Software Quality Assurance Implementation Plan

October 26, 2004

Defense Nuclear Facilities Safety Board

Chip Lagdon

Director

Office of Quality Assurance Programs

Overview

- SQA Training
- SQA Directives Status
- Code Summary
- EPI Code
- SQA Occurrences
- SQA Assessment Status
- Assessment - Lessons Learned
- Open 2002-1 IP Commitments
- Path Forward

SQA Training

- SQA Training Conducted
  - ASQ Software Quality Engineer Course Content
  - May - 22 attendees from NNSA, EM, & EH
  - October – 7 attendees from EM, SO, & LANL
- 3 FAQS Competencies not Addressed
  - #1 Specific to DOE Nuclear Safety
  - #3 Specific to DOE Software Applications
  - #9 Specific to Safety Analysis Standards
- Assist in Providing Qualification Approaches

Status of EM and NNSA Personnel

- NNSA Personnel Qualification:

- EM Personnel Qualification:

SQA Directives Status

- DOE O 414.1C Draft Complete
  - DOE-wide review (RevCom) September 2004
  - Comment Resolution in Progress
  - Issue DOE O 414.1C December 2004
- DOE G 414.1-4 Draft Complete
  - DOE-wide review (RevCom) October 2004
  - Comment Resolution in Progress
  - Issue DOE G 414.1-4 December 2004
  - Current commitment is February 2005

DOE O 414.1C Comments

- Applicability and Responsibilities
  - EH should provide the Policy for quality assurance, manage the Program, but not take an oversight or review role to assess implementation of the quality assurance program.
  - Comments conflict with EH's role to be more proactive in quality assurance (including SQA) that goes beyond writing and maintaining the policies.

DOE O 414.1C Comments (cont.)

- Safety Software Definitions and Grading Levels
  - Conflicting comments over scope and grading levels.
  - Concerns that descriptions of Levels A & B increase scope beyond the definition of safety software.
  - Scope requested to be increased to include software important to safety that would not be within definition of safety software.
- NQA-1-2000
  - EM, NNSA and NE expressed concerns over requiring a specific version of NQA-1 for SQA.

Code Summary

- Issued code guidance reports for ALOHA, MACCS2, EPI Code, MELCOR, CFAST & GENII
- Posted on SQA Knowledge Portal
  - Notified Users via SQA Newsletter/List Server
- Continue to work with Code Developers
- Letter issued to PSO’s to determine interest in upgrading

Toolbox Codes - Upgrades

Software Application	Version (s)	Level of Effort to Achieve Minimum Compliance with SQA Criteria, (Duration/Cost)	DSA Process Support Importance, (High/ Medium/ Low)	Level of Use in DOE Complex, (High/ Medium/ Low)	General Observations
1. MACCS2	1.13.1	1.5 Years $300K	High	High	•Supports Safety-Class Determination •Appendix A Applications •PRA Applications Support from NRC
2. CFAST	3.1.7 and 5.1	1.0 Year $250K	High	High	•Extensive NIST Validation Program •Supports functional requirements for safety SSCs and Administrative Controls
3. GENII	2.0	1.5 Years $345K	High	Low	•Appendix A Applications •Safety-Class Control Confirmatory Use •Extensive, ongoing support through EPA
4. MELCOR	1.8.5	1.5 Years $325K	Medium	Low	•Useful for multi-cell facilities •NRC-Supported •International Benchmark Program
5. ALOHA	5.2.3	1.5 Years $250K	Medium	Medium	•Extensive NOAA Development Program •Helps Support Identification of Safety-Significant Controls
6. EPIcode	7.0	1.0 Years $220K	Medium	Low	•Proprietary •Helps Support Identification of Safety-Significant Controls

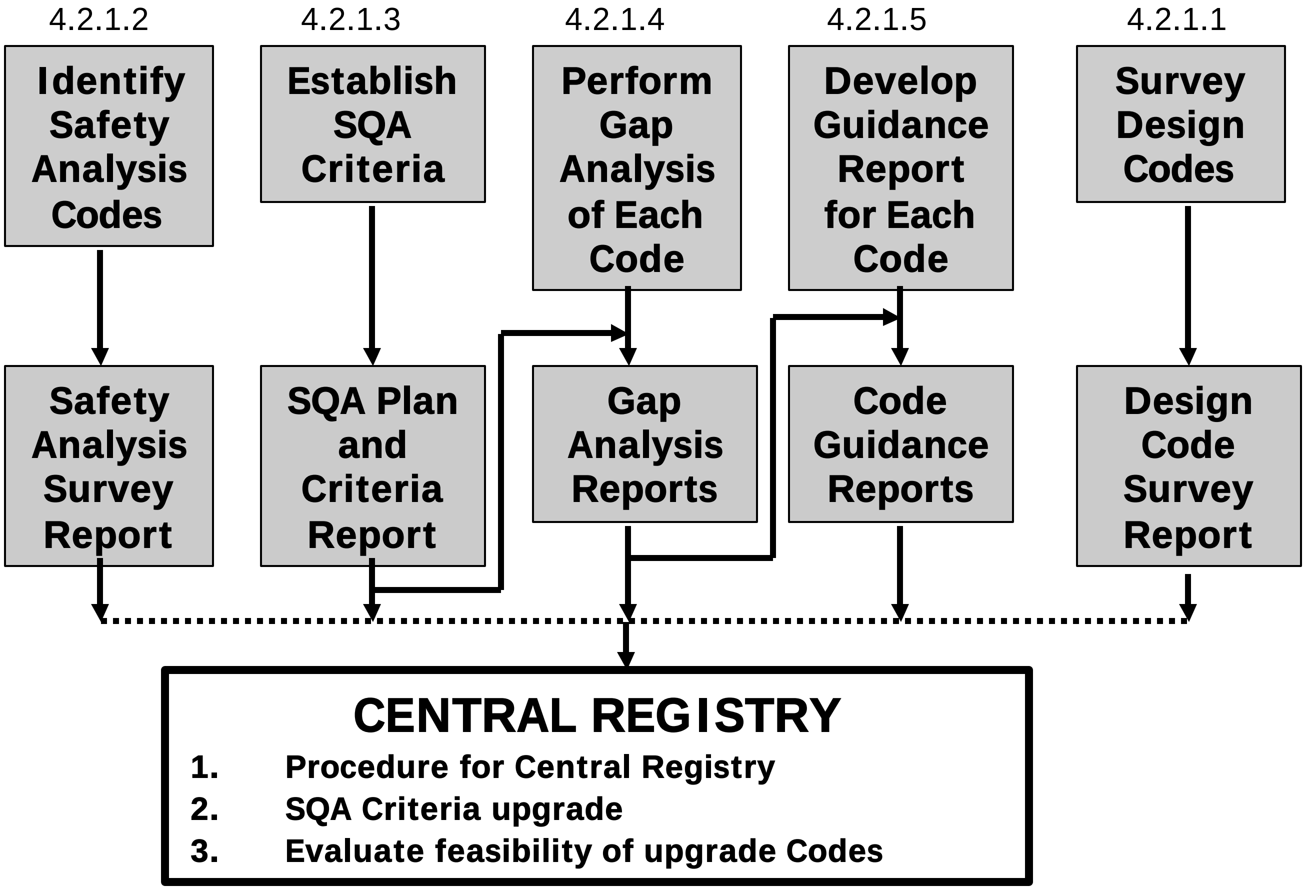
EPI Code

- EPI Code -Version 7 changed the evaporation rate of water from liquid spill scenarios by a factor 2.68 from previous versions.
- Concern was that certain chemical dispersions may result in higher concentrations in calculations using this code
- Central Registry email sent on 7/21 asked 4 questions
  - Could changes result in non-conservative impact?
  - Were users notified of the EPI Code changes?
  - Were calculations updated?
  - What version of the code is being used?

EPI Code (cont.)

- Negative response received from NTS, RL, ORP, SRS, Y-12, LLNL
  - Some use EPI Code for EPHA, different versions, but results are compared with other models
  - NA-41 uses ALOHA as the primary evaporative modeling program.
- LANL reported planning a PISA for one facility that used an older version of EPI Code – other facility DSA's used ALOHA or MACCS2
- Analysis of issue prepared by LLNL
  - Circulated through EFCOG
  - Recommendation is to update DSAs within the annual update cycle
- Issues Raised
  - Notification methods for code changes do not exist
  - Stresses importance of validating calculations for safety analysis work
  - Strengthens the case for having a fully functioning Central Registry that includes periodic surveys of design code usage in DSAs.

Overview of Code Commitments



	4.2.1.2	4.2.1.3	4.2.1.4	4.2.1.5	4.2.1.1
2002-1 Implementation Plan (IP) Commitments	Identify Safety Analysis Codes	Establish SQA Criteria	Perform Gap Analysis of Each Code	Develop Guidance Report for Each Code	Survey Design Codes
2002-1 IP Deliverables	Safety Analysis Survey Report	SQA Plan and Criteria Report	Gap Analysis Reports	Code Guidance Reports	Design Code Survey Report

CENTRAL REGISTRY

1. **Procedure for Central Registry**
2. **SQA Criteria upgrade**
3. **Evaluate feasibility of upgrade Codes**

Significant SQA Events

- AMWTP Facility Software
  - A software error could allow containers that have “failed” assay results to enter the Treatment Facility Mass Control Areas, creating a potential for a criticality event.
    - ID event investigation in progress
    - Lessons learned to be shared with SQA community
    - Implications for policy guidance and follow-up

Significant SQA Events

- Eberline HandECount Program Software
  - When performing a “update background” the background log is not updated unless the full 10 minute count is performed which may lead to invalid background information, creating false positive or false negative results.
    - Sent to S/CI registered users
    - SQA Central Registry List Server
    - Published Lessons Learned

SQA Assessment Status – EM & NNSA

- NNSA Assessment Status

- EM Assessment Status

Assessments – Lessons Learned

- Software Requirement Specification (SRS) and Software Design Document (SDD) are essential for developing quality software and life cycle maintenance.
  - Majority of software projects did not have SRSs and SDDs
  - Sites using the SRSs and SDDs have clear understanding of what was needed to develop and maintain software quality.
  - The sites without SRSs and SDDs appeared to be relying heavily on the available experts to ensure software is developed or procured to meet the project needs.

Assessments – Lessons Learned (cont.)

- Software procurement specifications should specify details of software requirements, not just catalog data.
  - Sites procuring PLC's for process systems only specified the vendors' catalog model information as procurement specifications
  - Supporting documentation for the suitability and applicability of the technical requirements not included

Assessments – Lessons Learned (cont.)

- Formal procedures for software problem reporting and corrective actions for software errors and failures need to be maintained and rigorously implemented.
  - Many sites resolve software errors and corrective actions at the project level and maintain informal coordination with vendors or other effected entities.
- Software quality assurance program and procedures should be rigorously implemented.
  - Assessments revealed inconsistencies in the requirements contained in the SQA program and procedures and their implementation.
  - Many sites rely on individual expertise and their personal effort and put less importance on corporate program.

Assessments – Lessons Learned (cont.)

- Appropriate qualifications and training on software use is essential for proper use of safety software.
  - Very sophisticated and complex software are being used without appropriate training in their use.
- Appropriate software control and configuration management are essential for safe use of the software.
  - Lack of proper control has resulted in multiple versions being available at the same time and even some with known errors.
  - Deficiencies have been noted with configuration control in terms of software version and documentation.
  - Inconsistencies exist in the requirements contained in the SQA program and procedures and their implementation.

Open 2002-1 IP Commitments

Commitment	Description	Responsibility	Status
4.1.4	Qualify Federal personnel	EM, NNSA	Open (9/04)
4.1.6	Revise FRA documents	NNSA	Open (4/04)
4.2.3.3 4.2.4.3	Conduct site assessments	EM, NNSA	Open (per schedule)
4.3.2.2	Issue SQA Directives	EH	Open (per 10/31/03 Letter)
4.3.3	Implement SQA Directives	EM, NNSA	Open (per issuance)

Path Forward

- Continue to support training and qualification of SQA personnel
- Begin upgrading toolbox codes
- Complete comment resolution and issue Order and Guide
- Institutionalize SQA under existing QA programs