Applying DOE O 414.1C and NQA-1 Requirements to ISM Software [Nonnuclear Safety Software]

Presented at:

2009 DOE Integrated Safety Management (ISM) Conference
Quality Assurance Session
Knoxville, TN
August 25, 2009

Presented by:

Norman P. Moreau, PE, CSQE, CQA
Theseus Professional Services, LLC

Software Failures

- Carbon Dioxide release during electrical maintenance at DOE facility. A design defect in the microprocessor-based fire control system caused the unexpected discharge of a carbon dioxide fire suppression system without annunciation of the evacuation warning alarm. One worker died and three others required hospitalization.

- A computer-driven 3-axis mill did not stop at the intended pre-programmed position, and a flat end mill cutter penetrated about 0.75 inch into high explosive item at a DOE facility. No initiation of the high explosive. The possibility of the tool inadvertently moving into the explosive had not been considered in the job safety analysis, and adequate controls had not been incorporated into software programs.

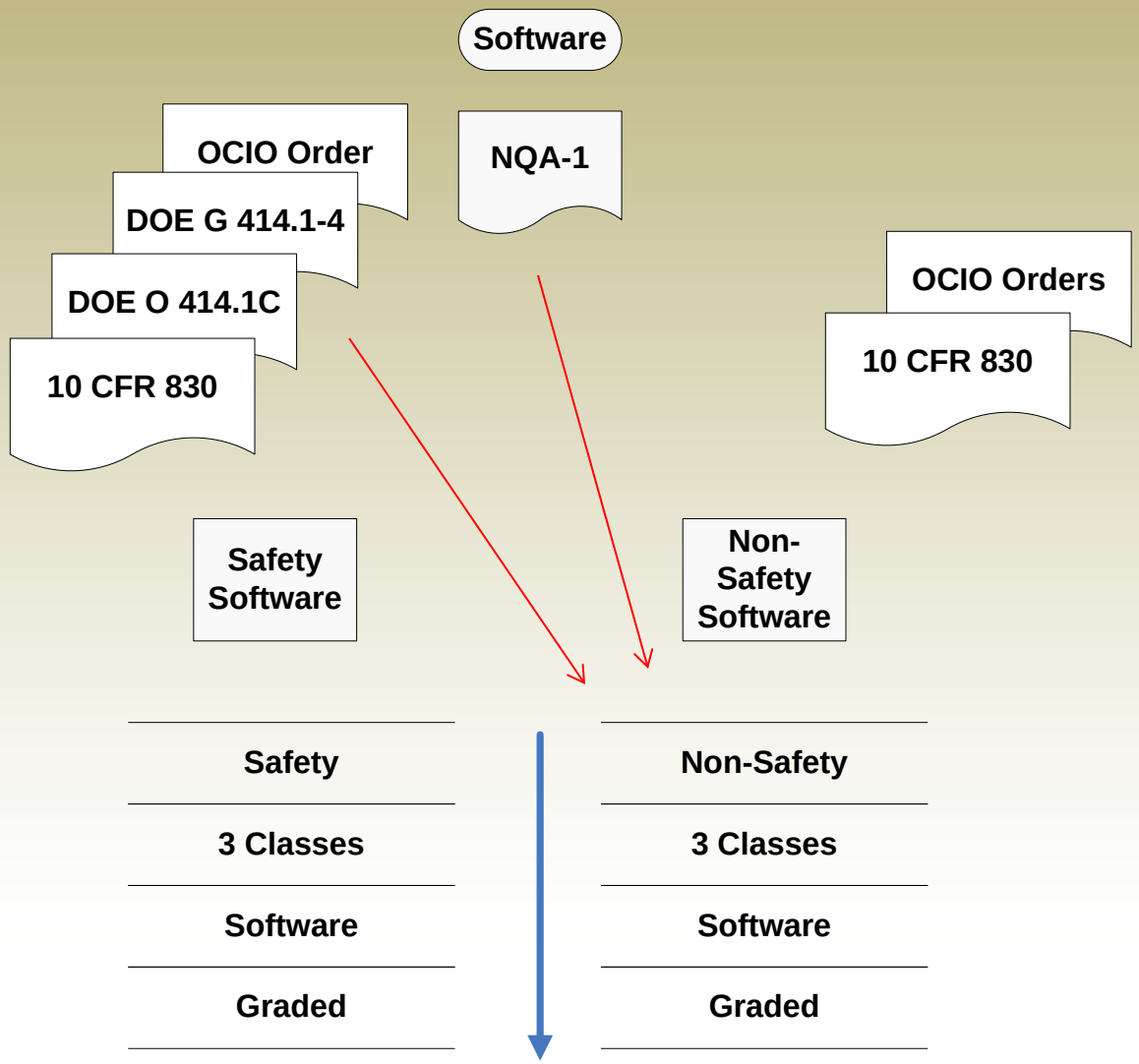
Software Failures

- Titan IV B-32 aborted after launch because software did not detect and correct a human error in the manual entry. Value should have been entered as –1.992476, but was entered as –0.1992476.

- Computerized training tracking system (TRAIN) reprogramming error resulted in expiration of Criticality Safety Training qualifications for several employees.

- Single faulty piece of embedded software, on a network card, sends out faulty data on the U.S. Customs and Border Protection network, bringing the entire system to a halt. Nobody is able to leave or enter the U.S. from the LA Airport for over eight hours.

Can DOE Order and NQA-1 Be Used In Non-Safety Software?



Using DOE O 414.1C: Non-safety Software - Classification

Software that is not designated safety software will be given the following software designations:

Level D Nonsafety Software (Safety and Hazard Analysis Software and Design Software)

- Software used in the design, analysis, or operation of structures, systems, or components where the software has been verified to provide accurate results within the range of software use. The software can be relied upon, and the results do not require additional checking when it used,

Using DOE O 414.1C : Non-safety Software - Classification

Level E Nonsafety Software

- Software that is either (1) not used in the design, analysis, or operations of structures, systems, or components; or (2) Software used in the design, analysis, or operations of structures, systems, or components where the software has not been verified to provide accurate results within the range of software use and the results are checked with each use in accordance with established instructions, processes, and procedures.

Using DOE O 414.1C : Non-safety Software - Classification

Level F Nonsafety Software

- Commercial Off-The -Shelf software that is defined as an operating system, general purpose utility, operating system utility, office support software, complier and associated libraries, support software, or database management software.

Using DOE O 414.1C : Software Quality Requirements

(1) Software project management and quality planning
(2) Software risk management
(3) Software configuration management
(4) Procurement and supplier management
(5) Software requirements identification and management
(6) Software design and implementation
(7) Software safety
(8) Verification and validation
(9) Problem reporting and corrective action
(10) Training of personnel in the design, development, use, and evaluation of safety software

Using DOE G 414.1-4: Common Types of Software [DOE G 414.1-4]

(1) Custom developed

- Material inventory and tracking database applications, accident consequence applications, control system applications, and embedded custom developed software that controls a hardware device

(2) Configurable

- Programmable Logic Controllers (PLC)

(3) Acquired

- Commercial off-the-shelf (COTS) software, such as operating systems, database management systems, compilers, software development tools, and commercial calculational software and spreadsheet tools (e.g., Mathsoft's MathCad and Microsoft's Excel).
- Downloadable software that is available at no cost to the user (referred to as freeware) is also considered acquired software.

Using DOE G 414.1-4: Common Types of Software [DOE G 414.1-4]

(4) Utility calculation

- COTS spreadsheet applications as a foundation and user developed algorithms or data structures to create simple software products

(5) Commercial design and analysis.

- Used in conjunction with design and analysis services

Using DOE O 414.1C : Graded Approach

- The process of ensuring that the levels of analyses, documentation, and actions used to comply with requirements are commensurate with —
  (1) the relative importance to nonnuclear safety, safeguards, and security;
  (2) the magnitude of any hazard involved;
  (3) the life-cycle stage of a facility or item;
  (4) the programmatic mission of a facility;
  (5) the particular characteristics of a facility or item;
  (6) the relative importance to ~~radiological and~~ nonradiological hazards; and
  (7) any other relevant factors.

Using DOE G 414.1-4 for: Grading

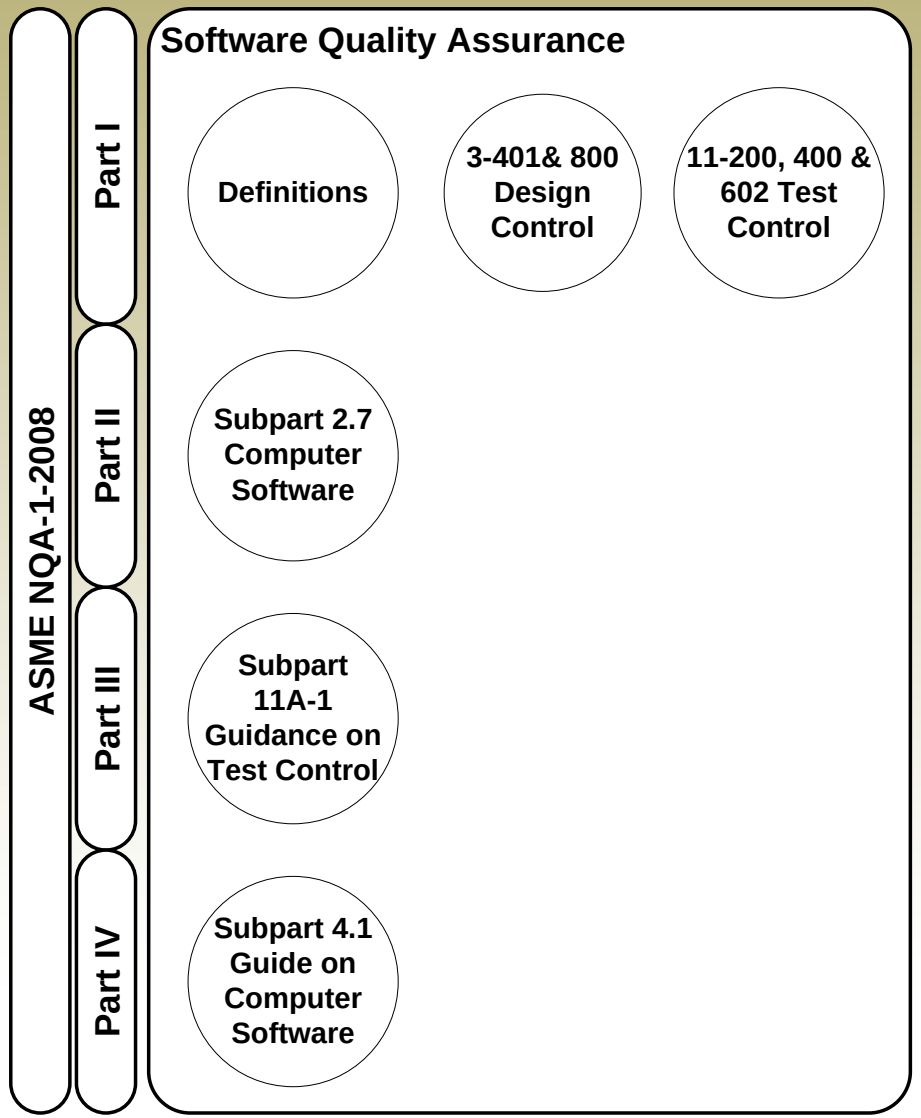
Table 4. Mapping Safety Software Types and Grading Levels to Software Quality Assurance (SQA) Work Activities

SQA Work Activity	Level A					Level B					Level C
	Custom Dev.	Configurable	Acquired	Utility Calcs	Commercial D & A	Custom Dev.	Configurable	Acquired	Utility Calcs	Commercial D & A	Custom Dev.
SW Project Mgmt. & Quality Planning	Full	Full	Grade	Grade	n/a	Full	Full	Grade	Grade	n/a	Grade
SW CM	Full	Grade	Grade	Grade	Grade	Full	Grade	Grade	Grade	Grade	Grade

Structure of ASME NQA-1-2008

- Forward
- Preparation of Technical Inquires
- Committee Roster
- Summary of Changes
- Part I Requirements for Quality Assurance Programs for Nuclear Facilities
- Part II Quality Assurance Requirements for Nuclear Facility Applications
- Part III Nonmandatory Appendices
- Part IV Nonmandatory Appendices: Positions and Application Matrices
- Interpretations

Where are software requirements and guidance in NQA-1-2008?



Understand the Structure of Subpart 2.7

100 General
- Applicability

101 Software Engineering
- Activities

102 Definitions
- Additional or Different than Part I

200 General Requirements
- 201 Documentation
- 202 Review
- 203 SCM
- 204 Problem Reporting and Corrective Action

300 Software Acquisition

400 Software Engineering Methods

500 Standards, Conventions, and Other Work Practices

600 Support Software

700 References

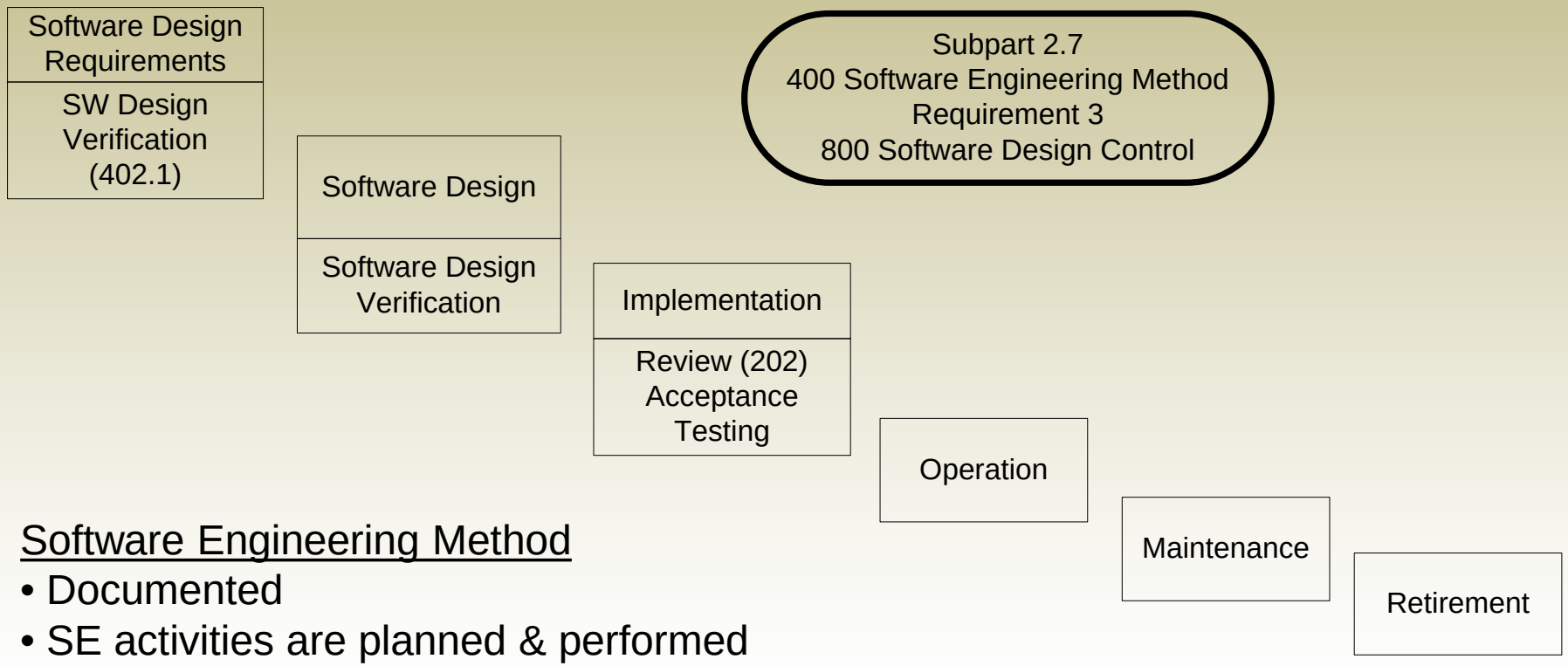
Also Structure of SP 4.1 except no definitions or reference para.

General

Subpart 2.7 – 100 General

- Requirements for Acquisition, Development, Operation, Maintenance, and Retirement
- Implemented through policies, procedures, plans, specifications, or work practices, etc., that provides the framework for software engineering activities
- SP 2.7 supplements Part I and used in conjunction with Part I when to the extent specified by the organization invoking the Subpart

Subpart 2.7
400 Software Engineering Method



<u>Software Engineering Method</u>

- Documented
- SE activities are planned & performed in a traceable and orderly manner
- Requirements of Req. 3 shall be met

Subpart 2.7
300 Software Acquisition

302 Otherwise Acquired Software

- Examples provided
- Perform evaluation
  - Identify and control prior to evaluation
  - Determine adequacy to support operation and maintenance
  - Identify activities to be performed and documented
- Determination documented and identify
  - Capabilities and limitations for intended use
  - Test plans and test cases
  - Instructions for use
- Document exceptions and justification for acceptance
- Evaluation and actions reviewed and approved
- Documentation and computer program establish current baseline
- Revisions evaluated

Other Sections

Subpart 2.7 – 500 Standards, Conventions, and Other Work Practices

Subpart 2.7 – 600 Support Software

Subpart 4.1 – 600 Support Software

Subpart 2.7 – 601 Software Tools

Subpart 2.7 – 602 System Software

Subpart 2.7 – 700 References

Summary

- Questions?
- For further information please contact:

Contact Information
Norm Moreau
Theseus Professional
Services, LLC
410-857-0023
nmoreau@theseuspro.com
http://www.theseuspro.com