



Office of Environment, Safety, and Health

New DOE Safety SQA Requirements and Central Registry

**Debra Sparkman,
Software Quality Engineer
Lawrence Livermore National Laboratory for
Office of Quality Assurance Programs**

UCRL-PRES-220598



Overview

- ◆ **Roles and Responsibilities**
- ◆ **Significant Changes to Order**
- ◆ **5 Main Safety Software Requirements**
- ◆ **DOE Safety Software Central Registry**
- ◆ **Summary & Resources**

Questions welcomed throughout presentation





Roles and Responsibilities





EH Roles and Responsibilities

- ◆ **Serves the Secretary as DOE's independent element responsible for safety of the public, workers and environment**
- ◆ **Develops and maintains QA policy, requirements, guides, and standards for all DOE work**
- ◆ **Conducts Nuclear Safety Regulation Enforcement**
- ◆ **Manages Safety Software Central Registry**





Significant Changes





DOE O 414.1C Safety Software Changes

- **Safety software established as specific category of software**
 - **Scope of 10 CFR 830 and DOE O 414.1C includes software related to nuclear (including radiological) facilities**
- **Identification of Safety Software definitions, responsibilities and requirements**
- **Federal staff with SQA responsibilities must be qualified according to TQP and DOE-STD-1172**





Safety Software Definitions

- ◆ **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 ISMS clause [48 CFR 970.5223-1].





Safety Software Definitions continued

- **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.





Safety Software Definitions continued

- ◆ **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 [48 CFR 970.5223-1].





The 5 Main Requirements





1. Federal SQA Technical Qualifications

- ◆ **Must be qualified according to the Technical Qualification Program and DOE-STD-1172:**
 - **Review & evaluate safety software plans and processes**
 - **Verify safety software plans and processes are based upon hazard and risk analyses**
 - **Verify that safety software is developed, procured, verified, validated, used and maintained according to nuclear safety requirements**
 - **Assess & monitor safety software QA programs**
 - **Provide technical support for accident & occurrence investigations as they relate to safety software**





2. Facility Design Authority Involvement

- ◆ **Safety software cannot and should not be separated from the “safety system”**
- ◆ **Facility Design Authority needs to be involved in all aspects of the safety software**
 - **Specifications**
 - **Acquisitions**
 - **Design and development**
 - **V&V**
 - **CM**
 - **Maintenance activities**
 - **Retirement**





3. Safety Software Inventory

- ◆ Identify, document, and maintain the safety software inventory
- ◆ DSAs, TSRs and other safety documentation will assist in the identification
- ◆ Focuses the application of DOE O 414.1C requirements to safety software
- ◆ Assists in applying engineering and financial resources effectively by focusing on software that impacts safety





4a. Define Grading Level

- ◆ Define grading levels
- ◆ Document in QAP or other appropriate document
- ◆ DOE reviews and approves
- ◆ DOE G 414.1-4 grading levels
 - Are recommended but can use any grading level as noted above
 - Will be used by DOE EH for their safety software





4b. Define Consensus Standards

- ◆ Order invokes ASME NQA-1-2000
- ◆ Standards that provide an equivalent level of SQA requirements to NQA-1 may be used
- ◆ Determination and documentation of equivalency is required
 - Crosswalk is needed
 - DOE G 414.1-4 Table 3 provides assistance
- ◆ Document in QAP or other appropriate document
- ◆ DOE reviews and approves the standards selected





5. Select and Implement Work Activities

- ◆ **Basic SQA practices**
- ◆ **Consistent with consensus standards**
- ◆ **Map very closely to most sites institutional SQA program practices**
- ◆ **All work activities are not applicable to every type of software (i.e. acquired vs. custom developed)**





10 Work Activities

- ◆ **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**
- ◆ **Verification and validation**
- ◆ **Problem reporting and corrective action**
- ◆ **Training of personnel in the design, development, use and evaluation of safety software**





DOE Safety Software Central Registry





Central Registry Today

Toolbox Code	Safety Analysis Area	Owner / Developer
ALOHA 5.2.3	Chemical dispersion and consequence analysis	NOAA, EPA
CFAST 3.1.7 and 5.1	Fire analysis	NIST
EPICode 7.0	Chemical dispersion and consequence analysis	Homann and Associates
GENII 1.485 and 2.0	Radiological dispersion and consequence analysis	PNNL, EPA
MELCOR 1.8.5	In-facility transport; leak path factor analysis	SNL, NRC
MACCS2 1.13.1	Radiological dispersion and consequence analysis	SNL, NRC, DOE





Central Registry Efforts

- ◆ **Integrated Models for Bioassay Analysis (IMBA) Evaluation**
 - **IMBA Expert DOE-Edition**
 - **IMBA Professional Plus**
 - **Completion May 2006**
- ◆ **CFAST Modifications**
 - **NRC V&V improvements**
 - **DOE gap analysis improvements**
- ◆ **GENII Modifications**
 - **Full version updates for Bechtel SAIC Company at Yucca Mtn**
 - **NESHAPS version for EPA**





Central Registry Efforts (continued)

- ◆ **Field to establish tool box code priority for upgrade**
- ◆ **Determining Funding Resources for other tool box code improvements**
- ◆ **Developing EH specific procedures for management of Central Registry**





In Summary





Important Things to Remember

- ◆ **Scope of 10 CFR 830 and DOE O 414.1C includes software related to nuclear (including radiological) facilities**
- ◆ **Maintain a safety software inventory**
- ◆ **In an approved DOE document, define grading levels & consensus standards**
- ◆ **Select and implement the SQA work activities in accordance with ASME NQA-1-2000 or equivalent level of SQA**
- ◆ **Central Registry work is ongoing**





Resources

- ◆ EH QA Web Site
 - <http://www.eh.doe.gov/qa>
- ◆ EH SQA Knowledge Portal
 - <http://www.eh.doe.gov/sqa>
 - [EH SQA Discussion Forum](#)
- ◆ DOE-STD-1172-2003, Safety Software Quality Assurance Functional Area Qualification Standard
 - <http://www.eh.doe.gov/techstds/standard/std1172/std11722003.pdf>





Resources continued

- ◆ QA - Bud Danielson
301-903-2954
bud.danielson@eh.doe.gov
- ◆ SQA - Debra Sparkman
301-903-6888
debra.sparkman@eh.doe.gov



