U.S. Department of Energy Orders Self-Study Program

DOE G 414.1-4

SAFETY SOFTWARE GUIDE FOR USE WITH 10 CFR 830, SUBPART A, QUALITY ASSURANCE REQUIREMENTS, AND DOE O 414.1C, QUALITY ASSURANCE

DOE G 414.1-2B

QUALITY ASSURANCE PROGRAM GUIDE

NNSA
National Nuclear Security Administration

DOE G 414.1-4
SAFETY SOFTWARE GUIDE FOR USE WITH 10 CFR 830, SUBPART A, QUALITY ASSURANCE REQUIREMENTS, AND DOE O 414.1C, QUALITY ASSURANCE
DOE G 414.1-2B
QUALITY ASSURANCE PROGRAM GUIDE
FAMILIAR LEVEL

OBJECTIVES

Given the familiar level of this module and the resources, you will be able to answer the following questions:

1. What is the purpose of DOE O 414.1D, attachment 3, *Suspect/Counterfeit Items Prevention*?
2. What are four ways of preventing introduction of suspect/counterfeit items (S/CIs) into DOE work?
3. What office would you contact before destroying or disposing of S/CIs and documentation?
4. Organizations, as part of their quality assurance programs (QAPs), should establish effective controls and processes that will do what three things?
5. What is the system used to report S/CIs to responsible DOE operations office managers and program managers?
6. What is the purpose of the government-industry data exchange program (GIDEP)?
7. What is the purpose of the S/CI notification process?
8. What are the seven indicators that should cause suspicion of fraud?
9. What should be done with the S/CI and documentation during the inspector general’s (IG’s) investigation?
10. What are three things the reporting and corrective action system covers?
11. What is the purpose of the quality improvement process?
12. What are the three typical results of quality problems in DOE?
13. What is the purpose of DOE’s noncompliance tracking system (NTS)?
14. How should quality problems be resolved and analyzed?
15. What are the four elements that must be included in the management of safety software?
16. What are the ten applicable safety software quality assurance work activities?
17. What are the five items that should be included in software engineering safety design practices?
18. How does DOE control the safety quality assurance activities of utility calculation or commercial design?
19. What is the difference between verification and validation?
20. How are new versions of software validated before they are used?

Note: If you think that you can complete the practice at the end of this level without working through the instructional material and/or examples, complete the practice now. The course manager will check your work. You will need to complete the practice at this level successfully before taking the criterion test.

RESOURCES

DOE O 210.2A, *DOE Corporate Operating Experience Program*. April 8, 2011.

DOE O 221.1A, *Reporting Fraud, Waste, and Abuse to the Office of Inspector General*. April 19, 2008.

DOE O 414.1D, *Quality Assurance*. April 25, 2011.

DOE G 414.1-2B, *Quality Assurance Program Guide*. August 16, 2011.

DOE G 414.1-4, *Safety Software Guide for Use with 10 CFR 830, Subpart A, Quality Assurance Requirements, and DOE O 414.1C, Quality Assurance*. June 17, 2005.

DOE M 231.1-2, *Occurrence Reporting and Processing of Operations Information*. August 19, 2003.

DOE P 450.4A, *Integrated Safety Management Policy*. April 25, 2011.

American Society of Mechanical Engineers, ASME-NQA-1b-2011, *Quality Assurance Requirements for Nuclear Facility Applications (QA)*. January 4, 2011.

International Atomic Energy Agency, IAEA-TECDOC-1169, *Managing Suspect and Counterfeit Items in the Nuclear Industry*. August 2000.

Office of Management and Budget Policy Letter No. 91-3, Reporting Nonconforming Products. April 9, 1991.

INTRODUCTION

According to DOE-STD-1146-2007, *General Technical Base Qualification Standard*, this module was to summarize the quality assurance information found in attachments 3, 4, and 5, of DOE O 414.1C, *Quality Assurance*, and its supporting guides, DOE G 414.1-3, *Suspect/Counterfeit Items Guide for Use with 10 CFR 830 Subpart A, Quality Assurance Requirements, and DOE O 414.1B, Quality Assurance*, DOE G 414.1-4, *Safety Software Guide for Use with 10 CFR 830 Subpart A, Quality Assurance Requirements, and DOE O 414.1C, Quality Assurance*, and DOE G 414.1-5, *Corrective Action Program Guide*.

DOE O 414.1C has been replaced by DOE O 414.1D. DOE G 414.1-3 and DOE G 414.1-5 have been replaced by DOE G 414.1-2B, *Quality Assurance Program Guide*. DOE O 414.1D, DOE G 414.1-4, and DOE G 414.1-2B will be covered in this self-study module.

This module is divided into three sections. Section one covers S/CI prevention, section two covers the corrective action management program, and section three covers the safety software quality requirements. The information provided will meet the relevant requirements in knowledge, skills, and abilities (KSA) number 19 of the DOE General Technical Base Functional Area Qualification Standard.

Completion of this module also meets certain requirements associated with the DOE facility representative (FR) program. The information contained in this module addresses specific requirements and as such does not include the entire text of the source document. Before continuing, you should obtain a copy of these guides. Copies of the DOE directives are available at http://www.directives.doe.gov/ or through the course manager.

SECTION 1—DOE O 414.1D, ATTACHMENT 3, SUSPECT/COUNTERFEIT ITEMS PREVENTION

Purpose

The purpose of DOE O 414.1D, attachment 3, is to state the requirements for DOE and its contractor organizations, as part of their QAPs, to establish, document, and implement effective controls and processes that will: ensure items and services meet specified requirements; prevent entry of S/CIs into the DOE supply chain; and ensure detection, control, reporting, and disposition of S/CIs.

Requirements

An organization's QAP must incorporate the following:

- Include S/CI oversight and prevention process commensurate with the facility/activity hazards and mission impact.
- Identify the position responsible for S/CI activities and for serving as a point of contact with the Office of Health, Safety, and Security (HSS).
- Provide for training and informing managers, supervisors, and workers on S/CI processes and controls (including prevention, detection, and disposition of S/CIs).
- Prevent introduction of S/CIs into DOE work by
  - engineering involvement in the development of procurement specifications during inspections and testing; and when maintaining, replacing, or modifying equipment;
  - identifying and placing technical and QA requirements in procurement specifications;
  - accepting only those items that comply with procurement specifications, consensus standards, and commonly accepted industry practices; and
  - inspecting inventory and storage areas to identify, control, and disposition for S/CIs.
- Include processes for inspection, identification, evaluation, and disposition of S/CIs that have been installed in safety applications and other applications that create potential hazards. Address the use of supporting engineering evaluations for acceptance of installed S/CI as well as marking to prevent future reuse.
- Conduct engineering evaluations to be used in the disposition of identified S/CIs installed in safety applications/systems or in applications that create potential hazards. Evaluations must consider potential risks to the environment, the public, and workers along with a cost/benefit impact, and a schedule for replacement (if required).
- Perform the evaluation to determine whether S/CIs installed in non-safety applications pose potential safety hazards or may remain in place. Disposition S/CIs identified during routine maintenance and/or inspections to prevent future use in these applications.
- Report to the DOE Office of Inspector General (OIG) per DOE O 414.1D, attachment 3, paragraph 3 and DOE O 221.1A, *Reporting Fraud, Waste, and Abuse to the Office of Inspector General*.
- Collect, maintain, disseminate, and use the most accurate, up-to-date information on S/CIs and suppliers.
- Conduct trend analyses for use in improving the S/CI prevention process.

DOE O 210.2A, *DOE Corporate Operating Experience Program,* requires review of existing lessons learned reports and submittal of new lessons learned reports for use in improving the S/CI prevention process.

Contact the DOE OIG before destroying or disposing of S/CIs and corresponding documentation, to allow the OIG to determine whether the items and documentation need to be retained for criminal investigation or litigation. S/CIs must be reported according to DOE M 231.1-2, *Occurrence Reporting and Processing of Operations Information*.

DOE G 414.1-2B, GUIDANCE ON SUSPECT AND COUNTERFEIT ITEMS

The approaches and methodologies described here were developed to meet the requirements for S/CIs described in DOE O 414.1D, attachment 3. Programs are free to choose any national or international consensus standards and industry best practices for S/CIs, as long as the QAP documents how the S/CI requirements in DOE O 414.1D are met.

Reporting S/CIs to DOE OIG

DOE O 221.1A requires DOE and contractor personnel to report instances of suspected fraud, waste, and abuse to the OIG. This all-encompassing requirement includes S/CIs. Reporting S/CIs pursuant to other DOE directives does not substitute for reporting S/CIs to the OIG.

DOE field elements and contractors report any S/CIs discovered during receipt, maintenance, testing, inspection, or use, and when there is reason to believe that a fraudulent act occurred during the manufacturing, shipping, testing, or certification of the S/CI. The following are some, but not all, indicators that should cause suspicion of fraud:

- Although item X was ordered and billed, evidence exists that the supplier intentionally provided item Y.
- The S/CI, sold as new, shows evidence of prior use.
- Evidence shows that the manufacturer or supplier intentionally provided altered or incomplete testing data, and/or did not disclose that some testing data were missing.
- Performance is inconsistent with certification or testing data furnished by the manufacturer or supplier.
- Product failure rate exceeds expectations.
- The manufacturer’s name, logo, serial number, or manufacture date appear to have been altered.
- Product is certified as meeting specified criteria, but fails independent QA test.

DOE or its contractors at the site where the S/CI(s) are initially discovered should report directly to the OIG. Responsibility for reporting S/CI(s) to the OIG should be defined at each location.

Reports to the OIG should be made to the local Office of Investigations within the OIG nearest the location where the S/CI(s) were initially discovered. Direct coordination with the local Office of Investigations will ensure communication of the necessary information, mailing address, telephone number, and fax number of the Office of Investigations for the local OIG field offices, as well as the contact information for the OIG hotline.

Report specific characteristics of the potential fraud, including the following:

- Description of the S/CI (e.g., raw material, fasteners, electrical components, valves, fittings, ratchet straps)
- Location of the discovery
- Name of manufacturer, distributor, and supplier
- Identifying numbers (e.g., serial number, model number, product code)
- Point of contact for information on the location of the S/CI and corresponding documentation
- Date of the S/CI discovery
- Occurrence report number
- Intended end use
- Significance of the S/CI
- Dollar value of the S/CI
- Other pertinent information, including any action that is underway by the DOE or other agencies

If an S/CI is identified, an occurrence report is submitted to ORPS (occurrence reporting and processing system), and the IG is notified according to the requirements in DOE O 221.1A. The S/CI may be reported by letter, telephone, fax, or electronic mail to the appropriate OIG field office. S/CIs and corresponding documentation should be held in a secure area per the local nonconforming item procedures until the IG has been notified and has responded to the notification and given disposition directions. S/CI procedures should address appropriate segregation of S/CI(s), where applicable, and the use of hold tags.

Responsibility in Reporting

The organization's QAP should include an S/CI oversight and prevention process commensurate with the facility/activity hazards and mission impact. The QAP should address responsibility for ensuring that the requirements are met, including the flow down of the requirements to contractors, subcontractors, suppliers, and vendors. S/CI requirements include

- identifying the position responsible for S/CI activities, and for serving as a point of contact with the HSS;
- reporting to the DOE OIG;
- issuing lessons learned reports for use in improving the S/CI prevention process according to DOE O 210.2A.

Guidance for most DOE S/CI requirements is provided in the International Atomic Energy Agency, IAEA-TECDOC-1169, *Managing Suspect and Counterfeit Items in the Nuclear Industry*.

OCCURRENCE REPORTING AND INFORMATION EXCHANGE

Reporting S/CI Discovery

DOE O 414.1D states that items, services, and processes that do not meet the specified requirements be identified, controlled, and corrected. DOE M 231.1-2, *Occurrence Reporting and Processing of Operations Information*, requires prompt reporting of all S/CIs, regardless of their location/application. S/CIs should be reported to the responsible DOE operations office manager and program manager by means of ORPS, and to the OIG. The use of ORPS and S/CI in ORPS does not substitute for reporting to the OIG.

Prompt reporting of S/CIs in ORPS contributes to improvement of safety, regulatory compliance, and reliability. The S/CI information reported in ORPS is used by program offices, other DOE contractors, HSS, OIG, and, where appropriate, by external agencies to prevent the spread of potentially hazardous items. For this reason, information reported should be sufficient to alert other organizations of S/CIs, and potential safety or performance problems associated with the items.

Historically, many S/CIs and defective items have been identified via ORPS. HSS reviews ORPS events on a daily basis for S/CIs and defective items (DIs) with potential safety impacts on DOE operations.

Government-Industry Data Exchange Program

The Office of Management and Budget Policy Letter No. 91-3, subject: Reporting Nonconforming Products, requires DOE to participate in the exchange of failure experience information concerning S/CIs. Accordingly, DOE and its contractors should participate in the government-industry data exchange program (GIDEP). HSS utilizes GIDEP as an S/CI information source to search for S/CIs that may have potential impacts on DOE operations. A data collection sheet (DCS) is then prepared and the information posted to the S/CI database on the HSS S/CI website. DOE and its contractors should also use GIDEP information in their procurement, inspection, and maintenance processes to prevent introduction of S/CIs, assist in the identification of S/CIs that have already entered the facility, and for reporting S/CI discoveries.

Consultation With Office of General Counsel

Federal program managers should consult with DOE's or NNSA's Office of General Counsel regarding legal questions arising from any S/CI occurrence. Typical legal questions involving an S/CI report include disclosure restrictions; procedures to protect government rights against S/CI suppliers; and proper liaison procedures among DOE programs and investigative, law enforcement, or prosecuting agencies. Within the Office of General Counsel, the Office of Assistant General Counsel for Civilian Nuclear Programs should be consulted for S/CI issues involving nuclear safety. For S/CI issues involving procurement and contractual-related issues, the Office of Assistant General Counsel for Procurement and Financial Assistance should be consulted.

S/CI Review, Analysis, and Notification

HSS has corporate responsibility for DOE's S/CI process. This responsibility includes the collection and review of information from internal and external sources, and the identification and dissemination of potential S/CI and DI information to the DOE complex. S/CI information sources include ORPS, GIDEP, Institute of Nuclear Power Operation, NTS database, accident investigation reports, and Nuclear Regulatory Commission generic communications.

For each potential S/CI identified, HSS prepares a DCS and assigns a tracking number. The DCS is used to facilitate review of the S/CI or DI and to document actions taken to resolve the issue. After appropriate review, the DCS is published by HSS.

HSS evaluates identified S/CIs and DIs using screening criteria for its applicability to DOE, and to determine what actions should be taken. HSS may obtain advice and assistance from other subject matter experts in DOE to assist in making this determination. Typical screening criteria include the following:

- Is this a repeat occurrence?
- Does the issue affect more than one site or have the potential to affect more than one site?
- Has the issue been declared an S/CI or DI, or does it have the potential to be declared an S/CI or DI?
- Is an investigation underway or about to be initiated regarding potential criminal activities?
- Does the issue have any immediate or potential regulatory, environmental, health, or safety impact?
- Could other organizations address the issue more appropriately?
- Does the issue have any complex-wide implication?
- Is this a legacy item(s) (e.g., high strength bolts found installed [time unknown], no manufacturer insignia, or unknown supplier)?

The purpose of the S/CI notification process is to provide a coordinated mechanism for the timely dissemination and field review of information concerning potential S/CIs. Based on the potential significance of the S/CI and its applicability to DOE, the information may be provided to the DOE complex using one of several methods.

- Operating experience notifications that potentially include the following:
    - HSS safety alert—if documentation clearly indicates that an S/CI or DI may be involved, and a significant regulatory, environmental, health, or safety impact exists
    - POC notification—if documentation indicates the S/CI or a DI may be in use at DOE facilities
    - Operating experience summary—if documentation indicates the S/CI or a DI may be applicable to DOE facilities
- Complex-wide submittal of ORPS reports
- DCS posted on the DOE HSS S/CI website at (http://www.hss.energy.gov/csa/csp/sci/), and possibly distributed through the e-mail listserver
- Possible notification of S/CI points of contact in the field or at headquarters (HQ)

S/CI information is also shared via other methods. The HSS operating experience committee conducts monthly conference calls and periodically discusses specific information regarding newly identified S/CIs or offers presentations from internal and external organizations concerning the status of existing and/or the development of S/CI programs. The operating experience Wiki page (http://operatingexperience.doe-hss.wikispaces.net/) hosts a dedicated web space for S/CI specific information, including informational publications, presentations, and videos from internal and external organizations.

Regardless of how the information is disseminated, field and HQ organizations should review the information for potential applicability to their own facilities and operations.

Note: You do not have to do example 1 on the following page, but it is a good time to check your skill or knowledge of the information covered. You may do example 1 or go to section 2.

EXAMPLE 1

Using the familiar level of this module and the resources, answer the following questions.

1. What is the purpose of DOE O 414.1D, attachment 3, *Suspect/Counterfeit Items Prevention*?

2. What are four ways of preventing introduction of S/CI into DOE work?

3. What is the purpose of the government-industry data exchange program (GIDEP)?

4. What are four of the seven indicators that should cause suspicion of fraud?

5. What should be done with the S/CI and documentation during the inspector general's investigation?

Note: When you have finished, compare your answers to those contained in the example 1 self-check. When you are satisfied with your answers, go to section 2.

EXAMPLE 1 SELF-CHECK

1. What is the purpose of DOE O 414.1D, attachment 3, *Suspect/Counterfeit Items Prevention*?
   The purpose of DOE O 414.1D, attachment 3, is to state the requirements for DOE and its contractor organizations, as part of their quality assurance programs (QAPs), to establish, document, and implement effective controls and processes that will: ensure items and services meet specified requirements; prevent entry of suspect/counterfeit items (S/CIs) into the DOE supply chain; and ensure detection, control, reporting, and disposition of S/CIs.

2. What are four ways of preventing introduction of suspect/counterfeit items into DOE work?
   Prevent introduction of S/CIs into the DOE work by
   - engineering involvement in the development of procurement specifications during inspections and testing; and when maintaining, replacing, or modifying equipment;
   - identifying and placing technical and QA requirements in procurement specifications;
   - accepting only those items that comply with procurement specifications, consensus standards, and commonly accepted industry practices; and
   - inspecting inventory and storage areas to identify, control, and disposition for S/CIs.

3. What is the purpose of the GIDEP?
   The Office of Health, Safety, and Security utilizes GIDEP as an S/CI information source to search for S/CIs that may have potential impacts on DOE operations.

4. What are four of the seven indicators that should cause suspicion of fraud?
   The following are some, but not all, indicators that should cause suspicion of fraud:
   - Although item X was ordered and billed, evidence exists that the supplier intentionally provided item Y.
   - The S/CI, sold as new, shows evidence of prior use.
   - Evidence shows that the manufacturer or supplier intentionally provided altered or incomplete testing data, and/or did not disclose that some testing data were missing.
   - Performance is inconsistent with certification or testing data furnished by the manufacturer or supplier.
   - Product failure rate exceeds expectations.
   - The manufacturer’s name, logo, serial number, or manufacture date appear to have been altered.
   - Product is certified as meeting specified criteria, but fails independent QA test.

5. What should be done with the S/CI and documentation during the inspector general’s investigation?
   S/CIs and corresponding documentation should be held in a secure area per the local nonconforming item procedures until the Office of the Inspector General has been notified and has responded to the notification and given disposition directions.

SECTION 2—DOE G 414.1D, CORRECTIVE ACTIONS MANAGEMENT

Problem Reporting and Corrective Action

Coupled with the configuration management of the software system, the problem reporting and corrective action process should address the appropriate requirements of the QAP corrective action system. The reporting and corrective action system will cover: methods for documenting, evaluating, and correcting software problems; an evaluation process for determining whether a reported problem is indeed a defect or an error; and the roles and responsibilities for disposition of the problem reports, including notification to the originator of the results of the evaluation. If the noted problem is indeed an error, the problem reporting and corrective action system should correlate the error with the appropriate software engineering elements; identify the potential impacts and risks to past, present, and future development and operational activities; and support the development of mitigation strategies. After an error has been noted, all users should be apprised to ascertain any impacts upon safety basis decisions.

Procurement documents should identify the requirements for suppliers to report problems to the supplier, any required supplier response, and the method for the purchasers to report problems to the supplier.

Maintaining a robust problem-reporting and corrective action process is obviously vital to maintaining a reliable and vital safety software system. This problem-reporting and corrective action system need not be separate from the other problem-reporting and corrective action processes if the existing process adequately addresses the items in this work activity.

This work activity should be fully implemented for all level A and B software types (custom developed, acquired, configurable, and commercial design and analysis) and for level C custom developed. This formal implementation should include documentation and tracking to closure of any problems reported for the software and authorization to perform the corrective action. A graded approach that reduces the formality of documenting problem reports and approving corrective actions taken may be applied for level A and B utility calculation safety software and all level C software applications except custom developed. This less formal implementation may include interoffice communications describing the problem identified and the corrective actions planned.

DOE G 414.1-2B—QUALITY IMPROVEMENT

Efforts related to quality improvement are intended to identify, control, and improve items, services, and processes. Improvement processes detect and prevent problems while identifying the causes of problems and work needed to prevent recurrence of problems through corrective actions. The quality improvement process is a disciplined management process based on the premise that all work can be planned, performed, measured, and improved. Management should ensure that the focus is on improving the quality of products, processes, and services by establishing priorities, promulgating policy, promoting cultural aspects, allocating resources, communicating lessons learned, and resolving significant management issues and problems that can hinder the organization from achieving its objectives. Management should balance safety and mission priorities when considering improvement actions, and implement safety and integrated safety management (ISM) systems for their operations and work practices, based on the ISM guiding principles provided in

DOE P 450.4A, *Integrated Safety Management Policy*.

Management should encourage employees to plan, develop, explore, and implement new ideas for improving products, processes, and services. Management commitment can be demonstrated by empowering employees to

- identify and report problems
- identify opportunities for improvement
- identify best management practices
- develop alternative approaches for addressing problems and recommend improvements
- implement the approved solution
- evaluate the improvement
- provide lessons learned to other organizations

Identified problems and other related information (positive and negative) from internal and external sources should be reviewed and analyzed to identify improvement opportunities. Implemented improvements should be monitored and methods established to verify their effectiveness.

Quality Improvement Processes

An effectively planned and implemented QAP is one that

- uses feedback to improve items, services, and the associated processes that produce them
- prevents or minimizes quality problems
- corrects problems that occur
- measures the effectiveness of corrective actions
- uses performance measures to identify strengths and weaknesses

Preventive action minimizes the occurrence of quality problems through appropriate design, inspection, procurement, and other process controls and assessment activities. DOE and contractor organizations should prioritize and focus their resources on preventive actions and on those quality problems that have the greatest potential for

- posing adverse safety risks to the environment and human health
- impacting the reliability of operations and products
- affecting the ability to meet customer requirements

As used in DOE G 414.1-2B, a quality problem is a collective term that may be

- a deficiency in an activity, product, service, item characteristic, or process parameter
- a noncompliance to a requirement
- an indeterminate/substandard condition, or a S/CI as defined in IAEA-TECDOC-1169
- conditions adverse to quality and/or significant conditions adverse to quality

Quality Feedback

Work activities and management systems can be continuously improved through assessment and feedback processes. Effective feedback from multiple sources is the foundation for processes designed to prevent, identify, and correct problems. The least desirable form of feedback results from accidents or unplanned events that self-disclose the quality problem. The process should include use of lessons learned from the local organization and other organizations. Identified improvement actions should be shared with other organizations. Management should track the actions to closure and ensure that the actions are effective in providing the anticipated improvements. Implementing effective feedback processes can support meeting the improvements. Implementing effective feedback processes can support meeting the requirements for the ISM core function on providing feedback and continuous improvement.

Contractors at DOE facilities should develop and maintain implementing procedures for the occurrence reporting and utilization of the requirements stated in DOE M 231.1-2. DOE M 231.1-2 requires that all notifications to DOE be timely according to the significance of the occurrence and that the written notification contain appropriate information describing the occurrence, significance, causal factors, and corrective actions.

DOE's noncompliance tracking system (NTS), operated and managed by DOE's Office of Enforcement, is another source of information for feedback on quality-related events. NTS is DOE's centralized, web-based system that allows contractors to voluntarily report non-compliances of nuclear safety and work safety, and health regulations, including the QA rule. See http://www.hss.doe.gov/enforce/Final_EPO_June_2009_v4.pdf for more information.

Identification of Problems Affecting Quality

Problems affecting quality may be identified by internal organization sources or external sources; but, once identified problems should be documented and evaluated to determine their significance. The method for determining significance of a problem and the process for handling problems should be documented as part of the QAP.

The cause of problems should be investigated and identified. Causes should be corrected to prevent recurrence of the problem. For straightforward problems, a simpler apparent cause process may be appropriate. For more serious or complex problems, a disciplined root cause analysis with a formal extent of condition review should be considered.

Problems that are not significant, but can be readily corrected, should be identified and documented. These types of problems may be handled in an expedient manner that may not necessarily need to follow the more formal processes for problem documentation disposition and corrective action.

Corrective Action/Resolution of Problems Affecting Quality

Problems that affect quality may be referred to as conditions adverse to quality and/or significant conditions adverse to quality, should be identified and corrected as soon as possible. The identification and reporting process should be documented and include a standard categorization of problem findings based on significance, criticality, severity, and potential impact on the safety, security, and mission of the site/organization. A corrective action/resolution process should consist of the appropriate steps, such as the following:

- Identifying a condition adverse to quality, and/or significant condition adverse to quality
- Taking appropriate actions as required to mitigate, stabilize, and/or prevent further progression of unsafe conditions or conditions adverse to quality
- Documenting the condition adverse to quality and/or significant condition adverse to quality

- Evaluating its significance and extent
- Analyzing the problem and determining its causes
- Reporting the planned actions to the organization identifying the problem
- Assigning responsibility for correcting the problem
- Taking prompt corrective (remedial) action and documenting that action
- Training or retraining personnel as appropriate
- Taking steps to prevent recurrence
- Verifying implementation
- Documenting closure
- Determining effectiveness of the corrective and preventive actions for significant problems
- Tracking and trending conditions adverse to quality as appropriate
- Communicating lessons learned as appropriate

Quality problems should be resolved individually and should be analyzed as part of a collection to identify systemic quality problems and opportunities for process improvement.

Note: You do not have to do example 2 on the following page, but it is a good time to check your skill or knowledge of the information covered. You may do the example or go to section 3

EXAMPLE 2

1. What are three things the reporting and corrective action system cover?

2. What is the purpose of the quality improvement processes?

3. What is the purpose of DOE's noncompliance tracking system (NTS)?

4. How should quality problems be resolved and analyzed?

Note: When you are finished, compare your answers to those contained in the example 2 self-check. When you are satisfied with your answers, go on to section 3.

EXAMPLE 2 SELF-CHECK

1. What are three things the reporting and corrective action system cover?
   The reporting and corrective action system will cover: methods for documenting, evaluating, and correcting software problems; an evaluation process for determining whether a reported problem is indeed a defect or an error; and the roles and responsibilities for disposition of the problem reports, including notification to the originator of the results of the evaluation.

2. What is the purpose of the quality improvement processes?
   Improvement processes detect and prevent problems while identifying the causes of problems and work needed to prevent recurrence of problems through corrective actions.

3. What is the purpose of DOE’s noncompliance tracking system (NTS)?
   The NTS is DOE’s centralized, web-based system that allows contractors to voluntarily report non-compliances of nuclear safety and work safety, and health regulations, including the QA rule.

4. How should quality problems be resolved and analyzed?

   Quality problems should be resolved individually and should be analyzed as part of a collection to identify systemic quality problems and opportunities for process improvement.

SECTION 3—DOE G 414.1D, SAFETY SOFTWARE QUALITY ASSURANCE REQUIREMENTS FOR NUCLEAR FACILITIES

Purpose

The purpose of DOE O 414.1D, attachment 4 is to prescribe the safety software quality assurance (SSQA) requirements for DOE nuclear facilities. Software, other than safety software as defined in DOE O 414.1D, is not subject to the requirements of DOE O 414.1D, attachment 4.

Requirements

Safety software must be acquired, developed, and implemented using ASME NQA-1-2011, part I and subpart 2.7 or other national or international consensus standards that provide an equivalent level of QA requirements as ASME-NQA-1b-2011, *Quality Assurance Requirements for Nuclear Facility Applications (QA)*. DOE-approved QAPs applicable to safety software based on the requirements from DOE O 414.1D are acceptable. Management of safety software must include the following elements:

- Involve the facility design authority in: the identification of requirements specification; acquisition; design; development; verification and validation (including inspection and testing); configuration management; maintenance; and retirement.
- Identify, document, control, and maintain safety software inventory. Inventory entries must include at a minimum the following: software description; software name; version identifier; safety software designation; grade-level designation; specific nuclear facility application used; and the responsible individual.
- Establish and document grading levels for safety software using the graded approach. Grading levels must be submitted to and approved by the responsible DOE approval authority.
- Using the consensus standard selected and the grading levels established and approved above, select and implement applicable SSQA work activities from the following list:
  - Software project management and quality planning
  - Software risk management
  - Software configuration management
  - Procurement and supplier management
  - Software requirements identification and management
  - Software design and implementation
  - Software safety analysis and safety design methods
  - Software verification and validation
  - Problem reporting and corrective action
  - Training of personnel in the design, development, use, and evaluation of safety software

DOE G 414.1-4—SAFETY SOFTWARE REQUIREMENT GUIDANCE

Safety should be designed into a system, just as quality should be built into the system and the information from the hazards analysis needs to be factored in the design.

DOE O 414.1D requires software quality assurance (SQA) work activities, referred to as work activities, to be performed for safety software. Applying industry-accepted software engineering and software quality engineering practices is generally the first approach to developing high quality software systems.

Software should be controlled in a traceable, planned, and orderly manner. The work activities, listed from DOE O 414.1D, cover tasks during the development, maintenance, and operations of safety software.

For software, project management starts with the system-level project management and quality planning. Software-specific tasks should be identified and either included within the overall system planning or in separate software planning documents. These tasks may be documented in a software project management plan (SPMP), an SQA plan (SQAP), a software development plan (SDP), or similar documents. They may be embedded in the overall system-level planning documents.

Typically the SPMP, SQAP, and/or SDP are the controlling documents that define and guide the processes necessary to satisfy project requirements, including the software quality requirements. These plans are initiated early in the project life cycle and are maintained throughout the life of the project.

The software project management and quality planning should include identifying all tasks associated with the software development and procurement, including procurement of services, estimate of the duration of the tasks, resources allocated to the task, and any dependencies.

Software project management and quality planning fully apply to custom-developed and configurable software types for both level A and B safety software. For level A and B acquired and utility calculation and all level C software applications, software project management and quality planning tasks can be graded. This grading should include the identification and tracking of all significant software tasks.

Safety system requirements provide the foundation for the requirements to be implemented in the software. These systems requirements should be translated into requirements specific for the software. These requirements should identify functional; performance; security, including user access control; interface and safety requirements; and installation considerations, and design constraints where appropriate.

Once the software requirements have been defined and documented, they should be managed to minimize conflicting requirements and maintain accuracy for later validation activities to ensure the correctness of the software placed into operations. Software requirements should be traceable throughout the software life cycle.

Software Design and Implementation

During software design and implementation the software is developed, documented, reviewed, and controlled. The software design elements should identify the operating system, function, interfaces, performance requirements, installation considerations, design inputs, and design constraints. The software design should be complete and sufficient to meet the software requirements.

Methods to mitigate the consequences of software failures should be an integral part of the software design. Specific software analysis and design methods for ensuring safety functions are well thought out and addressed properly should be performed throughout the software development and operations life cycles.

During the initial concept and requirement analysis phases for the software, potential failures need to be identified and evaluated for their consequences of failure and probability of occurrence. Some potential problems are: complex or faulty algorithm; lack of proper handling of incorrect data or error conditions; buffer overflow; and incorrect sequence of operations due to either logic or timing faults.

The design of the software is critical to ensuring safe operation of the system. The software design should consider principles of simplicity, decoupling, and isolation to eliminate the hazards. The safety features should be separate from non-safety modules, minimizing the impact of failure of one module on another. Software engineering safety design practices should include process flow analysis, data flow analysis, path analysis, interface analysis, and interrupt analysis during the design phase.

When hazards related to software functions cannot be eliminated, the hazard should be reduced and/or monitored. Software can experience partial failures that can degrade the capabilities of the overall system that may not be immediately detectable by the system. In these instances, other design techniques, such as building fault detection and self-diagnostics into the software, should be implemented. Software control functions can be performed incrementally rather than in a single step, reducing the potential that a single failure of a software component would cause an unsafe state.

The software safety work activity for level A custom-developed, configurable, and acquired safety software should fully meet this requirement. For this software type the safety analysis for the software components should be performed. For level A custom-developed safety software, the design concepts that include simplicity of modules that perform safety functions and isolation of those modules should be part of the design considerations. Where the design of the software modules still presents an unacceptable risk to failure of the safety system, fault tolerant and self-diagnostics designs should be implemented.

This work activity does not apply to utility calculation or commercial design and analysis safety software types unless the safety analysis determines that complexity of the utility calculation warrants the use of these techniques. For commercial design and analysis software, the software safety activities are performed by the service supplier. DOE controls the SQA activities of that software through procurement agreements and specifications.

Verification and Validation

Verification and validation (V&V) is the largest area within SQA work activities. Verification is performed throughout the life cycle of the safety software and validation activities are performed at the end of the software development or acquisition processes to ensure the software meets the intended requirements. V&V activities should be performed by competent staff other than those who developed the item being verified or validated. V&A activities include reviews, inspections, assessments, observations, and testing.

Reviews and inspections of software deliverables requirement specifications, procurement documents, software design, code modules, test results, training materials, user documentation, and processes that guide the software development activities should be performed. Traceability of the software requirements to the software design should be performed. Verification of the software design, using one of the previously listed methods, should be completed prior to approval of the software for use.

Software testing activities should be planned and documented. Test cases and procedures, including expected results, should be created. All test activity deliverables should be under configuration management. Test results should be documented and all test activity deliverables placed under configuration management.

Acceptance testing should include functional testing, performance testing, security testing, stress testing, and load testing. Failure mode analysis can be used for defining negative test cases and procedures. Testing strategies that may be appropriate for acceptance testing include equivalence class testing, branch and path testing, statistical-based and boundary value testing.

Additionally, the system should continually be monitored to estimate its continuing reliability and safety. Periodic testing of the operational system should be performed to detect any degradation. If testing is not possible, monitoring using quantitative measurements should be performed.

When a new version of a software product is obtained, predetermined and ad hoc test cases and procedures should be performed to validate the system meets the requirements and does not perform any unintended functions.

Modern utility calculation applications, such as spreadsheet programs, have grown dramatically in power, with a corresponding growth in risk. Utility calculation applications are installed on virtually every desktop, and user files containing algorithms and data can be easily modified by users. For more complex or extensive calculations, where checking and verification of calculation results are impractical or undesirable, the user files containing the calculation formulas, algorithms, or macros should be subject to the entire software life-cycle process.

For level A safety software all deliverables should be reviewed using V&V methods. In addition, traceability of the requirements to the design and from requirements to test cases should be performed. For level B safety software, deliverables that include requirements, test plans and procedures, and test results should be reviewed using V&A methods.

For all level A safety software except utility calculations, acceptance testing work activities should be planned and documented; acceptance test cases and procedures, including expected results should be created; test results should be documented; and all test activity deliverables should be under configuration management. Test results should be documented and all test activity deliverables placed under configuration management.

For level A software, continual monitoring of safety software operations based upon historical failure data and results of periodic reassessment of hazards should be performed. For level A, B, or C software, when new releases of the safety software have been developed, reviews and acceptance testing of changed documents and software should be performed.

Note: You do not have to do example 3 on the following page, but it is a good time to check your skill or knowledge of the information covered. You may do the example or go to the practice.

EXAMPLE 3

1. What are the four elements that must be included in the management of safety software?

2. What are four of the ten applicable safety software quality assurance (SSQA) work activities?

3. What are the five items that should be included in software engineering safety design practices?

4. What is the difference between verification and validation?

5. How are new versions of software validated before they are used?

Note: When you are finished, compare your answers to those contained in the example 3 self-check. When you are satisfied with your answers, go on to the practice.

EXAMPLE 3 SELF-CHECK

1. What are the four elements that must be included in the management of safety software?

   The four elements that must be included in the management of safety software are:

   - Involve the facility design authority in: the identification of requirements specification; acquisition; design; development; verification and validation (including inspection and testing); configuration management; maintenance; and retirement.
   - Identify, document, control, and maintain safety software inventory. Inventory entries must include at a minimum the following: software description; software name; version identifier; safety software designation; grade level designation; specific nuclear facility application used; and the responsible individual.
   - Establish and document grading levels for safety software using the graded approach. Grading levels must be submitted to and approved by the responsible DOE approval authority.
   - Using the consensus standard selected and the grading levels established and approved above, select and implement applicable SSQA work activities.

2. What are four of the ten applicable SSQA work activities?

   Note: Any four of the following constitute a correct answer.
   The SSQA work activities are:

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

3. What are the five items that should be included in software engineering safety design practices?

   Software engineering safety design practices should include process flow analysis, data flow analysis, path analysis, interface analysis, and interrupt analysis during the design phase.

4. What is the difference between verification and validation?

   Verification is performed throughout the life cycle of the safety software and validation activities are performed at the end of the software development or acquisition processes to ensure the software meets the intended requirements.

5. How are new versions of software validated before they are used?

   When a new version of a software product is obtained, predetermined and ad hoc test cases and procedures should be performed to validate that the system meets the requirements and does not perform any unintended functions.

PRACTICE

This practice is required if your proficiency is to be verified at the familiar level. This practice will prepare you for the criterion test. You will need to refer to the DOE directives to answer the questions in the practice correctly. The practice and criterion test will also challenge additional skills that you have acquired in other formal and on-the-job training.

1. What are four ways of preventing introduction of suspect/counterfeit items into DOE work?

2. Organizations, as part of their quality assurance programs, should establish effective controls and processes that will do what three things?

3. What is the purpose of the government-industry data exchange program (GIDEP)?

4. What are four of the seven indicators that should cause suspicion of fraud?

5. What are three things the reporting and corrective action system covers?

6. What are the three typical results of quality problems in DOE?

7. How should quality problems be resolved and analyzed?

8. What are four of the ten applicable safety software quality assurance work activities?

9. How does DOE control the safety quality assurance activities of utility calculation or commercial design?

10. How are new versions of software validated before they are used?

Note: The course manager will check your practice and verify your success at the familiar level. When you have successfully completed this practice, go to the general level.

DOE G 414.1-4
SAFETY SOFTWARE GUIDE FOR USE WITH 10 CFR 830, SUBPART A, QUALITY ASSURANCE REQUIREMENTS, AND DOE O 414.1C, QUALITY ASSURANCE
DOE G 414.1-2B
QUALITY ASSURANCE PROGRAM GUIDE
GENERAL LEVEL

OBJECTIVES

Given the familiar level of this module, and a scenario, you will be able to answer the following questions:

1. What are the reporting requirements for suspect/counterfeit items (S/CIs)?
2. What are the requirements for handling of S/CIs and their documentation?

Note: If you think that you can complete the practice at the end of this level without working through the instructional material and/or the examples, complete the practice now. The course manager will check your work. You will need to complete the practice in this level successfully before taking the criterion test.

Resources

DOE Orders Self-Study Program, DOE G 414.1-4 and DOE G 414.1-2B, Familiar Level. September 2011.

DOE O 414.1D, *Quality Assurance*. April 25, 2011.

DOE G 414.1-2, *Quality Assurance Program Guide*. August 16, 2011.

DOE G 414.1-4, *Safety Software Guide for Use with 10 CFR 830, Subpart A, Quality Assurance Requirements, and DOE O 414.1C, Quality Assurance*. June 17, 2005.

.

INTRODUCTION

The familiar level of this module covered the S/CI prevention, the corrective action management program, and the safety software quality requirements found in DOE G 414.1-4 and DOE G 414.1-2B. In the general level of this module, students are asked to apply the information contained in the familiar level and the guides to a scenario related to these guides. Please refer to the resources listed on the previous page to make your analysis and answer the questions.

Note: You do not have to do the example on the following page, but it is a good time to check your skill and knowledge of the information covered. You may do the example or go on to the practice.

EXAMPLE SCENARIO

Please review the following scenario, and then answer the questions that follow.

Scenario

On March 31, 2010, during testing of populated circuit boards, the collider-accelerator department (C-AD) discovered linear technology analog-to-digital converters (ADCs) were non-functioning. The ADC, part number LTC2209CUP, was supplied by MS HiTech. The circuit boards where the ADCs are installed are not used in any safety systems. Their failure could not present a hazard to the public or worker health and safety. Based on additional testing performed by the C-AD, x-rays taken of the ADCs by the contractor's (BNL) instrumentation division, and discussions between C-AD personnel and linear technology, it was determined that some of the ADCs supplied by MS HiTech were counterfeit.

Immediate actions:

- Circuit boards with the non-functioning linear technology ADCs supplied by MS HiTech have been segregated from other populated circuit boards.
- ADCs supplied by MS HiTech, which have not been installed in circuit boards have been segregated.
- Linear technology department has been consulted on inspection results (x-ray images and visual inspection of part marking) and concurs that parts are counterfeit.

Corrective actions:

- Suspect ADCs will be removed from un-installed circuit boards and with un-used ADCs be forwarded to the BNL S/CIs coordinator.
- Installed functional circuit boards that have linear technology ADCs installed will be inspected at the conclusion of the FY 2010 relativistic heavy ion collider run. Suspect parts will be removed from circuit board and sent to the BNL S/CI coordinator.
- The C-AD QA manager will work with the BNL S/CI coordinator and representatives from the BNL property and procurement management division to address procurement of electronic parts.
- MS HiTech will be contacted at the conclusion of the counterfeit ADC integrated circuit investigation.

DOE G 414.1-2B, section 5.4.1, *Reporting S/CI Discovery*

DOE O 414.1D, *Quality Assurance*, states that items, services, and processes that do not meet the specified requirements be identified, controlled, and corrected. DOE M 231.1-2, *Occurrence Reporting and Processing of Operations Information*, requires prompt reporting of all S/CIs, regardless of their location/application. Suspect/counterfeit items should be reported to the responsible DOE operations office manager and program manager by means of the occurrence reporting processing system (ORPS), and to the Office of Inspector General (OIG).

Requirements applicable to this scenario:
DOE G 414.1-2B, section 5.4.2, *Government-Industry Data Exchange Program*

The Office of Management and Budget Policy Letter No. 91-3 requires DOE to participate in the exchange of failure experience information concerning S/CIs. Accordingly, DOE and its contractors should participate in the government-industry data exchange program (GIDEP).

1. Were the requirements of reporting the S/CI to the responsible DOE operations office manager and program manager by means of the ORPS system and to the IG met?

2. Were the S/CIs reported to the industries involved?

When you are satisfied with your answers compare them to the ones contained in the example self-check.

EXAMPLE SELF-CHECK

Your answer does not have to match the following exactly. You may have added more corrective actions or cited other requirements from the Order that apply. To be considered correct, your answer must include at least the following.

1. Were the requirements of reporting the S/CIs to the responsible DOE operations office manager and program manager by means of the ORPS system and to the IG met?
   The S/CIs were reported to the operations office manager and program manager by means of the ORPS system. The scenario does not state if the OIG was notified.

2. Were the S/CIs reported to the industries involved?
   Yes.

PRACTICE

This practice is required if your proficiency is to be verified at the general level. The practice will prepare you for the criterion test. You will need to refer to the Order to answer the questions in the practice correctly. The practice and criterion test will also challenge additional analytical skills that you have acquired in other formal and on-the-job training.

Please review the following scenario and answer the questions that follow.

Scenario

During a routine quarterly inspection of a "Big Joe Lift" by a contract material handling mechanic, four bolts were noted as suspect items. The suspect bolts from a non-critical application were removed and replaced. Suspect bolts were then sent to a test laboratory for final disposition by corporate subject matter expert personnel.

Big Joe Lift—walk behind—in-service date 7/07/1987
Model# FDC-40106
Equip# 9635029
Prop# SS54916
Four (4) load back rest bolts—non-critical application
Grade 5, diameter 5/8", length 1 and ½", course threaded bolts displayed markings of suspect hardware

Material handling mechanics have been contracted to do the preventative and remedial maintenance and repair site-wide on the forklifts since 2001. No S/CIs have previously been reported since the contract initiation in 2001.

As part of a proactive maintenance program for preventative maintenance and S/CIs inspection the maintenance engineering manager and maintenance operations project lead agreed to increase the rigor of the inspection for S/CIs during normal quarterly preventative maintenance. It was also agreed that all forklifts would be inspected by the end of February and a new S/CIs report form would be used to inspect and document any S/CIs found.

Immediate actions taken:

- The suspect bolts from a non-critical location were removed and replaced.
- Suspect bolts were then sent to a test laboratory for final disposition by corporate subject matter expert personnel.

Applicable DOE directives:
DOE O 414.1D, section 1, *Purpose*

To set forth requirements for DOE and its contractor organizations, as part of their quality assurance programs, to establish, document, and implement effective controls and processes that will: 1) ensure items and services meet specified requirements; 2) prevent entry of S/CIs into the DOE supply chain; and 3) ensure detection, control, reporting, and disposition of S/CIs.

Applicable DOE directives:
DOE G 414.1-2B, section 5.4.1., *Reporting S/CI Discovery*

Suspect/counterfeit items should be reported to the responsible DOE operations office manager and program manager by means of ORPS, and to the OIG.

Write your answers below and then bring the completed practice to the course manager for review.

1. How did the contractor change their quality assurance program to more readily identify S/CIs?

2. Did all the immediate actions fulfill the requirements of reporting the occurrence? If not, what other required actions should be taken in this incident?

Note: The course manager will check your practice and verify your success at the general level. When you have successfully completed this practice, the course manager will give you the criterion test.