This document was prepared in conjunction with work accomplished under Contract No. DE-AC09-96SR18500 with the U. S. Department of Energy.

DISCLAIMER

Safety Software Guide Perspectives for the Design of New Nuclear Facilities (U)

Kevin R. O'Kula

Washington Safety Management Solutions LLC
P. O. Box 5388
Aiken, SC 29804-5388
Email: kevin.okula@wsms.com; Phone: 803.502.9620

Debra Sparkman

Department of Energy, Office of Quality Assurance Programs
DOE/EH-31, EH-31/270CC
Washington, DC 20585-0270
Email: debra.sparkman@eh.doe.gov; Phone: 301.903.6888

INTRODUCTION

In June of this year, the Department of Energy (DOE) issued directives DOE O 414.1C and DOE G 414.1-4 to improve quality assurance programs, processes, and procedures among its safety contractors. Specifically, guidance entitled, *Safety Software Guide for use with 10 CFR 830 Subpart A, Quality Assurance Requirements, and DOE O 414.1C, Quality Assurance, DOE G 414.1-4*, provides information and acceptable methods to comply with safety software quality assurance (SQA) requirements. The guidance provides a roadmap for meeting DOE O 414.1C, *Quality Assurance,* and the quality assurance program (QAP) requirements of Title 10 Code of Federal Regulations (CFR) 830, Subpart A, Quality Assurance, for DOE nuclear facilities and software application activities. [1, 2]

The order and guide are part of a comprehensive implementation plan that addresses issues and concerns documented in Defense Nuclear Facilities Safety Board (DNFSB) Recommendation 2002-1. [3] Safety SQA requirements for DOE as well as National Nuclear Security Administration contractors are necessary to implement effective quality assurance (QA) processes and achieve safe nuclear facility operations. DOE G 414.1-4 was developed to provide guidance on establishing and implementing effective QA processes tied specifically to nuclear facility safety software applications. The Guide includes software application practices covered by appropriate national and international consensus standards and various processes currently in use at DOE facilities.

While the safety software guidance is considered to be of sufficient rigor and depth to ensure acceptable reliability of safety software at all DOE nuclear facilities, new nuclear facilities are well suited to take advantage of the guide to ensure compliant programs and processes are implemented. Attributes such as the facility life-cycle stage and the hazardous nature of each facility operations are considered, along with the category and level of importance of the software.

The discussion provided herein illustrates benefits of applying the Safety Software Guide to work activities dependent on software applications and directed toward the design of new nuclear facilities. In particular, the Guide-based systematic approach with software enables design processes to effectively proceed and reduce the likelihood of rework activities. Several application examples are provided for the new facility.

SQA GUIDE METHODOLOGY

The Safety Software Guide is a comprehensive, non-mandatory approach document that uses a graded approach to define recommended software work activities. The Guide includes software applications that meet safety software definitions as stated in DOE O 414.1C. This includes software applications important to safety that may be included or associated with structures, systems, or components (SSCs). Safety software includes

- safety system software (performs a function as part of a SSC)
- safety and hazard analysis software and design software (classifies, designs, or analyzes nuclear facilities), and
- safety management and administrative control software (performs a hazard control function).

Software Types

The NQA-1-2000-based Safety Software Guide defines work activities appropriate for five software types that are typically used in DOE applications. [4] These include:

1. ***Custom developed software*** is built specifically for a DOE application or to support the same function for a related government organization. Examples of custom developed software includes material inventory and tracking database applications, accident consequence

applications, control system applications, and embedded custom developed software that controls a hardware device.

2. ***Configurable software*** is commercially available software or firmware that allows the user to modify the structure and functioning of the software in a limited way to suit user needs. An example is software associated with Programmable Logic Controllers (PLCs).
3. ***Acquired software*** is generally supplied through basic procurements, two-party agreements, or other contractual arrangements. Acquired software includes commercial off-the-shelf (COTS) software, such as operating systems, database management systems, compilers, software development tools, firmware, freeware, and commercial calculational software and spreadsheet tools.
4. ***Utility calculation software*** typically uses COTS spreadsheet applications as a foundation and user developed algorithms or data structures to create simple software products. The utility calculation software is used frequently to perform calculations associated with the design of an SSC.
5. ***Commercial design and analysis software*** is used in conjunction with design and analysis services provided to DOE from a commercial contractor. An example would be where DOE or an M&O contractor contracts for specified design services support.

Grading Levels and SQA Work Practices

Given the common types of software used in DOE facilities for safety applications, the extent of Guide-based work practices are based on its grading level. Safety software grading levels should be described in terms of the application's safety consequence and regulatory compliance. The Guide recommends the following grading levels:

- **Level A:** This grading level includes safety software applications that meet one or more of the following criteria.
  1. Software failure that could compromise a limiting condition for operation.
  2. Software failure that could cause a reduction in the safety margin for a safety SSC that is cited in DOE approved documented safety analysis.
  3. Software failure that could cause a reduction in the safety margin for other systems such as toxic or chemical protection systems.
  4. Software failure that could result in nonconservative safety analysis, design, or misclassification of facilities or SSCs.
- **Level B:** This grading level includes safety software applications that do not meet Level A criteria but meet one or more of the following criteria.
  1. Safety management databases used to aid in decision making whose failure could impact safety SSC operation.
  2. Software failure that could result in incorrect analysis, design, monitoring, alarming, or recording of hazardous exposures to workers or the public.
  3. Software failure that could comprise the defense in depth capability for the nuclear facility.
- **Level C:** This grading level includes software applications that do not meet Level B criteria but meet one or more of the following criteria.
  1. Software failure that could cause a potential violation of regulatory permitting requirements.
  2. Software failure that could affect environment, safety, health monitoring or alarming systems.
  3. Software failure that could affect the safe operation of an SSC.

The grading level criteria are intended to provide for a higher grade level for software in nuclear facilities categorized as Category 1, 2 or 3 and the lower grading level for software in less than Category 3 facilities. [5] Table 1 indicates the recommended grading criteria relative to facility categorization.

Table 1. Use of Safety Software Guide for Software Types, Levels, and Facility Hazard Categories

Software type	Facility Hazard Category, 1 - 3			Facility Hazard Category, < 3		
	Grading level			Grading level		
	A	B	C	A	B	C
Safety System Software	X	X				X
Safety & Hazard Analysis Software & Design Software*	X	X	X	X	X	X
Safety Management & Admin Controls Software	X	X	X			X

The Guide uses the software application type, grading level, and facility categorization to recommend the SQA work activities for the software in question. The ten work activities are:

1. Software project management and quality planning
2. Software risk management
3. Software configuration management (SCM)
4. Procurement and supplier management
5. Software requirements identification & management
6. Software design and implementation
7. Software safety
8. Verification &Validation
9. Problem reporting and corrective action, and
10. Training of personnel in the design, development, use, and evaluation of safety software.

Guidance on meeting requirements for these activities is given in DOE G 414.1-4. Table 2 delineates required SQA work practices according to grading level and software type. Level C work activities have been omitted for clarity.

APPLICATION TO NEW FACILITIES

The use of the Safety Software Guide is illustrated with application to a Hazard Category-2 nuclear facility that is in design. While all software use for the design of the facility should be compliant with the Order and Guide, three are selected here for discussion purposes: a) Structural engineering software for design of the facility; b) Emergency preparedness facility software; and c) Accident analysis software for support of the Preliminary Documented Safety Analysis (PDSA).

A. Structural Analysis Software

The first software to be considered is a structural analysis application. Table 1 indicates that for Hazard Category 2 facilities that safety analysis and design software can be designated as Level A, B, or C. In view of the Level A criterion 4 – software failure could result in non-conservative safety analysis, design, or misclassification of facilities or SSCs, this software is regarded as Level A, best fitting the commercial design and analysis software type. Following Table 2 (based on Table 4 of the Safety Software Guide), of the ten SQA work practices, the requirements should be fully met for three: 1) procurement and supplier management; 2) software requirements identification & management; and 3) problem reporting & corrective action. Others can either be met using a graded approach or are not applicable. Because the structural analysis software is often proprietary, and a licensed copy is procured, part of the fees paid for the software application are for the software developer's SQA program, and the work practices are met through this mechanism.

B. Emergency Preparedness Software

The next type of software in this example is safety system software tied to air flow management in the facility's confinement system. It is configurable, commercially available, and allows modification such that it can be tailored to suit user needs in the facility. This software application is judged to be Level A because its failure could compromise a limiting condition for operation, and could cause a reduction in the safety margin for a safety SSC. Due to these factors, the safety contractor should address eight of the ten work practices fully (practices 1, 2, 4, 5, and 7-10). Software configuration management (3) and software design and implementation (6) could be met on a graded basis.

C. Accident Analysis Software

The final group of software applications includes accident analysis software. This can be considered to be custom-developed software that was developed by DOE, the Nuclear Regulatory Commission, or another government entity for the same analytical function (e.g. fire analysis, radiological dispersion and dose analysis, or similar accident analysis purpose). The toolbox codes including ALOHA, CFAST, EPIcode, GENII, MACCS2, and MELCOR, are in this group. It is judged that software of the type would be at the Level B grading level because software failure could result in incorrect analysis as well as compromise the defense in depth capability. Following Table 2, work practices 1, 3, 4, 5, 6, and 9 should be met fully to be compliant with the Order. Work practices for software risk management, safety, verification & validation, and training could be met on a graded basis.

CONCLUSIONS

The Safety Software Guide, *DOE G 414.1-4*, provides a roadmap for meeting DOE O 414.1C and the quality assurance program requirements of 10 CFR 830, Subpart A, Quality Assurance, for DOE nuclear facilities and software application activities. Using a systematic approach of categorizing software, assessing its grading level, and matching it to its facility safety function, SQA work practices are recommended for specific software applications. Use of the Guide to new facility design should streamline design activities that depend on software applications and significant reduce the likelihood of redesign and other resource miscalculations. Three specific types of software applications are used to illustrate implementation of the Guide.

REFERENCES

1. DOE O 414.1C, *Quality Assurance*, U. S. Department of Energy, Washington, D. C., (June 2005).
2. Title 10 Code of Federal Regulations (CFR) 830, Nuclear Safety Management.
3. Defense Nuclear Facilities Safety Board (DNFSB) Recommendation 2002-1, *Quality Assurance for Safety-Related Software*, Washington, D.C. (September 2002).
4. ASME NQA-1-2000, *Quality Assurance Program for Nuclear Facilities*, American Society of Mechanical Engineers, (2001).
5. DOE-STD-1027-92, *Hazard Categorization and Accident Analysis Techniques for Compliance with DOE Order 5480.23, Nuclear Safety Analysis Reports*, CN No. 1, U.S. Department of Energy, Washington, D.C., (September 1997).

Table 2. Mapping Safety Software Types and Grading Level to SQA Work Activities

SQA Work Activity	Level A					Level B				
	Custom Developed	Configurable	Acquired	Utility Calculations	Commercial D & A	Custom Developed	Configurable	Acquired	Utility Calculations	Commercial D & A
1. Software (SW) Project Management & Quality Planning	Full	Full	Grade	Grade	n/a	Full	Full	Grade	Grade	n/a
2. SW Risk Management	Full	Full	Full	Full	n/a	Grade	Grade	Grade	Grade	n/a
3. SW Configuration Management	Full	Grade	Grade	Grade	Grade	Full	Grade	Grade	Grade	Grade
4. Procurement & Supplier Management	Full	Full	Full	Full	Full	Full	Full	Full	Full	Full
5. SW Requirements Identification & Management	Full	Full	Full	Full	Full	Full	Full	Full	Full	Full
6. SW Design & Implementation	Full	Grade	n/a	Grade	n/a	Full	Grade	n/a	Grade	n/a
7. SW Safety	Full	Full	Full	n/a	n/a	Grade	Grade	Grade	n/a	n/a
8. Verification & Validation	Full	Full	Full	Grade	n/a	Grade	Grade	Grade	Grade	n/a
9. Problem Reporting & Corrective Action	Full	Full	Full	Grade	Full	Full	Full	Full	Grade	Full
10. Training Personnel	Full	Full	Full	Full	n/a	Grade	Grade	Grade	Grade	n/a