

# **MONITORING AND SHARING OF SOFTWARE ISSUES TO REDUCE RISK OF IMPACTS TO MISSION AND SAFETY**

**Donna R. H. Riggs, Oak Ridge Office**

**Debra R. Sparkman, Chief of Nuclear Safety Staff**

**2010 DOE ISM Champions Workshop**

**September 15, 2010**

# Authors Short Biography

- **Donna R. H. Riggs** 
- Bachelor of Science, 1983  
Master of Science, 1990  
Industrial Engineering  
University of Tennessee, Knoxville
- Weapons Engineer, Y-12 Site  
Office 1983 – 1991
- Sr. Quality Assurance Engineer,  
Oak Ridge Office, 1991 – present
- Registered Engineer in TN, 1998
- NQA-1 Lead Auditor
- Federal Technical Capability  
Program-qualified for Quality  
Assurance and Safety Software  
Quality Assurance
- Chair, EM/NE/SC Software Quality  
Assurance Support Group

- **Debra R. Sparkman** 
- Bachelor of Science, 1984  
Computer Science  
University of the Pacific
- Software Developer and Quality  
Engineer, Lawrence Livermore  
National Laboratory, 1976 – 2006
- Software Quality Subject Matter  
Expert, Chief of Nuclear Safety  
Office, 2006 – present
- NQA-1 Lead Auditor
- Federal Technical Capability  
Program-qualified for Safety  
Software Quality Assurance
- CNS Sponsor, EM/NE/SC Software  
Quality Assurance Support Group

# Why Is Software Important?

- **DOE mission is to advance the national, economic, and energy security of the United States; to promote scientific and technological innovation in support of that mission; and to ensure the environmental cleanup of the national nuclear weapons complex.**
- **Scientific research, engineering design, and facility operations are essential to success.**
- **Research and engineering analysis and design results must be accurate, credible, repeatable, and verifiable.**
- **Oversight and control of facility operations must provide consistent and expected actions and produce acceptable products and results.**
- **Software is increasingly used as a key component in these areas.**

# **EM/NE/SC Software Quality Assurance Support Group**

- **Chartered by the Office of the Chief of Nuclear Safety in 2007**
- **21 DOE organizations are represented through the participation of over 40 contacts**
- **Liaisons**
  - **DOE Office of Health, Safety and Security (HSS)**
  - **National Nuclear Security Administration (NNSA)**
  - **Chief of Defense Nuclear Safety (CDNS)**
  - **Defense Nuclear Facilities Safety Board (DNFSB)**
- **Networking for emerging issues with software (errors, assumptions, incorrect usage, events, lessons learned, etc.)**
- **Officers from field or support offices**

# Support Group Roles

- **Technical resource for DOE SQA matters**
- **Promote consistent line SQA oversight programs**
- **Share DOE SQA program information**
- **Communicate SQA lessons learned**
- **Provide technical assistance and mentoring from experienced SQA staff**
- **Assist in the field implementation of DOE SQA requirements**

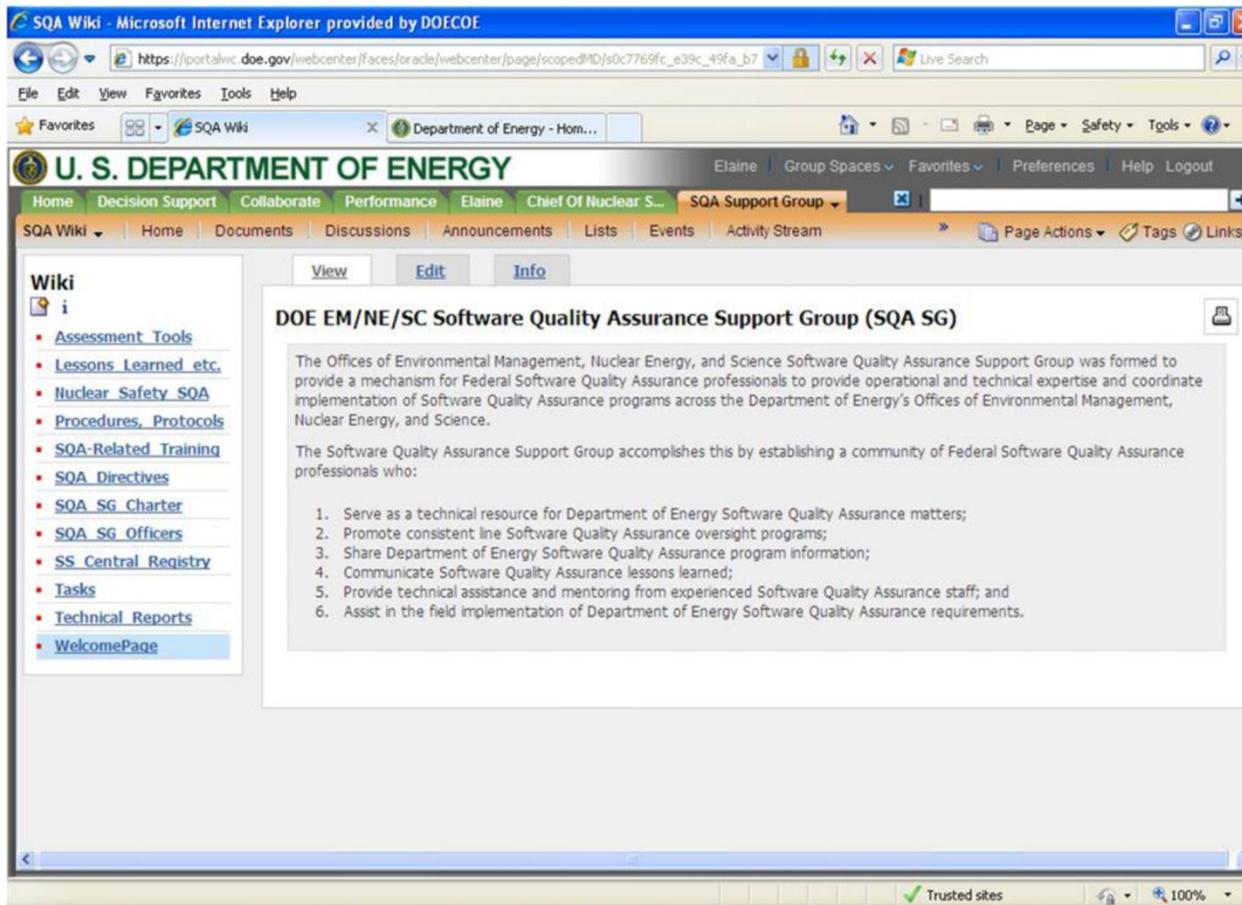
# Communication Methods

- **Monthly conference calls**
- **Annual meeting and continuing education**
- **Technical reports**
- **Just-in-time email messages**
- **Website hosted by Idaho Site Office  
[www.id.doe.gov/sqa/](http://www.id.doe.gov/sqa/)**

# Annual Meeting

- **Identification of common issues and needs**
- **Form teams to work on prioritized needs**
- **Tours when practicable**
  - **High Flux Isotope Reactor (Cat I)**
  - **Spallation Neutron Source (Accelerator)**
- **Continuing Education**
- **Sharing Best Practices**

# iPortal Under Development



Monitoring and Sharing of Software Issues  
to Reduce Risk of Impacts to Mission and  
Safety

# Facilitating Mission and Reducing Safety Risks

- **Increase Staff Competency**
- **Issue Technical Papers**
- **Influence DOE Requirements for Software**
- **Provide Early Notification of Software Issues**
- **Learn from Field Examples**
- **Reduce Recurrence of Events**

# Staff Competency Goals

- **Competent staff and adequate resources mitigate or eliminate barriers or risks**
- **Promote professional development and mentoring of EM, NE, and SC Federal staff**
- **Facilitate implementation of the Department's Safety Software Quality Assurance Functional Area Qualification Standard, DOE-STD-1172**
  - **Issued in 2003, under revision led by HSS**

# Staff Competency Methods

- **Classroom training**
  - **NQA-1 Applied to Software**
    - 50+ DOE Federal Staff
    - Nine+ of twelve competencies in DOE-STD-1172
  - **Who, Why, When, Where, What, and How (W5H) The Story of SQA in the DOE Complex**
    - Basic software engineering and software quality
    - An approach for implementing a graded SQA program
- **Facilitate experience in performing SQA assessments**
  - Identify opportunities at various sites
  - Coordinate mentoring of members
- **Topics on monthly conference calls**
- **Presentations at annual meeting**
- **Assist Qualifying Officials upon request**

# Technical Papers

- **SQASG-TP-07-01, *DOE Safety Software Examples***
- **SQASG-TP-09-01, *DOE Nuclear Safety Software Functional Qualification Standard Training***
- **SQASG-TP-09-02, *DOE Nuclear Safety Software Inventory Attributes***
- **SQASG-TR-10-01, *Systematic Approach to Implementing the Quality Requirements of DOE O 414.1C for Software***
- **Two more expected to be completed by the end of 2010**

# Influence on DOE Requirements

- **Ensure members are aware of DOE directives in development or under revision to assist in broader review**
- **Host technical discussions resulting in a more comprehensive technical review of the draft directives**
- **Selected content of technical papers under consideration for inclusion in DOE Order 414.1D, *Quality Assurance*, to promote more consistent implementation of DOE requirements**

# Early Notification of Software Issues

- **Promptly address software-related issues, defects, and improper usage to avoid multiple occurrences across DOE**
- **EM Waste Treatment Plant (WTP) staff identified in late June 2009 a software defect causing inconsistent results from MELCOR Accident Consequence Code System (MACCS)2 V1.13.1 and V2.4 widely used across the DOE complex to evaluate safety basis accident scenarios.**
  - **Communicated to SQA SG members during the July teleconference and in a detailed e-mail in July.**
  - **DOE Safety Advisory was issued in late August 2009.**

# Early Notification of Software Issues

- **SC Pacific Northwest National Laboratory staff identified in late February a scenario using the merged cell and mathematical functions within Microsoft Excel<sup>®</sup> that resulted in incorrect values.**
  - **The SQA SG took immediate action to validate the error and communicate the issue, along with an example, to all members of the SQA SG.**
  - **The DOE Safety Advisory issued in late March 2010.**

# Early Notification of Software Issues

- **NA Savannah River Site event on July 12, 2010 related to shutdown of a safety significant programmable logic controller (ICS Triplex T8110B processor) causing all air monitors in a facility to be non-operational**
  - **Product Notice issued by Rockwell Automation on June 17, 2010 for a kernel fault in T8110 processors resulting in unexpected system shutdown**
  - **Product Notice received by SRS in June, reviewed and filed**
  - **Kernel fault and firmware fix determined to apply to T8110B**
  - **Product Notice not revised to include T8110B processors**
  - **Email to SQA Support Group on August 12, 2010**

# Learning from Field Examples

- **Share actual procedures and methods used in the field**
  - Procedure to ensure quality in Excel spreadsheets used in engineering calculations
  - Critique of contractor quality assurance program plans
  - Assessment criteria and lines of inquiry for software
- **Technical discussions increase and refresh knowledge as well as promote consistent expectations for contractors' performance**

# Reducing Recurrence of Events

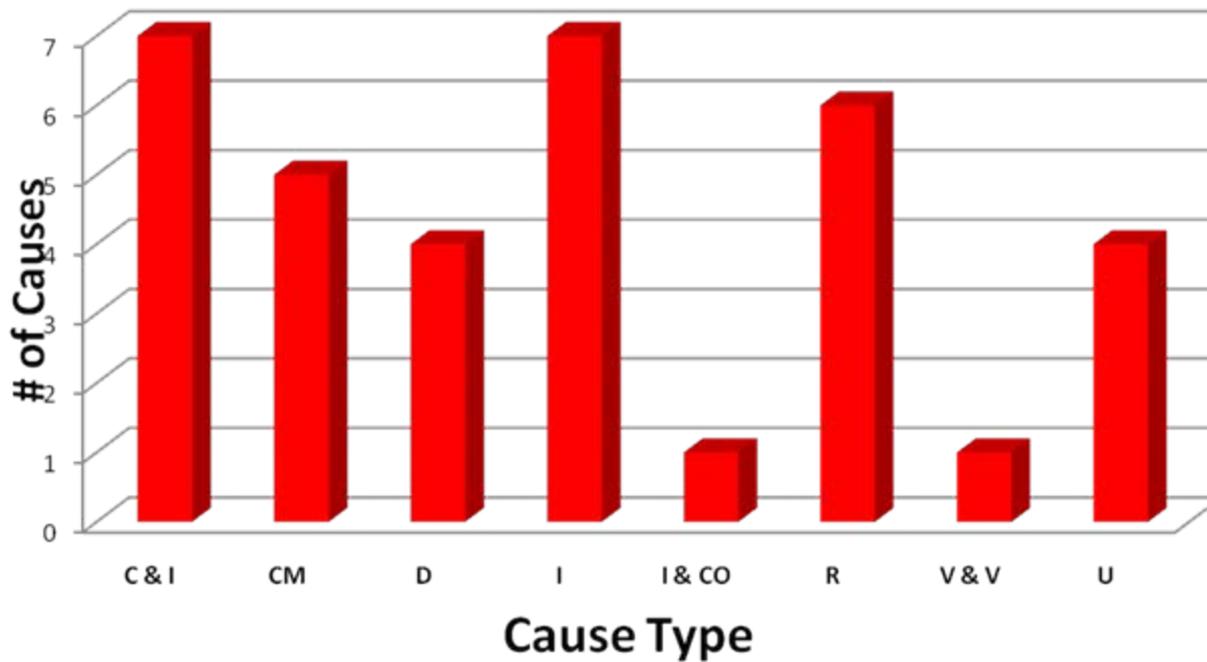
- **Task to identify, track, and analyze the event data collected as first step in preventing recurrence**
- **Analyzed thirty occurrence reports related to software in DOE's Occurrence Reporting and Processing System (ORPS) database**
- **Events about equally divided between NNSA (30%), EM (30%), and SC (27%)**
- **NE has the others (13%)**

# Reducing Recurrence of Events

- **Majority of the causes are related to:**
  - **Coding and implementation (C&I)**
  - **Input (I)**
  - **Requirements (R)**
  - **Configuration management (CM)**
- **Other causes:**
  - **Design (D)**
  - **User (U)**
  - **Verification and validation (V&V)**
  - **Installation and Check Out (I & CO)**

# Reducing Recurrence of Events

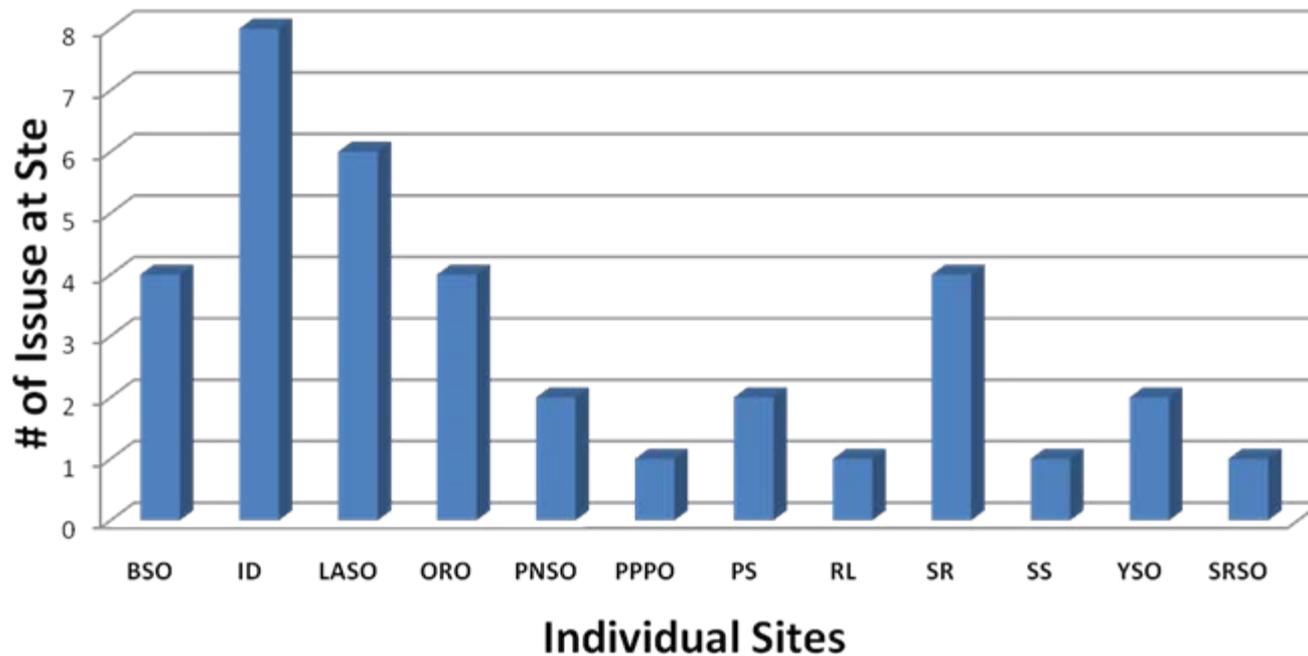
Safety Software & Non-Safety Software Causes  
CY 2008 - Q2 2010



Monitoring and Sharing of Software Issues  
to Reduce Risk of Impacts to Mission and  
Safety

# Reducing Recurrence of Events

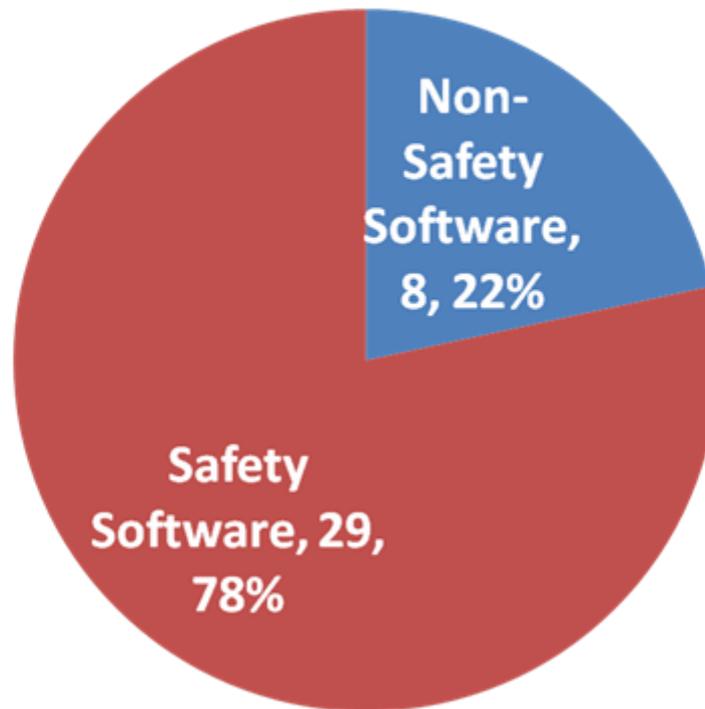
Safety & Non-Safety Software Issues Per Site  
(CY 2008 - Q2 2010)



Monitoring and Sharing of Software Issues  
to Reduce Risk of Impacts to Mission and  
Safety

# Reducing Recurrence of Events

Safety vs. Non-safety Software, 1/1/08-8/31/10



Monitoring and Sharing of Software Issues  
to Reduce Risk of Impacts to Mission and  
Safety

# Conclusion

- **Organizational structure, communication methods, training courses, technical reports, and data analyses in place to share knowledge**
- **Number of qualified Federal staff increased as a result of training courses and an assessor assistance program**
- **Technical papers used as references by Federal and contractor staff**

# Conclusion

- **Prompt dissemination of software-related concerns to initiate necessary actions to avoid multiple occurrences across DOE sites**
- **Technical interchanges via e-mail, teleconferences, and face-to-face meetings increased the quality of the reviews for DOE draft directives**
- **Trending provides foundation for understanding, and then correcting, root causes to ensure success of DOE's mission and decrease safety risks**

# Questions?

**D. R. H. Riggs, PE**  
**U.S. Department of Energy**  
**Oak Ridge Office**  
[RiggsDRH@oro.doe.gov](mailto:RiggsDRH@oro.doe.gov)  
**865.576.0063**