
SAFETY SOFTWARE
DOE O 414.1C
&
DOE G 414.1-4 Summary

Carl Mazzola for
Department of Energy, Environment Safety and Health,
Office of Quality Assurance Programs
October 2004



Purpose & General Information



- Improve DOE and contractor safety software
- Secretarial Commitment to DNFSB (Rec 2002-1)
- Focused on nuclear facility safety
- Compatible with national standards
- Compatible with current program requirements
- Does not supersede externally regulated software
- Current Status: Final stages of issuance

Scope & Definitions



Safety Software. Includes the following:

- **Safety System Software** - Software for a nuclear facility that **performs a safety function** as part of a structure, system, or component **and** is **cited in** either (a) a DOE approved **documented safety analysis** or (b) an approved **hazard analysis** per DOE P 450.4, *Safety Management System Policy*, dated 10-15-96, and the DEAR clause.

Scope & Definitions (cont'd)



Safety Software. Includes the following:

- Safety and Hazard Analysis Software and Design Software - Software that is **used to classify, design, or analyze** nuclear facilities. This software is not part of a structure, system, or component (SSC) but helps to **ensure the proper accident or hazards analysis** of nuclear facilities or an SSC that performs a safety function.

Scope & Definitions (cont'd)



Safety Software. Includes the following:

- Safety Management and Administrative Controls Software - Software that **performs a hazard control function** in support of nuclear facility or radiological safety management programs or technical safety requirements or other software that performs a control function necessary to provide adequate protection from nuclear facility or radiological hazards. This **software supports eliminating, limiting, or mitigating** nuclear hazards to workers, the public, or the environment as addressed in 10 CFR 830, 10 CFR 835, and the DEAR ISMS clause.

Basic Safety Software



Requirements DOE O 414.C

- Facility design authority involvement in identifying software specification acquisition, design, development, verification and validation (including inspection and test), configuration management, maintenance, and retirement.
- Identify, document, and maintain safety software inventory.
- Establishes ASME NQA-1-2000 or other national or international consensus standards that provide an equivalent level of quality assurance requirements as NQA-1-2000, must be used.
- Establish grading levels for safety software. Document those grading levels in the QAP.
- Select and implement the applicable software quality assurance work activities using the grading levels.

10 Required SQA Work Activities



1. Software project management
2. Software risk management
3. Software configuration management
4. Procurement & vendor management
5. Software requirements identification & management
6. Software design & implementation
7. Software safety design
8. Verification & validation
9. Problem reporting & corrective action
10. Training of personnel in the design, development, use & evaluation of safety software

Federal Responsibilities

DOE O 414.C



- Technical competency for oversight
- Formal qualifications for SQA points of contact
- Line assesses contractors to approved QAP and safety software processes
- EH issues requirements & guidance
- EH manages DOE SQA Program (central registry, monitor implementation, training, notifications, SME Panel, etc.)

Guidance Basics DOE G 414.1-4



- Provides detail **guidance** on **how** to implement the 10 work activities.
- Each work activity is described including sub-activities.
- Identifies grading based upon **software source types** and **level of impact** (Level A, B or C).
- Work activities are **fully** implemented or **graded**.
- In most instances, optional implementation of sub-activities provides the grading.

Description of Grading Levels



Level A includes safety software applications that meet one or more of the following criteria:

- ❑ Software failure that could compromise a limiting condition for operation.
- ❑ Software failure that could cause a reduction in the safety margin for a safety SSC that is cited in DOE approved documented safety analysis.

Grading Levels Description (cont'd)



Level A continued -

- ❑ Software failure that could cause a reduction in the safety margin for other systems such as toxic or chemical protection systems that are cited in either: 1) DOE approved documented safety analysis or, 2) an approved hazard analysis per DOE P 450.1 Safety Management System Policy and the DEAR ISMS clause.
- ❑ Software failure that could result in non-conservative safety analysis, design or misclassification of facilities or SSCs

Grading Levels Description (cont'd)



Level B includes safety software applications that do not meet Level A criteria but meet one or more of the following criteria:

- Safety management databases used to aid in decision making whose failure could impact safety SSC operation.
- Software failure that could result in incorrect analysis, design, monitoring, alarming, or recording of hazardous exposures to workers or the public.
- Software failure that could comprise the defense in depth capability for the nuclear facility.

Grading Levels Description (cont'd)



Level C includes software applications that do not meet Level B criteria but meet one or more of the following criteria:

- Software failure that could cause a potential violation of regulatory permitting requirements.
- Software failure that could affect environment, safety, health monitoring or alarming systems.
- Software failure that could affect the safe operation of an SSC.

Software Source Types

DOE G 414.1-4



1. Custom developed
2. Configurable
3. Acquired
4. Utility calculations
5. Commercial design & analysis

Graded Work Activities Guidance



SQA Work Activity	A					B					C				
Sw Source Type (see previous slide)	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
Sw project mgmt & QA	Full	Full	Grd	Grd	n/a	Full	Full	Grd	Grd	n/a	Grd	Grd	Grd	Grd	n/a
Sw risk mgmt	Full	Full	Full	Full	n/a	Grd	Grd	Grd	Grd	n/a	Grd	Grd	Grd	Grd	n/a
SCM	Full	Grd	Grd	Grd	Grd	Full	Grd								
Procurement & supplier mgmt	Full														
Sw rqmts id & mgmt	Full														
Sw design & implementation	Full	Grd	n/a	Grd	n/a	Full	Grd	n/a	Grd	n/a	Full	Grd	n/a	Grd	n/a
Sw safety	Full	Full	Full	n/a	n/a	Grd	Grd	Grd	n/a	n/a	Grd	Grd	Grd	n/a	n/a
V&V	Full	Full	Full	Grd	n/a	Grd	Grd	Grd	Grd	n/a	Grd	Grd	Grd	Grd	n/a
Prblm Rptng	Full	Full	Full	Grd	Full	Full	Full	Full	Grd	Full	Full	Grd	Grd	Grd	Grd
Training	Full	Full	Full	Full	n/a	Grd	Grd	Grd	Grd	n/a	Grd	Grd	Grd	Grd	n/a

Additional Guidance Elements



Matrix of 10 work activities to:

- Quality requirements in 10 CFR 830
- ASME NQA-1-2000

DOE's Central Registry Management Process

- Add, modify, or remove codes
- Criteria for evaluation based upon 10 work activities
- Contains detail procedures and evaluation input forms

Safety Software Assessment Tools

- Based upon 10 work activities and sub-activities
- Uses grading from the Guide
- Provides basic guidance on performing an assessment

Order & Guide Summary



- Order and Guide include SQA practices that are based upon consensus standards
- Order and Guide define a graded approach
- Order requires use of ASME NQA-1-2000 or equivalent level of quality assurance requirements
- Guide provides suggestions for implementing each of the 10 work activities using the graded approach
- Guide provides evaluation/assessment criteria for Central Registry and site specific safety software
- Guide provides procedures for maintaining Central Registry

Order & Guide Status



- All issues have been resolved
- PSO concurrence and DNFSB agreement expected early May
- Issuance expected early June
- Kick off general information meeting mid-late June

Contacts



- Bud Danielson
 - Bud.Danielson@eh.doe.gov
- Debra Sparkman
 - Debra.Sparkman@eh.doe.gov
- Robert Loesch
 - Robert.Loesch@eh.doe.gov