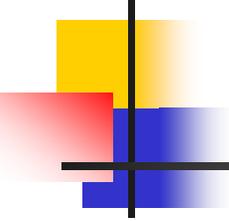


Progress in Addressing DNFSB
Recommendation 2002-1 Issues:
Improving Accident Analysis
Software Applications

Cliff Glantz, Pacific Northwest National Laboratory
for the Department of Energy/Office of Environment, Safety
and Health

2005 New Orleans SCAPA Meeting

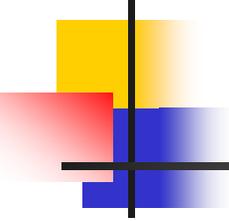
May 5, 2005



Presentation Outline

- Background on DNFSB Recommendation 2002-1
- Safety Analysis DOE's Implementation Plan (IP) Commitments
 - DOE Central Registry
 - Gap Analysis Reports for Toolbox Software
 - Code Guidance Reports
 - Improved Communication Links
 - Safety Software Guide (DOE G 414.1-4)
- Case Studies
- What is Past is Prologue: Current and Near-Term Actions





DNFSB Recommendation 2002-1

- Issued “Quality Assurance for Safety-Related Software” in September 2002
- Little progress and results in addressing SQA deficiencies identified in:
 - DNFSB Technical Report 25, *Quality Assurance for Safety Related Software at Department of Energy Defense Nuclear Facility*, January 2000
 - Earlier SQA programs identified by EH since 1989
- DNFSB public meeting on quality assurance held in August 2001
- Prompt actions needed in:
 - Defining SQA responsibility and authority
 - Recommending computer codes for safety analysis and design
 - Changing the Directive System
 - Conducting research and development



DNFSB Recommendation on Computer Codes

Identify:

- **Software** that would be recommended for use in performing design and analyses of SSCs important to safety, and for analysis of expected consequences of potential accidents.
- **Organization** responsible for management of each of these software tools, including SQA, technical support, configuration management, training, notification to users of problems and fixes, and other official stewardship functions.



Recommendation 2002-1 Implementation Plan

- DOE accepted Recommendation 2002-1 in November 2002
- Issued Implementation Plan (IP) in March 2003 with 26 Commitments
- Initiated work in June 2003
- EH responsible for 17 Commitments and overall completion of IP
- NNSA and EM responsible for 9 Commitments and performance and oversight of SQA activities at sites
- Nearly complete (May 2005) with QA Order and Safety Software Guide



2002-1 IP Commitments on Safety Analysis Codes and Toolbox: Process Improvements for Safety Analysis

Commitment	Description	Implementation Date	Status
4.2.2	Establish and implement a Central Registry	June 2004	<i>Completed</i>
4.2.1.3	Perform SQA gap analyses on toolbox codes	June 2004	<i>Completed</i>
4.2.1.4	Issue code-specific guidance reports	July 2005	<i>Completed</i>
4.4.2	Identify methods for capturing and clearly communicating SQA lessons learned, new technology, innovative technology, . . . , to ensure SW quality	June 2004	<i>Completed</i>
4.3.2.1 & 4.3.2.2	Establish a schedule to develop, revise, approve, and issue SQA directives including DOE O 414.1C	May 2005	<i>Approval Expected in May 2005</i>



Process Improvement 1: SQA Knowledge Portal & Central Registry

- Launched June 2004
 - <http://www.eh.doe.gov/sqa/>
 - Promotes continuous improvement and knowledge sharing of safety of safety SQA and related information
 - Consolidates information and contains links to SMEs, procedures, training material, program descriptions, good practices, lessons learned and Central Registry toolbox codes
- Active Pages (Partial list)
 - Central Registry
 - Site Assessments and CRADs
 - Discussion forum & Listserver
 - Training
 - SQA Directives
 - Sharing information and lessons learned
 - SQA Library
 - SQA Links & Newsletter



SQA Knowledge Portal is Cornerstone of Process Improvements

The screenshot shows the homepage of the SQA Knowledge Portal. At the top, there is a header for the U.S. Department of Energy, Office of Environment, Safety and Health. Below this is a navigation bar with links for Home, Department of Energy, Site Map, Search ES&H, Security and Privacy Notices, and Disclaimer. The main content area is divided into several sections:

- Left Sidebar:** Contains navigation links for About Us, ES&H Program/Topics, ES&H Corporate Reporting Databases, Resources/Tools, Software Quality Assurance Home, Central Registry, Central Registry Listserver, Site Assessments and CRADS, Discussion Forum, Training, SQA Directives, Sharing Information and Lessons Learned, SQA Library, and SQA Links.
- Hot Topics:** Lists "Accident Type A and B Investigations" and "Electrical Safety Campaign".
- Software Quality Assurance Knowledge Portal:** A central section with a welcome message and a list of key resources: Central Registry, Site Assessments and CRADS, and a partially visible Site Assessments and CRADS description.
- Latest News:** Features two news items: "OE Summary 2005-06 Discusses Carbon Monoxide Exposures (04/07/2005)" and "OE Summary 2005-05 Warns of the Hazards of Defeating Safety Interlocks (03/22/2005)". It also includes a link for "Special Operations Report published on Laser Safety (03/10/2005)" and a "More News" link.
- Events:** Lists the "2005 Pollution Prevention Workshop".

SQA Central Registry

(http://www.eh.doe.gov/sqa/central_registry.htm)

- **Includes six designated codes recognized for DOE “Toolbox”**
 - ALOHA, CFAST, EPIcode, GENII, MACCS2, MELCOR
 - Widespread application for Safety Basis document support
 - Routine use in DOE Complex for source term, facility leakpath, and dispersion/consequence analyses
- **Current information**
 - Guidance reports – code-specific applicable regimes, default inputs, and sample input file/output samples
 - Gap analyses – programmatic actions to improve codes against SQA requirements and technical recommendations for improving codes for safety analysis use
 - Design code survey and recommendations for toolbox

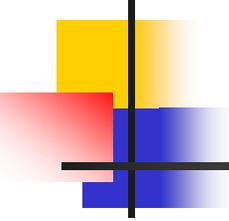


SQA Central Registry

- Additions, Revisions and Deletions

- **Safety Software Guide**
 - Discusses Toolbox SW in Section 3.2 *Special-Purpose SW Applications*
 - Appendix B – *Procedure for Adding, Revising, or Deleting SW*
- **Templates will be added to Central Registry page**
 - Software Information Template - Submitting SW for consideration to Toolbox
 - Submitted by sponsoring organization
 - Software Evaluation Template – Evaluating SW to demonstrate equivalency for Toolbox
 - Submitted by independent organization
 - Determination of acceptance to Toolbox made by Office of Quality Assurance





DOE Central Registry

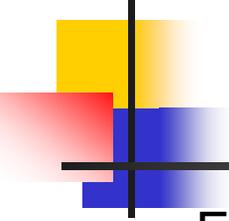
- Formed Safety Analysis Software Group (SASG) in 2001
- Used process and products from previous Accident Phenomenology and Consequence (APAC) Evaluation Program for code identification
- Developed, distributed and reviewed code survey of SQA practices, processes and procedures
- Identified computer codes used in support of accident analyses
- Screened over 200 computer codes
- Designated six computer codes for the “toolbox”



Safety Analysis Codes Designated for Toolbox

Code	Safety Analysis Area	Owner/Developer
CFAST (Consolidated Model of Fire Growth and Smoke Transport)	Fire analysis	NIST
ALOHA (Areal Locations of Hazardous Atmospheres)	Chemical dispersion and consequence analysis	NOAA, EPA
EPIcode (Emergency Prediction Information Code)	Chemical dispersion and consequence analysis	LLNL. Maintained by Homann Assoc. (Proprietary)
MELCOR (Methods for Estimation of Leakages and Consequences of Releases)	In-facility transport; leak path factor analysis	SNL, NRC
GENII (Hanford Environmental Dosimetry System (Generation II))	Radiological dispersion and consequence analysis	PNNL, EPA
MACCS2 (MELCOR Accident Consequence Code System 2)	Radiological dispersion and consequence analysis	SNL, NRC, DOE





Process Improvement 2: Gap Analyses for DOE Toolbox Software

Evaluating toolbox codes against SQA standards

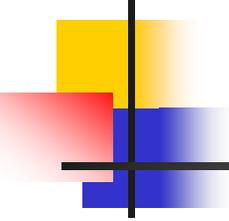
1. Primary Criteria

- Nuclear Safety Management Rule (10 CFR 830 Subpart A)
- NQA-1-2000, Subpart 2.7 and applicable parts of Part I
- DOE O 414.1C (QA), DOE G 414.1-2 9 (Quality Assurance Management System Guide), DOE N 411.1 (SQA)
- Related industry and international standards

2. Implementing Criteria

- Survey of QA programs in DOE Complex & NRC Nuclear Facilities
- Pick SRS, SNL, and YMP





Ten Requirements Evaluated for Gap Analysis of Designated Toolbox Codes

- **Level B, Existing Software – developed outside adherence to SQA standards**
- **Requirements**
 - **Software Classification**
 - **SQA Procedures/Plans**
 - **Requirements**
 - **Design**
 - **Implementation**
 - **Testing**
 - **User Instructions**
 - **Acceptance Testing**
 - **Configuration Control**
 - **Error Notification**
- **Added training evaluation and planned software improvement plans**



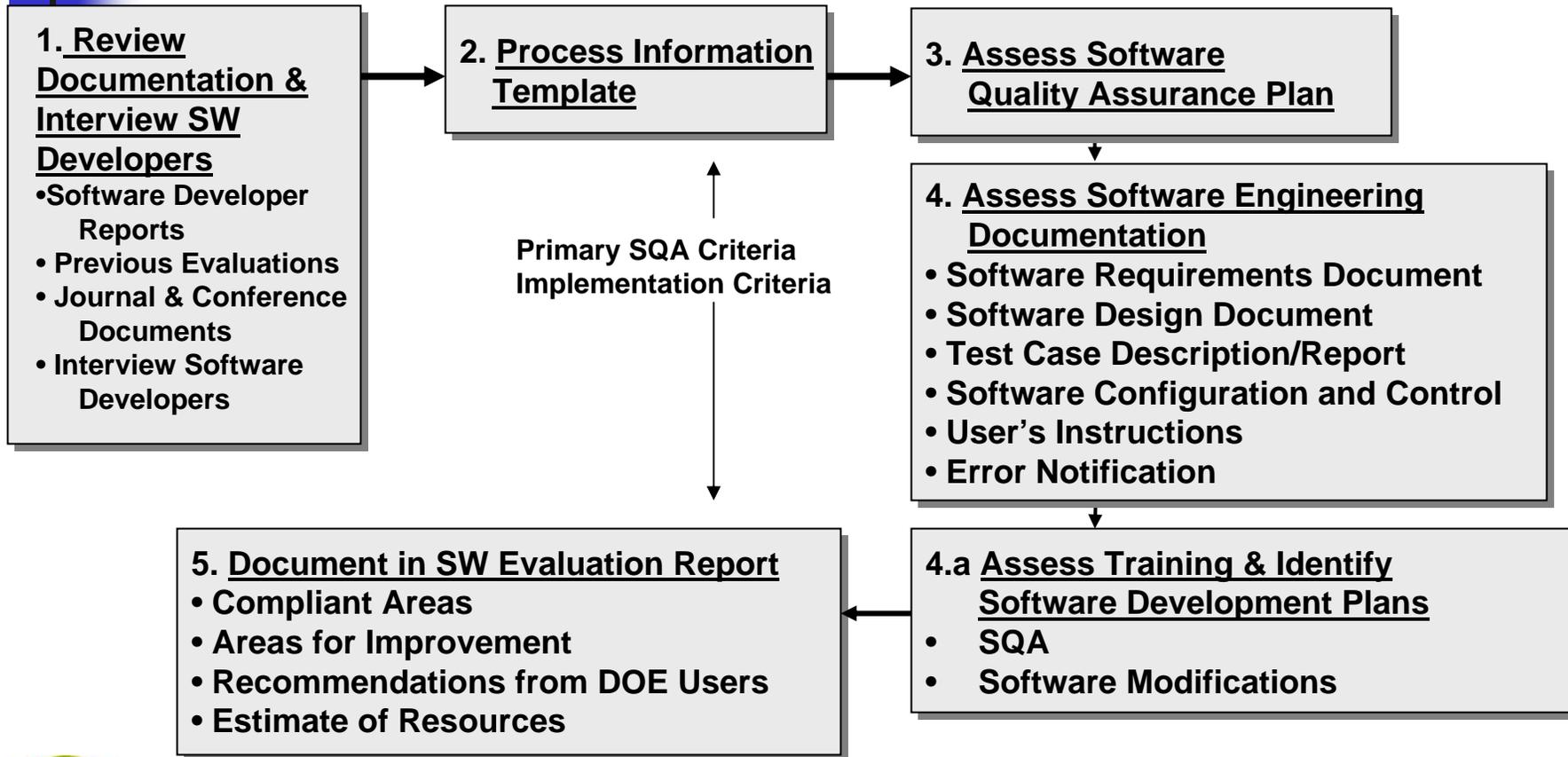
Implementing Procedures Based on Graded Application

REQUIREMENTS	Computer Software Origin		
	Level B Development	Level B Existing	Level B Purchased
1. Software Classification	Required*	Required	Required
2. SQA Procedures/Plans	Required	Required	
3. Dedication	Graded**	Graded	
4. Evaluation	Graded	Required	
5. Requirements	Required	Required	
6. Design	Required	Required	
7. Implementation	Required	Required	
8. Testing	Required	Required	
9. User Instructions	Required	Required	
10. Acceptance Test	Required	Required	
11. Operation & Maintenance	Required	Required	
12. Configuration Control	Required	Required	
13. Error Impact	Graded	Graded	
14. Access Control	Required	Required	

- Level B software applications important for DSA support
- Indirect effect
- Ten of 14 important for software developers
- Four of 14 relevant to software users



Gap Analysis Process for Toolbox Codes



Outcome of SQA Gap Analysis Evaluation

- Generic Results for Designated Software
 - Software found deficient in 3 or more primary criteria
=> Take compensatory measures
 - Continue to use but take interim measures
- Dialog with Software Developers
 - Recognize gaps and correct
 - Improve communications with DOE Users
- Advise Software Users and Safety Analysis Managers
 - Value of SQA pedigree for supporting safety basis
 - Technical model capabilities and limitations
 - Training needs
- Gap reports
http://www.eh.doe.gov/sqa/central_registry.htm

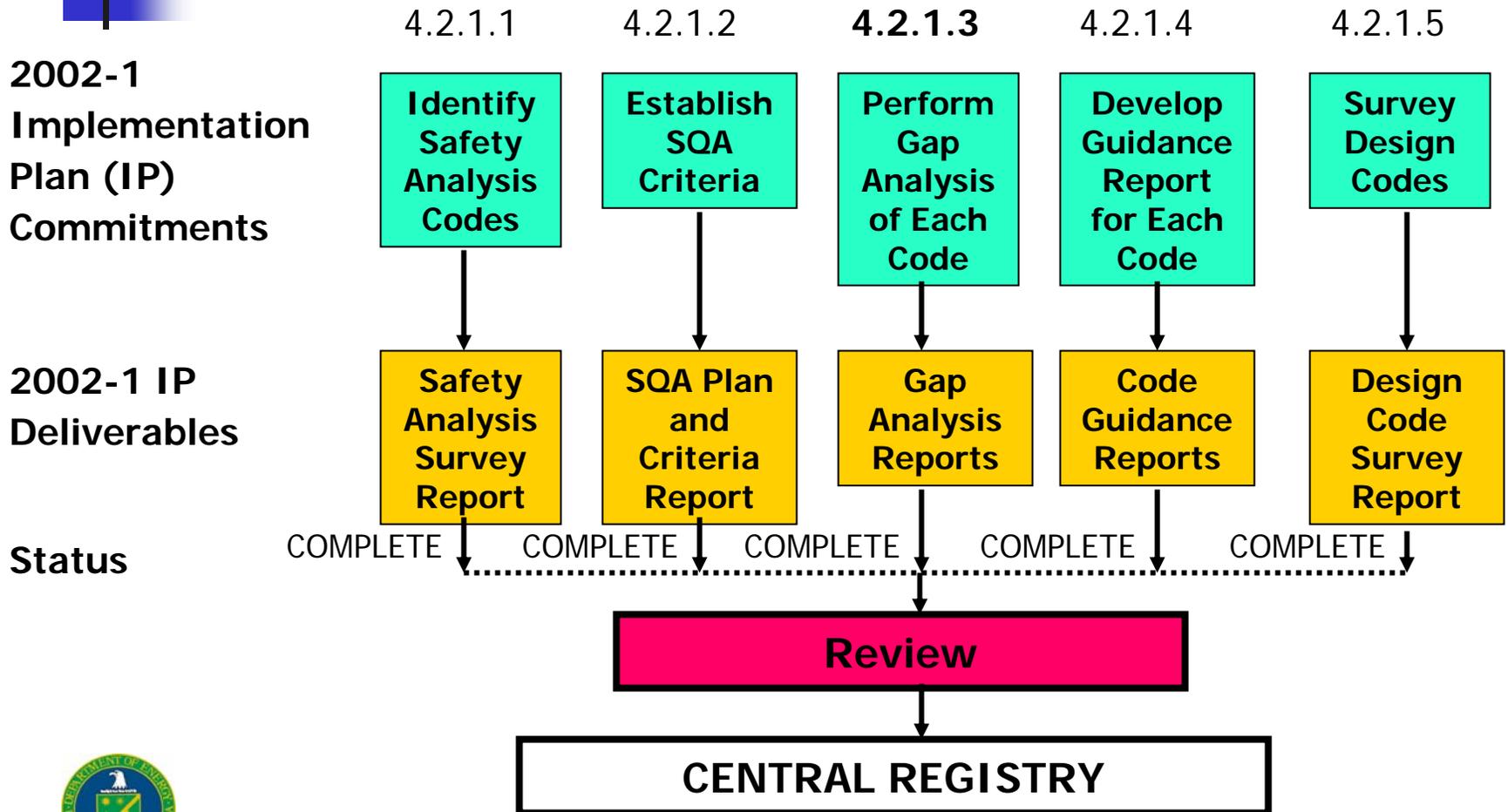


Process Improvement 3: Guidance on Use of DOE Toolbox Software

- Applicability information for DSA support – tailored to DOE needs
- Code Development information and SQA background
- Code limitations
- Input parameter recommendations as applicable
- Default input value recommendations for site-independent parameters
- Examples of code applications



Completion of IP Toolbox Code Documentation



Current SQA Library – Partial Listing

(http://www.eh.doe.gov/sqa/central_registry.htm)

SQA Library

This section of the webpage contains SQA documents, reports, and presentations.

PROGRAM DOCUMENTS

- Implementation Plan for DNFSB 2002-1 html WORD
- DNFSB Tech 25 html pdf
- NNSA Report on the Selection of Computer Codes pdf

CODES

- Final Design Code Survey Report Volume 1 (03/11/2004)
- Final Design Code Survey Report Volume 2 (02/24/2004)
- Design Code Survey Form
- SQA Plan Criteria
- ALOHA Final Gap Analysis Final Guidance Report
- CFAST Final Gap Analysis Final Guidance Report
- EPIcode Final Gap Analysis Final Guidance Report
- GENII Final Gap Analysis Final Guidance Report
- MACCS2 Final Gap Analysis Final Guidance Report
- MELCOR Final Gap Analysis Final Guidance Report



Process Improvement 4: Web-Based Sharing of SQA Information

- Discussion Forum
 - Virtual workspace for end users
 - General Issues, toolbox SW use, lessons learned
- Sharing Information/Lesson Learned Site
 - SQA applications and what was learned
 - Initial examples
 - Hanford SQA Safety Assessments
 - Fissile Tracking System at AMWTF
 - DOE/ID Best Practices
 - Training opportunities
- Websites:
 - <http://www.eh.doe.gov/sqa/discussionforum.htm>
 - http://www.eh.doe.gov/sqa/lessons_learned.htm



Process Improvement #5: Safety Software Guide

- **DOE G 414.1-4: *SAFETY SOFTWARE GUIDE for Use with 10 CFR 830 Subpart A, Quality Assurance Requirements, and DOE O 414.1C, Quality Assurance***
- **Purpose**
 - Provides information & acceptable methods for implementing SQA requirements of DOE Order O 414.1C
 - Includes software application practices covered by national and international consensus standards
- **Scope**
 - Covers: grading SQA requirements, applying to lifecycle phases, developing procurement controls, documenting customer requirements, managing SW configuration through lifecycle phases, performing Verification & validation processes, SW configuration reviews, and training
 - Includes safety system software and safety analysis and design SW
- <http://www.eh.doe.gov/sqa/directives/g4141-4.pdf>



Contents to Safety Software Guide – May 2005 Release

1. INTRODUCTION

1.1 Purpose

2. INTENDED USE AND RESPONSIBILITIES

2.1 Scope

2.2 Safety Software Application Types

2.3 Software Source Types

2.4 Graded Application

2.5 Responsibility for Safety Software

2.6 Safety Software Quality Program

2.7 Software Quality Assurance Program

3. GENERAL INFORMATION

3.1 System Quality and Safety Software

3.2 Risk and Safety Software

3.3 Special-Purpose Software Applications

3.3.1 Toolbox and Toolbox-Equivalent Software Applications

3.3.2 Existing Safety Software Applications

3.4 Continuous Improvement, Measurement, and Metrics

3.5 Use of National/International Standards

4. RECOMMENDED PROCESS

5. GUIDANCE

5.1 Software Safety Design Methods

5.2 Software Work Activities

5.2.1 Software Project Management and Quality Planning

5.2.2 Software Risk Management

5.2.3 Software Configuration Management

5.2.4 Procurement and Supplier Management

5.2.5 Software Requirements Identification and Management

5.2.6 Software Design and Implementation

5.2.7 Software Safety Design

5.2.8 Verification and Validation

5.2.9 Problem Reporting and Corrective Action

5.2.10 Training of Personnel

6. ASSESSMENT AND OVERSIGHT

6.1 General

6.2 DOE and Contractor Assessment

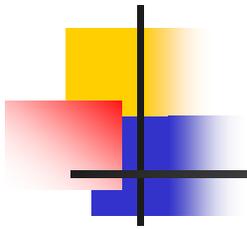
6.3 DOE Independent Oversight



Contents to Safety Software Guide – Appendices

APPENDIX A.	ACRONYMS AND DEFINITIONS
APPENDIX B.	PROCEDURE FOR ADDING OR REVISING SOFTWARE TO OR DELETING SOFTWARE FROM THE DOE SAFETY SOFTWARE CENTRAL REGISTRY
APPENDIX C.	USE OF ASME NQA-1-2000 AND SUPPORTING STANDARDS FOR COMPLIANCE WITH DOE 10 CFR 830 SUBPART A AND DOE O 414.1C
APPENDIX D.	QUALITY ASSURANCE STANDARDS FOR SAFETY SOFTWARE IN DEPARTMENT OF ENERGY NUCLEAR FACILITIES
APPENDIX E.	SAFETY SOFTWARE ANALYSIS AND MANAGEMENT PROCESS
APPENDIX F.	DOE O 414.1C CRITERIA REVIEW AND APPROACH DOCUMENT
APPENDIX G.	REFERENCES





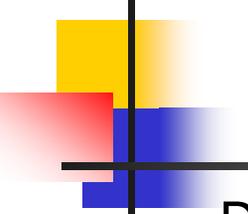
Case Studies on Improvements Through Central Registry Implementation

- **Case Study #1 – EPIcode evaporation model**
 - **Code guidance report noted change to liquid evaporation model**
 - **Change to EPA Offsite Consequence Analysis screening tool basis – 2.7 factor increase**
 - **Dissemination of issue through EH-31, SQA Knowledge Portal & EFCOG Steering Committee**

1. Could this change result in a non-conservative impact with respect to your DSA? Is this a significant change in the effects of liquid evaporation cases that would really matter to the safety analysis? Would the new information (increase by factor of 2.68 in evaporation rate) impact the safety decisions made at your facility?
2. Were your users notified of the EPIcode changes? (If so, how?).
3. What have your EPIcode users done? Were safety analyses reviewed to update appropriate documentation? Did the results change and if so how?
4. What version of EPIcode are you presently using?

- **One-Site, one-facility impact**





Case Study #2 – SQA Improvements

- Day-to-day use of SQA Knowledge Portal is good
- Toolbox SW developers
 - Aware of large DOE user group
 - Sensitized to 10 CFR 830 and QA Order requirements
 - Code websites improved
- Toolbox SW Users
 - **Discussion forum and other communication venues**
 - Better familiarity with appropriate domains for use
 - Aware of SQA requirements for safety basis code
 - Recognition of accident analysis examples
- DOE Complex software users, managers, and SW developers
 - Understand requirements and evaluation metrics for SQA
 - Availability of Safety Software Guide



What's Past is Prologue: Current and Near-Term SQA Improvements

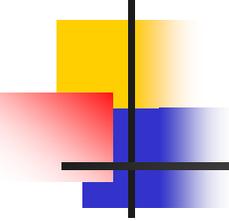
1. **Evolving needs for software indicate changes to toolbox**
 - Exercise software information & evaluation templates
 - Candidates for addition {e.g. IMBA, HOTSPOT}
2. **Improving communications and database access**
 - Notifications should be more timely and effective
 - Expect Prototype of EH Software Use Database
3. **Instilling Safety SQA Culture**
 - Some resistance present in incorporating SQA among programs, practices, and procedures
 - Ongoing need for user training and developer cooperation, and communication of success stories
4. **Upgrade Toolbox Software**
 - CFAST first, but through support-sharing with other stakeholder
 - Prioritize codes for upgrade



Prioritization Planning for Toolbox Upgrades

Software	DSA Support Importance	Extent of Use in DOE Complex	Comment
ALOHA (Areal Locations of Hazardous Atmospheres)	Medium	Medium	<ul style="list-style-type: none"> ■ NOAA, Sponsor ■ Supports Safety- Significant SSC Identification
CFAST (Consolidated Model of Fire Growth and Smoke Transport)	High	High	<ul style="list-style-type: none"> ■ NIST, Sponsor ■ Supports functional requirements for SSCs and ACs
EPIcode (Emergency Prediction Information Code)	Medium	Low	<ul style="list-style-type: none"> ■ Homann and Assoc. ■ Supports Safety- Significant SSC Identification
GENII (Hanford Environmental Dosimetry System (Generation II))	High	Low	<ul style="list-style-type: none"> ■ EPA, Sponsor ■ Supports Safety-Class SSC Identification
MACCS2 (MELCOR Accident Consequence Code System 2)	High	High	<ul style="list-style-type: none"> ■ NRC, Sponsor ■ Supports Safety-Class SSC Identification
MELCOR (Methods for Estimation of Leakages and Consequences of Releases)	Medium	Medium	<ul style="list-style-type: none"> ■ NRC, Sponsor ■ LPF tool





EH Contacts and Resources

Chip Lagdon, Acting, Chief of Nuclear Safety
301-903-4218, chip.lagdon@eh.doe.gov

Bob Loesch, Acting Director, EH Office of Quality Assurance
Programs, 301-903-4443, robert.loesch@eh.doe.gov

DOE Central Registry:
http://www.eh.doe.gov/sqa/central_registry.htm

DOE Directives:
<http://www.directives.doe.gov/>

