New DOE Software Quality Assurance Requirements and Implications for Meteorology and Consequence Assessment Software

Cliff Glantz
Pacific Northwest National Laboratory
cliff.glantz@pnl.gov  509.375.2166
Outline

- The push for increased software quality assurance (SQA) at DOE nuclear facilities
- The new DOE SQA Order and Guide
- SQA Work Activities
- The graded approach allowed for SQA
- Implications for meteorological and consequence assessment software
- Need for balancing software technical capabilities and SQA
The Driver for New SQA Requirements


Found quality assurance problems in software (1) used to control safety systems and (2) used for safety design and analysis applications.

Found “no adequate oversight mechanism or comprehensive set of standards in place” for SQA.
Follow-up to the Initial DNFSB Report

DNFSB issued *Quality Assurance for Safety-Related Software* released in Sept 2002

Found efforts to improve SQA to be “stalled”

Called for prompt action to:

- Define responsibility and authority for SQA within DOE
- Designate a set of SQA-approved computer codes for safety analysis and design
- Establish requirements and guidance in the DOE directives system for a rigorous SQA process.
Implementation Plan for DNFSB Recommendations

- DOE accepted the DNFSB recommendations in Nov 2002
- Issued implementation plan in Mar 2003 with 26 commitments
- Included establishing a Central Registry for DOE Toolbox Codes used for safety design and analysis
- Currently has six codes in the toolbox: ALOHA, EPI, CFAST, GENII, MACCS2, & MELCOR
The SQA Order and the Guide

- DOE’s Environmental, Safety, and Health led the effort to complete the DOE SQA Order (DOE O 414.1C) and the Safety Software Guide (DOE G 414.1-4).

- One of the first questions asked by Site personnel: What types of software fall into the safety software category and are therefore covered by this order and guide?
What is Safety Software?

1. Software that performs a safety function as part of a structure, system, or component (SSC) at a nuclear facility and is cited in either (1) a DOE approved documented safety analysis or (2) an approved hazard analysis.

2. Software that is used to classify, design, or analyze nuclear facilities. This software is not part of an SSC but helps to ensure the proper accident or hazards analysis of nuclear facilities or an SSC that performs a safety function.
What is Safety Software? (cont)

3. Software that meets one or more of the following:
   - performs a hazard control function in support of nuclear facility or radiological safety management program
   - performs a control function necessary to provide adequate protection from nuclear facility or radiological hazards.
   - supports eliminating, limiting, or mitigating nuclear hazards to workers, the public, or the environment.
DOE O 414.C: The new DOE SQA Order

- Calls for more rigor in software design, development, documentation, testing, configuration management, and maintenance.
- Requires the use of ASME NQA-1-2000 or other national or international consensus standards that provide an equivalent level of quality assurance requirements.
- Allows a graded approach for implementing SQA work activities.
The Order’s Ten SQA Work Activities

1. Software project management
   - Identify tasks
   - Allocate resources
   - Determine schedule
   - Identify interdependencies

2. Software risk management
   - Assess what can go wrong
   - Determine what risks are important to address
   - Describe actions to mitigate these risks
SQA Work Activities (cont)

3. Software configuration management
   ● Establish system for configuration control and change management
   ● Maintain through entire life-cycle

4. Procurement and vendor management
   ● Requirements for supplier notification of defects, new releases, etc.
   ● Mechanisms for reporting defects and requesting assistance from vendor
   ● QA documentation/certification
5. Software requirements identification and management
   - Includes functional, performance, and security requirements
   - Requirements should be traceable through the life-cycle of the software

6. Software design and implementation
   - Describe how software will interface with other components
   - Complete functional and logical design information
7. Software safety design
   - Identify hazards that can potentially defeat a safety system
   - Design strategies to eliminate or mitigate these hazards

8. Verification and validation
   - Required at the end of software development and throughout life-cycle
   - Includes reviews of documentation, acceptance testing, periodic testing to identify any degradation of performance
SQA Work Activities (cont)

9. Problem reporting & corrective action
   ● Methods for documenting, evaluating, and correcting software problems
   ● Roles and responsibilities

10. Training of personnel
   ● Training in design, development, use, and evaluation of safety software
DOE G 414.1-4: The SQA Guidance Document

- Provides detailed guidance on how to implement the 10 SQA work activities
- Each work activity is described including sub-activities
- Establishes three levels of SQA (Level A, B, and C) to allow a graded approach for conducting selected SQA work activities. The SQA level is based on the type of safety application.
- In many instances, optional implementation of sub-activities provides the grading.
Software is **Level A** if it Meets One of the Following:

- A software failure could represent a limiting condition for operation of the facility.
- A software failure could cause a reduction in the safety margin for a safety system.
- A software failure could result in a non-conservative safety analysis, design, or misclassification of a facility.
Software is **Level B** if it Meets One of the Following:

- It is a safety management database used to aid in decision making and its failure could impact the operation of a safety SSC.
- A software failure could result in incorrect analysis, design, monitoring, alarming, or recording of hazardous exposures to workers or the public.
- A software failure that could compromise the defense in depth capability for the nuclear facility.
Software is **Level C** if it Meets One of the Following:

- A software failure could cause a potential violation of regulatory permitting requirements.
- A software failure could affect environment, safety, health monitoring or alarming systems.
- A software failure could affect the safe operation of an SSC.
The SQA Guide’s Specified Software Types

1. Custom developed
2. Configurable
3. Acquired
4. Utility calculations
5. Commercial design & analysis
<table>
<thead>
<tr>
<th>SQA Work Activity</th>
<th>Custom</th>
<th>Config.</th>
<th>Acquired</th>
<th>Utility</th>
<th>D&amp;A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Project Management</td>
<td>Full</td>
<td>Full</td>
<td>Graded</td>
<td>Graded</td>
<td>n/a</td>
</tr>
<tr>
<td>Risk Management</td>
<td>Full</td>
<td>Full</td>
<td>Full</td>
<td>Full</td>
<td>n/a</td>
</tr>
<tr>
<td>Configuration Management</td>
<td>Full</td>
<td>Graded</td>
<td>Graded</td>
<td>Graded</td>
<td>Graded</td>
</tr>
<tr>
<td>Procurmnt &amp; Supplier Mng.</td>
<td>Full</td>
<td>Full</td>
<td>Full</td>
<td>Full</td>
<td>Full</td>
</tr>
<tr>
<td>Requirements ID &amp; Mng.</td>
<td>Full</td>
<td>Full</td>
<td>Full</td>
<td>Full</td>
<td>Full</td>
</tr>
<tr>
<td>Design &amp; Implementation</td>
<td>Full</td>
<td>Graded</td>
<td>n/a</td>
<td>Graded</td>
<td>n/a</td>
</tr>
<tr>
<td>Safety</td>
<td>Full</td>
<td>Full</td>
<td>Full</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Verification &amp; Validation</td>
<td>Full</td>
<td>Full</td>
<td>Full</td>
<td>Graded</td>
<td>n/a</td>
</tr>
<tr>
<td>Problem Reporting</td>
<td>Full</td>
<td>Full</td>
<td>Full</td>
<td>Graded</td>
<td>Full</td>
</tr>
<tr>
<td>Training</td>
<td>Full</td>
<td>Full</td>
<td>Full</td>
<td>Full</td>
<td>n/a</td>
</tr>
<tr>
<td>SQA Work Activity</td>
<td>Type of Software</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Custom</td>
<td>Config.</td>
<td>Acquired</td>
<td>Utility</td>
<td>D&amp;A</td>
</tr>
<tr>
<td>Project Management</td>
<td>Full</td>
<td>Full</td>
<td>Graded</td>
<td>Graded</td>
<td>n/a</td>
</tr>
<tr>
<td>Risk Management</td>
<td>Graded</td>
<td>Graded</td>
<td>Graded</td>
<td>Graded</td>
<td>n/a</td>
</tr>
<tr>
<td>Configuration Management</td>
<td>Full</td>
<td>Graded</td>
<td>Graded</td>
<td>Graded</td>
<td>Graded</td>
</tr>
<tr>
<td>Procurmnt &amp; Supplier Mng.</td>
<td>Full</td>
<td>Full</td>
<td>Full</td>
<td>Full</td>
<td>Full</td>
</tr>
<tr>
<td>Requirements ID &amp; Mng.</td>
<td>Full</td>
<td>Full</td>
<td>Full</td>
<td>Full</td>
<td>Full</td>
</tr>
<tr>
<td>Design &amp; Implementation</td>
<td>Full</td>
<td>Graded</td>
<td>n/a</td>
<td>Graded</td>
<td>n/a</td>
</tr>
<tr>
<td>Safety</td>
<td>Graded</td>
<td>Graded</td>
<td>Graded</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Verification &amp; Validation</td>
<td>Graded</td>
<td>Graded</td>
<td>Graded</td>
<td>Graded</td>
<td>n/a</td>
</tr>
<tr>
<td>Problem Reporting</td>
<td>Full</td>
<td>Full</td>
<td>Full</td>
<td>Graded</td>
<td>Full</td>
</tr>
<tr>
<td>Training</td>
<td>Graded</td>
<td>Graded</td>
<td>Graded</td>
<td>Graded</td>
<td>n/a</td>
</tr>
<tr>
<td>SQA Work Activity</td>
<td>Type of Software</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------------------------</td>
<td>------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Custom</td>
<td>Config.</td>
<td>Acquired</td>
<td>Utility</td>
<td>D&amp;A</td>
</tr>
<tr>
<td>Project Management</td>
<td>Graded</td>
<td>Graded</td>
<td>Graded</td>
<td>Graded</td>
<td>n/a</td>
</tr>
<tr>
<td>Risk Management</td>
<td>Graded</td>
<td>Graded</td>
<td>Graded</td>
<td>Graded</td>
<td>n/a</td>
</tr>
<tr>
<td>Configuration Management</td>
<td>Graded</td>
<td>Graded</td>
<td>Graded</td>
<td>Graded</td>
<td>Graded</td>
</tr>
<tr>
<td>Procurmnt &amp; Supplier Mng.</td>
<td>Full</td>
<td>Full</td>
<td>Full</td>
<td>Full</td>
<td>Full</td>
</tr>
<tr>
<td>Requirements ID &amp; Mng.</td>
<td>Full</td>
<td>Full</td>
<td>Full</td>
<td>Full</td>
<td>Full</td>
</tr>
<tr>
<td>Design &amp; Implementation</td>
<td>Full</td>
<td>Graded</td>
<td>n/a</td>
<td>Graded</td>
<td>n/a</td>
</tr>
<tr>
<td>Safety</td>
<td>Graded</td>
<td>Graded</td>
<td>Graded</td>
<td>n/a</td>
<td>n/a</td>
</tr>
<tr>
<td>Verification &amp; Validation</td>
<td>Graded</td>
<td>Graded</td>
<td>Graded</td>
<td>Graded</td>
<td>n/a</td>
</tr>
<tr>
<td>Problem Reporting</td>
<td>Full</td>
<td>Graded</td>
<td>Graded</td>
<td>Graded</td>
<td>Graded</td>
</tr>
<tr>
<td>Training</td>
<td>Graded</td>
<td>Graded</td>
<td>Graded</td>
<td>Graded</td>
<td>n/a</td>
</tr>
</tbody>
</table>
Current Status of the New SQA Order and Guide

- All major issues have been resolved among the key regulatory and review agencies - including the DOE Program Secretarial Officer and the DNFSB
- Issued this week!
- Kick-off general information meeting (a video conference) will be held in DC on July 25.
Will Meteorology Software be Covered by these New Requirements?

The applicability of the new standards is not crystal clear – a lot of discretion will be given at each Site to the DOE staff member responsible for SQA. Likely to be covered are:

- Consequence assessment models for safety planning/design and emergency response applications
- Software used to generate health and safety action levels
- Software used to generate data or products used directly or indirectly by decision makers to make decisions regarding health and safety.
A Caution -- Balance Needed…

▶️ SQA should never be the only criteria used to select a software tool.

▶️ Technical quality and applicability to the problem must be of equal or greater importance.

▶️ We cannot allow SQA requirements to stymie innovation and accuracy.
Summary

- The new SQA Order and Guide have been issued to improve SQA for DOE’s safety-related software.
- The new Order requires use of ASME NQA-1-2000 or equivalent type of standard to guide SQA work.
- The Guide defines a graded approach for SQA.
- The new Guide provides suggestions for implementing each of the 10 major SQA work activities.
- Meteorological and consequence assessment modeling software will be affected by the new Order and Guide.
For More Information...

Key EH Contacts:
- Bud Danielson -- Bud.Danielson@eh.doe.gov
- Debra Sparkman -- Debra.Sparkman@eh.doe.gov
- Robert Loesch -- Robert.Loesch@eh.doe.gov

To get the latest information on the Order and Guide – go to the DOE/EH’s SQA website
Welcome to the Department of Energy’s Office of Environment, Safety and Health’s (EH) Software Quality Assurance (SQA) Knowledge Portal. The purpose of this Knowledge Portal is to promote continuous improvement and the sharing of knowledge of safety software quality assurance among interested parties across the DOE complex. It consolidates information and contains links to subject matter experts, procedures, training material, program descriptions, good practices, lessons learned and the Central Registry Toolbox Codes. The Portal also provides capabilities for member collaboration in product development and threaded discussions.