Format*** section provides a suggested report format.
- The ***References*** section lists selected references relevant to software quality assurance (SQA).

# 2.0 BACKGROUND

The 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) require the same high level of quality needed to provide adequate protection for the public, the 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 level of quality assurance (QA) 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 on November 21, 2002 and committed to developing an IP. DOE 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 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 industry or Federal agency standards where practical, and
- A process that will track continuous improvements and initiatives in software technology.

The scope of the IP includes safety software at the Department's defense nuclear facilities. The IP defines **Safety software**, to include 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 a 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, the proper analysis and design of safety SSCs, and the proper identification, maintenance, and operation of safety SSCs.

# 3.0 ASSESSMENT GUIDELINES

## 3.1 Purpose and Scope

The purpose and scope of this CRAD is to provide a set of consistent assessment criteria and guidelines for the assessment of safety system software and firmware that performs an SC or SS function, as described in the Background section. The scope of the assessment, henceforth, is called "I&C software."

I&C software is generally supplied by the product manufacturer. Quality assurance (QA) controls for the manufacturers' software are usually maintained by the manufacturers. However, users at DOE sites may also add to or modify application of this software (e.g., modifying a PLC because of the versatility of its application). Software modifications of this type are also within the scope of this assessment.

The assessment criteria and guidelines provide a consistent framework for assessing the processes that are currently in place to ensure that the I&C software being used in safety-related instrumentation and control systems in defense nuclear facilities is adequate. **These assessments will only be conducted on I&C software that is currently in use**. Those systems that have undergone DNFSB Recommendation 2000-2 IP reviews, using the associated CRAD that included SQA, may be able to use those reviews as a basis for these assessments.

Should an issue arise that casts doubt on the validity of software previously used to support design or development, it will be resolved using the Unreviewed Safety Question (USQ) Determination (USQD) process. Generic USQs will be used to the extent possible to preclude multiple facilities' developing separate USQDs for the same problem. **Individual sites should tailor the scope of this assessment to suit the specific usage of I&C software in their safety systems.**

## 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 assessing I&C software applications. Therefore, are not repeated in the Criteria and Approach sections that follow.

- SQA assessments of I&C software should begin by determining all existing software to which this CRAD applies. This could be accomplished by updating the list of vital safety systems compiled in response to DNFSB Recommendation 2000-2, *Configuration Management, Vital Safety Systems*, to ensure that it is current and accurate, and identifying those SC and SS SSCs from the list that use software. The functions and the consequences of its failure should then be qualitatively assessed, and the software selected for the assessment should be representative of the safety system software applications at the site. The assessment team should verify that all I&C software used in safety system applications has been identified using the definition of safety system software provided. The team should then sample SC and SS I&C software. The SC and SS I&C software should be consistent with the Documented Safety Analysis (DSA), the facility Safety Analysis Reports (SARs) and the Technical Safety Requirements (TSRs). The assessments should be limited to a representative sample to avoid unnecessary and excessive assessments.

- Existing software attributes such as complexity and importance to safety should be considered when determining the rigor and adequacy of the software QA. Additional guidance is provided in the tailoring sections of this CRAD.

- The team should review the results previous assessments, such as the reviews performed in response to DNFSB Recommendation 2000-2 IP and other SQA reviews, to gather data as appropriate. This review will enable the team to understand previous assessments, I&C software qualification processes, associated requirements and performance criteria, and assumptions concerning system operations.

- The physical boundaries of the software within the safety system or subsystem level or portions thereof under review should be agreed upon by DOE, the contractor line management and the team prior to the start of the assessment, and should be documented in the assessment report.

- Where applicable, I&C software should be categorized in the same manner as other system components using DOE-STD 3009-94, and the appropriate level of rigor should be applied to its design and use.

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

- Software is one component in a safety system. In many instances, it is difficult to separate the software safety functions from the rest of the system. The four critical areas for any safety system component are: 1) the safety functions and performance requirements, 2) adequacy of standards and controls applied, 3) testing and maintenance, and 4) configuration management.

- The assessment of specific I&C software applications should begin with gaining an understanding of the overall system and documenting the system safety functions, the performance criteria that the system must meet to successfully accomplish its safety functions, and the role of the software in ensuring that these functions and criteria are met. The potential consequences of failure of the software and the associated effects on system operability should be understood and documented.

- The team should review any lessons learned from past events associated with I&C software applications and include any additional attributes as appropriate in the Assessment Plan.

- The facility staff should assist the team in 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 point of contact for further information.

- Procedures and records for I&C software V&V, testing, and maintenance should be evaluated for adequacy and to determine whether or not they are appropriate and are being used to verify that software requirements and performance criteria described in the software requirements documentation are satisfied.

- If the team identifies a condition that poses an imminent threat to personnel or facility safety, line management must be notified immediately. Team personnel should immediately point out the

imminent threat condition to their points of contact or appropriate facility manager and notify the assessment team leader as soon as practical.

- For commercial off-the-shelf (COTS) software and proprietary software, it is not the intent of the assessment to evaluate individual software. Instead, the assessment should verify that for work activities using safety COTS and proprietary software, procurement and software control processes are in place to ensure that software used in the work activities is adequate.

## 3.3 Assessment Methodology

The assessment should address the following major activities:

- The team shall prepare the 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 I&C software, which includes software that performs a safety function as part of an SS and SC system as defined in facility DSAs and TSRs. I&C software is an integral part of a safety system. I&C software classification should be consistent with SSC classification unless otherwise justified for case-specific application. The team should use facility-specific DSAs and TSRs for the selection of I&C software.

- The team should review the applicable standards for assistance in developing the lines of inquiry and to determine their appropriateness for the I&C software being assessed. The applicable standards may be obtained from the facility staff and/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 use interview methods as well as informal discussions with program developers, users, and sponsors to supplement and complement the documented information.

A suggested sequence for this assessment includes: team selection, site-specific tailoring, preparation and optional pre-assessment visit, onsite assessment, and briefing 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 team leadership.
- Should be a Federal employee.
- Should not be in the line organization of the facility for the system under assessment.
- Should document technical and lead capabilities in a short biographical sketch, which will be included in the assessment report.

Team members:

- Should have demonstrated capability in performing safety system or I&C software technical assessments.
- Collectively should have a working knowledge of the types of hazards associated with SC and SS systems within defense nuclear facilities, the safety basis process, software development practices, systems engineering, and I&C software applications.
- Can be Federal employees, site contractors, or subcontractor experts.
- Can be from any DOE field or Headquarters office or their contractors or subcontractors.
- Should not have contractor line management responsibility for the system 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 will be included in the assessment report.

**Site-Specific Tailoring**

These assessment criteria and guidelines were not developed for a specific I&C software 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 operational readiness of I&C software and its ability to operate safely on a continued basis. 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 and its 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. Acquired software, such as COTS, may not be modified and can be viewed within the system as a "black box". Custom software is completely modifiable and may require additional SQA processes over those of acquired software. Some acquired software can be configured specifically for its application or its source code can be modified to meet application specific requirements. In these instances a higher level of SQA requirements should be expected. However, these requirements may not be as high as custom software for the specific application.

Generally, for acquired software that is not modified, system level controls should be in place and are adequate. The only exception is in configuration management. Software level configuration management procedures to control the software components are needed. For acquired software that can be modified or configured, the subset of functions and their associated components should have software level controls. For custom software, full software controls should be in place. Additional guidance is included within the Tailoring section in each topical area.

The assessment should consider the effectiveness of SQA processes that are separate from system quality processes. In many instances, especially with acquired software, the separation of software from the system may increase costs but not increase the safe operation of the system.

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 the system documentation.

For SSCs that have been in operation for several years, the team should consider using an approach similar to the *a posteriori* review described in ANS 10.4. This approach takes advantage of available program development products and program staff as well as the experience of the users. The purpose of an *a posteriori* review is to determine if the system produces valid responses. The level of *a posteriori* review may range from a simple demonstration that the software produces reasonable results for a representative sample of inputs or test cases 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.

Using the *a posteriori* approach, the verification and validation of legacy I&C software for which documentation such as system qualification plans and test reports, and software design description, procurement specifications does not exist or cannot be found may consist primarily of the review of system test procedures and records, and verification that the test results are consistent with the software requirements, and have been consistently uniform. Documentation of the software requirements is necessary to ensure that future changes to the software are adequately controlled and consistent with system operation as assumed in the facility safety basis. If the software requirements are not adequately documented, the perceived requirements should be developed and documented as described in ANS 10.4.

**Preparation and Optional Pre-Assessment Site Visit**

The team should request information needed to understand the I&C software functions, software design, configuration management, level of modification, and other SQA requirements 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 assessment 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 assessment 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, the assessment team leader should hold a short entrance meeting. 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 is listed below.

- Identification of the agreed upon boundaries for the assessment.
- Assessment schedule, including interviews.
- Team introduction.
- System overview, including role of the I&C software.
- Ability of the I&C software to perform its safety basis functions.
- 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**

When the assessment is complete, the assessment team leader and site management should arrange a briefing with appropriate facility and DOE field management on the assessment results. The assessment team leader will send the final report 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 Description (SDD)
- Software V&V
- Software User Documentation
- Software Configuration Management (SCM)
- Software Quality Assurance (SQA)
- Software Procurement
- 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 I&C 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 guide the team in assessing the quality of the I&C software. However, the team may choose to select another approach to meet assessment-specific needs.

- ***Tailoring:*** Includes suggested approaches and additional guidance for the team to consider when performing the assessment.

Existing QA requirements or other requirements such as procurement, for I&C 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 at DOE sites 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, level of customization, 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.

## 4.1 Software Requirement Description

**Objective:**

I&C software functions, requirements, and their bases are defined and documented.

**Criteria:**

1. The functional and performance requirements for the I&C software are complete, correct, consistent, clear, testable, and feasible.
2. The I&C software requirements are documented and consistent with the system safety basis.
3. The software requirements description (SRD) is controlled and maintained.
4. Each requirement should be uniquely identified and defined such that it can be objectively verified and validated.

**Approach:**

Review the appropriate safety basis documents, such as DSAs, SARs, TSRs, and system documentation, such as the SDD, and procurement specifications, to determine if the I&C software requirements are consistent with the safety system design and safety basis. These requirements may exist either as a standalone document (e.g., SRD) or embedded in another. Determine if the following types of requirements are addressed as appropriate:

- Functionality - the safety functions the software is to perform during normal, abnormal, and emergency situations,
- Performance - precision and accuracy requirements and the time-related issues of software operation such as time-dependent input-to-output relations, speed, recovery time, response time, frequency of reading input and updating output, throughput, and interrupt handling,
- Design constraints - any elements that will restrict design options,
- Attributes - non-time-related issues of software operation such as portability, acceptance criteria, security, access control, and maintainability, and
- External interfaces - interactions with people, hardware, and other software.

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.

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

**Tailoring:**

For acquired software, the above requirements may exist in a system design description or other system level documentation. For those components in acquired software that are configured or modified, the applicable requirements should be detailed either in a separate software requirements description or associated documentation. The modified software requirements should be uniquely identified. For custom software, the SRD should be available having each requirement uniquely defined.

## 4.2 Software Design Description

**Objective:**

The software design description (SDD) depicting the logical structure, information flow, logical processing steps, and data structures, are defined and documented.

**Criteria:**

1. All I&C software related requirements are implemented in the design.
2. All design elements are traceable to the requirements.
3. The design is correct, consistent, clearly presented, and feasible.

**Approach:**

Review the appropriate documents, such as vendor specifications for I&C software design, and a description of the components and subcomponents of the software design, including databases and internal interfaces. 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 I&C software requirements and any interactions with non-safety components.
- 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 strategies and the use of interrupt protocols.
- The design described in a manner suitable for translating into computer codes.

Note: In instances where the SDD 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 it performs.

**Tailoring:**

For acquired software, the design of the software components may be included with the SRD in the system design description or other system level documentation. For those components in acquired software that are configured or modified, the design of those components should be detailed either in a separate SDD or associated documentation. For custom software, the design information should be

contained in an SDD or comparable set of documentation. If this documentation is unavailable, the source code program listings may be used to assist in understanding the design.

## 4.3 Software Verification and Validation

**Objective:**

The V&V process and related documentation for I&C software are defined and maintained to ensure that (a) the software adequately and correctly performs all its intended functions; and that (b) the software does not perform any adverse unintended function.

**Criteria:**

1. All I&C software requirements and software designs 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 appropriate documents, such as test plans, test cases, test reports, system qualification plans and reports, and vendor qualification reports to determine if:

- An established process for validating the requirements exists.
- The V&V process includes an assessment to demonstrate whether the software requirements and system requirements are correct, complete, accurate, consistent, and testable.
- Dynamic testing has been performed to confirm time-dependent input-output relations, speed, recovery time, response time, frequency of reading input and updating output, throughput, and interrupt handling, as specified in the SRD.
- Each test case is executed in accordance with the test procedures and test plan.
- Correct inputs have been used for each test case.
- A sufficient number of tests has been executed to test all I&C software requirements.
- Tests representative of the anticipated application have been executed.
- Hardware and software configurations pertaining to the software V&V are specified.
- Results of V&V activities including test execution, observations, inspections, and reviews are documented.
- V&V is complete, and all unintended conditions are dispositioned before software is approved for use.
- Traceability exists from software requirements to design and testing, and, as appropriate, to user documentation.
- V&V is performed by individuals or organizations that are sufficiently independent of the development of the I&C software.
- For SSCs that have been in operation for several years, the team should consider using an approach similar to an ANS 10.4 *a posteriori* review.

**Tailoring:**

For acquired software that is not modified, V&V requirements and activities are generally integrated into system level V&V requirements and activities. Many of the V&V requirements may be included in the procurement specification requirements, vendor quality assurance requirements, vendor qualification reports, or vendor manuals. System test documentation may contain the applicable software test requirements. For acquired software that has been configured or modified, the modified components should be reviewed for the applicable V&V requirements listed above. For custom software, all requirements listed above should be considered.

## 4.4 Software User Documentation

**Objective:**

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

**Criteria:**

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 correct operation of the software and to provide assistance for error conditions.
4. Appropriate software design and coding documentation to assist in 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 messages or other indications as a result of improper input, 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 to custom software.

**Tailoring:**

For acquired software that is not modified, the software user documentation is generally included as part of any system user documentation. Documentation for future modifications of the software is not applicable. For the components in the acquired software that have been modified, information specific to those components should exist. For custom software, all of the above items should be available in one or more sources, and the source code can supply some of this information. The source code can describe the user input and outputs as well as the design structure.

## 4.5 Software Configuration Management

**Objective:**

Software components and products are identified and managed, and changes to those items are 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 I&C 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. This baseline should include operating system components, any associated runtime libraries, acquired software executables, custom-developed source code files, users' documentation, the appropriate documents containing software requirements, software design, software V&V procedures, test plans and procedures, and any software development and quality planning documents.
- Review procedures governing change management for installing new versions of the software components including 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, 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.

**Tailoring:**

Whether software is acquired or custom, practices are vital to the safe SCM operation of a system. Even with acquired software that is not modified, the requirements for managing the software configuration noted above should be reviewed for applicability. This topical area should have the least variability in tailoring for the I&C software components and products.

## 4.6 Software Quality Assurance

**Objective:**

Software quality activities are evaluated for applicability to the I&C software, defined to the appropriate level of rigor, and implemented.

**Criteria:**

1. Software quality activities and software practices for requirements management, software design, SCM, procurement controls, V&V including reviews and testing, and documentation have been evaluated and established at the appropriate level for proper applicability to the I&C software under assessment.
2. The software quality 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 identifies:

- The software products to which it applies,
- The organizations responsible for maintaining software quality, along with their tasks and responsibilities,
- Required documentation such as SRD, SDD, V&V, SCM, and software user documentation,
- Supplier control provisions for meeting established requirements,
- Standards, conventions, techniques, or methodologies that guide software development and ensure compliance,
- Methods for error reporting and corrective action,
- Any tailoring or note of non-applicability of SQA activities, and
- The effectiveness of implementing the SQA activities by assessing other topical areas.

**Tailoring:**

SQA activities should exist in the applicable areas. For acquired software, many if not all the SQA requirements will be included with the system level QA requirements. The required documentation will be embedded within the system level documents. A separate SQA plan may not exist but applicable components should be integrated into the system QA plan. As for acquired or custom software, an SQA plan covering, all of the software components modified, should exist either as a standalone document or embedded within one or more documents. The required software documentation should exist as stated in the appropriate topical area sections.

## 4.7 Software Procurement

**Objective:**

Acquired software meets the applicable level of quality to ensure the safe operation of the system.

**Criteria:**

1. Agreements for acquiring software programs or components identify the quality requirements appropriate for their use.
2. Acquired software is verified to meet the identified quality requirements.

**Approach:**

Vendors that supply COTS and other types of acquired software are evaluated to ensure that the software is developed under an appropriate QA program and are capable of providing software that satisfies the specific requirements. The volume of commercial use of the vendor software should be considered in determining the adequacy of the vendor's QA program. The assessment of software procurement process shall include the following:

- Determine the existence of acquired software quality requirements. These requirements may be embedded in the DOE contractors' or subcontractors' procurement requirements or processes, software or system requirements description, software or system design description, or a software quality plan.

- Review the methods used to verify that acquired software meets the specified quality requirements, and determine if these methods are effective. These methods may be included in a software quality plan or software test plan.

- Review evidence that the acquired 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.

**Tailoring:**

This topical area is associated primarily with the use of acquired software and acquired software that has been modified. The modified components of acquired software and custom software may have associated software such as compilers and run-time libraries. For these types of software, verifying the quality of the acquired software is integrated with the V&V activities for the custom software.

## 4.8 Software Problem Reporting and Corrective Action

**Objective:**

A process for I&C software problem reporting is established, maintained, and controlled, including notification of errors, failures, and corrective action development.

**Criteria:**

1. Documented practices and procedures for reporting, tracking, and resolving problems or issues are defined and implemented.
2. Organizational responsibilities for reporting issues, approving changes, and implementing corrective actions are identified and found to be effective.

**Approach:**

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

- A formal procedure exists for software problem reporting and corrective action development that addresses software errors, failures, and resolutions.
- The problems that impact the operation of the software are promptly reported to affected organizations.
- Corrections and changes are evaluated for impact and approved prior to being implemented.
- Corrections and changes are verified for correct operation and to ensure that no side effects were introduced.
- Preventive measures and corrective actions are provided to affected organizations in a timely manner.
- The organizations responsible for problem reporting and resolution are clearly defined.

**Tailoring:**

Acquired software is typically embedded within a system. Determining whether a problem is related to the hardware, the acquired software, or another cause may not be immediately known. Procedures to report problems, notify appropriate individuals, and implement corrective actions may be included with system level problem reporting and other procedures. For custom software, the problem reporting and notification process may be independent of system level problem reporting. Consideration should be given to the technical benefits and cost effectiveness in having separate problem reporting and notification procedures.

# 5.0 REPORT FORMAT

The report is intended for cognizant facility managers and DOE line management, and should include the sections described below. 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 state the name of the site, facilities assessed, and dates of assessments.

2. **Signature Page.** All team members, signifying their agreement as to the report content and conclusions reached in the areas to which they were assigned, should sign a signature page. In the event all team member signatures cannot be obtained due to logistical considerations, the assessment team leader should obtain 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. **Introduction.** The introduction should provide information and background regarding the site, facility, system, team composition, methodology, and any definitions applicable to the review.

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

7. **Assessment Results.** State whether the assessment criteria are satisfied and describe any exceptions. Summarize opportunities for improvement and include a qualitative conclusion regarding the ability of the system to perform its safety functions in its current condition and to remain reliable over its life cycle. Recommended actions may also be included. Note any topical areas that were not assessed and any limitations to the qualitative conclusion. 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 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]
   - System operability issues or concerns
   - Opportunities for improvement
   - Recommended changes to criteria and guidance

10. **Documents and References.** Title, number, revision, and issue dates.

11. **Software Quality Assurance Data.**

12. **Biographies of Team Members.**

# 6.0 REFERENCES

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

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

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

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

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

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

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

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

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

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

10. IEEE Std. 610.12, *Standard Glossary of Software Engineering Terminology*

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

12. 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*

13. 10 CFR 830.120, *Nuclear Safety Management,* Quality Assurance Requirements

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

15. DOE G 420.1-1, Facility Safety

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

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