SAND2013-2471C

Risk-Informed Approach to Grading Software

World Conference on Quality and Improvement
Session ISE 07
May 7, 2013 10:45am-11:45am

Dr. David E Peercy depeerc@sandia.gov
Sandia National Laboratories
ASQ Software Division Territorial Councilor, SouthWest Region
SAND2013-2471C

ASQ®
The Global Voice of Quality™

Topics

- Presentation Context
  - Consequence, Likelihood, Risk, Practices
  - System/Software Integration
- Determining Appropriate Software Practices Using a Risk-Informed Approach
  - Step 1: Determine Consequence of Failure Level
  - Step 2: Determine Likelihood of Failure Level
  - Step 3: Determine Risk Level and Associated Practice Level
  - Step 4: Risk Level Adjustment
- Example
  - Application of the process

Terminology

- Consequence
  - The impact, or severity, of an undesired system event (e.g., safety accident) were it to occur.
- Likelihood
  - A measure (quantitative or qualitative) that a product, as implemented using a specific set of product practices, will successfully implement its intended functions; that is, the product will NOT fail in a way that results in an undesired system event.
- Risk
  - The likelihood of an event, hazard, threat, or situation occurring and its undesirable consequences; a potential problem.

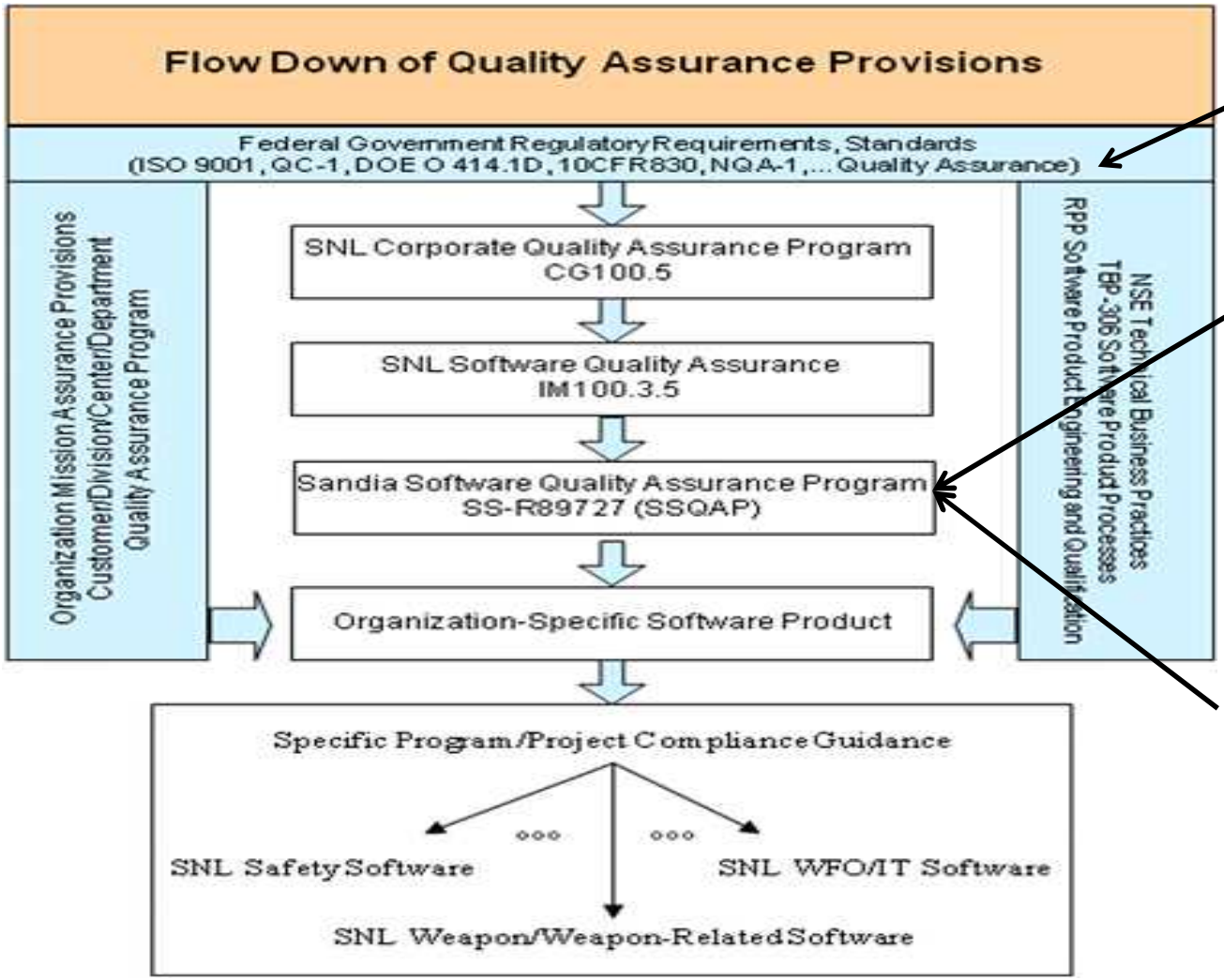
Presentation Context

In our case we are interested in **software** products and how to determine what **software practices** are appropriate to apply in order to have an acceptable level of risk that a failure will not occur – within the context of a specific application domain and a specific system in which the software is deployed.

Graded Approach

A graded approach for determining an acceptable software practice level based on consequence and likelihood levels is described in this presentation. The risk-informed approach depends on the system context for the software application and is linked to the practice activities of the SEI CMMI®. In addition, depending on the criticality of the software (e.g., safety-consequences) additional practice activities are defined.

Sandia Software Quality Assurance Program Context



Multiple Source Requirements

Risk-Informed Graded Approach

Practices Based On CMMI®

Process/Practice Categories of Interest

Process areas common to international standards and frameworks, are:

Configuration Management	Project Planning
Deployment	Requirements Development
Integrated Teaming	Requirements Management
Life Cycle Support	Risk Management
Measurement and Analysis	Technical Solution
Product Integration	Validation
Project Monitoring and Control	Verification

Documented practices are performed within these process areas. The practice level determines each project's implementation of the process areas cited above. Implemented practices must incorporate the following global practices:

- Role-based Training
- Relevant Stakeholders Involvement
- Objective Evaluation
- Collection of Improvement Information
- Problem Reporting and Corrective Action
- Quantitative Measurement, as determined by the project/organization business needs

Risk-Informed Process Steps

- Step 1: Determine Consequence of Failure Level
  - The consequence table provides five levels of potential impact or consequence of an undesirable event resulting from a software failure. The consequence level is selected based on the intended use for the software application and the potential consequence of a software failure without consideration of potential mitigation factors.
- Step 2: Determine Likelihood of Failure Level
  - The likelihood table provides five levels of likelihood that a software failure would result in an undesirable event. In this case, all non-software-specific mitigations are considered.
- Step 3: Determine Risk Level and Practice Level
  - The pairing of the consequence and likelihood of failure levels determines the risk level for a software product. Each of the risk levels is associated with a recommended practice implementation level. The recommended practice level provides the additional software mitigations against failure that should provide an acceptably low level of risk.
- Step 4: Risk Level Adjustment
  - If a different practice level than the one resulting from the combination of consequence and likelihood of failure levels is warranted, then specific adjustments with documented rationale can be performed.

The specific tables for consequence and likelihood that are illustrated are specific to the Sandia National Laboratories domains of application, but are typical of all applications. These tables should be tailored as appropriate for other organization use.

Process Step 1: Determine Consequence Level

Consequence table provides five levels of potential impact or consequence of an undesirable event resulting from a software failure: C0, C1, C2, C3, and C4 (from lowest to highest consequence respectively).

The consequence level is selected based on the intended use for the software application and the potential consequence of a software failure **without consideration of potential mitigation factors** (such as hardware barriers).

Consequence of Failure Tiers

Consequence Levels Depending on Application

NOTE: Determining consequence level is done without relying on any mitigations – even though they may exist. Determining likelihood is where mitigations **externa**l to the software are taken into consideration. It may also require the integrated use of system fault trees, system failure mode determination, system failure mode and effects analysis.

Process Step 2: Determine Likelihood Level

The likelihood provides five levels of likelihood that a software failure would result in an undesirable event: L0, L1, L2, L3, and L4 (from lowest to highest likelihood respectively). In this case, all non-software-specific mitigations (such as hardware, independent external/internal reviews) are considered.

- Five likelihood of failure tiers: negligible (L0), low (L1), moderate (M), high (H), and very high (VH)
- Likelihood of failure level: qualitatively/quantitatively determined based on multiple factors
- Failure is based on worst case system failure: application, consequence, likelihood combination
- Likelihood of failure level: determined by all possible system mitigation/compensatory measures
- Mitigations: analyzed to determine how much the likelihood is reduced from the L4 level
- If there are no system mitigations and the software failure would cause the specified system failure and associated consequence, then the likelihood of failure level is L4
- If such system mitigations and compensatory measures were probability measures (such as from a formal fault tree analysis), then the likelihood of failure levels could be described in terms of failure rates and/or distributions. However, that is not typically the case for all the possible mitigation effects.
- Justification for reduction of likelihood of failure levels: documented rationale is captured
- Likelihood of failure level: reduced one level for each major set of mitigation measures

Process Step 2: Likelihood Mitigation Examples

- System hardware failure protection mechanisms in direct fault tree relation to the potential software failure, such as system hardware failure protection mechanisms (e.g., safety interlocks)
- Internal system analysis/reviews that protect against the use of incorrect software results
- Independent external/SME reviews of analysis results that are based at least partially on the results of software execution
- Independent verification/validation of the software results (this may or may not be part of the actual software practices)
- Software characteristics/factors based on the nature of the application use

  Such factors might relate to software complexity, such as scope and number of external requirements; degree of innovation required; software dependencies such as the number and types of external interfaces; product/project stability and integration issues; budget and schedule pressure; uniqueness of the technology being implemented in software. Some of these factors/characteristics may or may not be part of the actual software practices.

Process Step 3: Determine Risk/Practice Level

The combination (i.e., pairing) of the consequence and likelihood of failure levels determines the risk level for a project: N (negligible), L (low), M (moderate), H (high), and VH (very high). Each of these risk levels is associated with a recommended practice implementation level: P0, P1, P2, P3, and P4 (from lowest to highest practice level respectively).The recommended practice level provides the additional software mitigations against failure that should provide an acceptably low level of risk.

Graded Risk Level (RL)
Associated SSQAP Recommended Practice Level (PL)

Likelihood Tier Undesirable event due to software failure	**Consequence Tier** Undesirable Event				
	C4 (Catastrophic)	**C3** (Severe)	**C2** (Moderate)	**C1** (Low)	**C0** (Negligible)
L4 (Very High)	**RL = VH PL = P4**	**RL = VH PL = P4**	**RL = H PL = P3**	**RL = M PL = P2**	**RL = L PL = P1**
L3 (High)	**RL = VH PL = P4**	**RL = H PL = P3**	**RL = M PL = P2**	**RL = M PL = P2**	**RL = L PL = P1**
L2 (Moderate)	**RL = H PL = P3**	**RL = M PL = P2**	**RL = M PL = P2**	**RL = L PL = P1**	**RL = L PL = P1**
L1 (Low)	**RL = M PL = P2**	**RL = M PL = P2**	**RL = L PL = P1**	**RL = L PL = P1**	**RL = N PL = P0**
L0 (Negligible)	**RL = L PL = P1**	**RL = L PL = P1**	**RL = L PL = P1**	**RL = N PL = P0**	**RL = N PL = P0**

Legend:
RL values: N = negligible, L = low, M = moderate, H = high, VH = very high
PL values: P0, P1, P2, P3, and P4 are defined in the Guidance to SSQAP Practice Levels. Practice activities related to these practice levels are provided in Table 3-3.

Process Step 3: Practice Level Activities

The Practice Levels essentially correlate with the CMMI maturity levels for software: P0 – ML0, P4-ML4/5. Each of the Process Areas have associated activities/tasks/etc that are dependent upon the particular practice level. A notional table of these activities that have been derived from the CMMI maturity levels is included below.

Practices Table

NOTE: If the highest consequence level and subsequent combination with likelihood resulting in the highest risk involves safety, then the additional safety practices would apply.

Safety SW Practices

InsructionsForDetermining-Safety SW

Process Step 3: Practice Level Guidance

P0 – Start with a thoughtful selection of value-adding practices from the P1 column.
P1 – Complete the remaining P1 column practices. Consider value-adding P2 column practices.
P2 – Complete the remaining P2 column practices. Consider value-adding P3 column practices.
P3 – Complete the remaining P3 column practices. Consider value-adding P4 column practices.
P4 – Complete the remaining P4 column practices.

P3 – Add these activities to each relevant Process Area:

- M.1 Establish an Organizational Policy
- M.2 Plan the Process
- M.3 Provide Resources
- M.4 Assign Responsibility
- M.5 Train People
- M.6 Manage Work Products
- M.7 Identify and Involve Relevant Stakeholders
- M.8 Monitor and Control the Process
- M.9 Objectively Evaluate Adherence
- M.10 Review Status with Higher Level Management

P4 – Add these activities to each relevant Process Area:

- H.1 Establish a Defined Process
- H.2 Collect Improvement Information

Process Step 4: Risk Level Adjustment

If a different practice level than the one resulting from the combination of consequence and likelihood of failure levels is warranted, then specific adjustments with documented rationale can be performed.

- Some factors (such as project or product complexity, security assurance, system engineering practices, and current versus desired technical maturity levels of the product) should be considered in this adjustment.
- Based on the software application and information in Steps 1-3, determine if more or less formality is appropriate for the specific software application.
- Some examples of project complexity factors include
  - team size and co-location (with larger and dispersed teams being more complex)
  - stability level of organization (both customer and developer)
- Some product complexity factors include
  - stability of requirements (with more instability being higher complexity)
  - number of requirements (the more requirements, the more complex), and
  - technical difficulty of meeting requirements (e.g., system technology being supported)

An Application Example

MCNP5 is an analysis code that is acquired from a regulatory-controlled repository. Its use is as an acquired product with additional practice activities conducted specific to its application use, as applicable.

Application-Specific Use

MCNP5 is utilized for the design and/or evaluation of the performance of nuclear facility SSCs. It is not software which operates or otherwise controls SSCs. The design/evaluation process is controlled by the quality assurance program, which includes peer and/or committee review of SSC design and modification and facility and experiment/activity safety analyses, the use of applicable design standards, and testing to evaluate design adequacy. In addition, there are regulatory requirements governing facility safety design practices, as well as the selection of conservative design and operational safety limits. Thus, a failure of a MCNP5 resulting in a calculation error would not result in the loss of a physical safety barrier. It could, however, result in a design inadequacy or a regulatory violation or facility shutdown due to significant regulatory issues.

Process Step 1: Determine Consequence Level

1. Determine Consequence level below.

____ **C4** -Death or serious injury to occupational worker
-Injury or illness to the public
-Severe offsite damage to the environment

____**C3** -Injury or illness to occupational worker
-Impact requiring immediate evacuation
-Severe damage to the environment contained within site property boundaries (onsite)
-Loss of primary safety barrier
-Incorrect classification of a facility resulting in severely reduced safety design

_X__**C2** -Loss of secondary safety barrier with no affect on primary safety barrier
-Regulatory violation or Facility shutdown due to significant regulatory issues
-Facility design inadequacy
-A system or subsystem failure that results in a significant facility shutdown

____**C1** -Minor damage to the environment contained within site property boundaries (onsite)
-Raise concerns with regulator
-Minor loss of facility availability

____**C0** -Negligible impact to employees or the public
-Negligible impact to the environment

Based on the MCNP5 application use and potential failures, the consequence level is determined to be C2.

Process Step 2: Determine Likelihood Level

The design/evaluation process is controlled by a quality assurance program which includes the following “external” activities that reduce the likelihood of software use failure:

(1) Peer and/or committee review of SSC facility design and any modifications

(2) Experiment/activity safety analyses independent of the software analysis results

(3) Independent testing to evaluate facility design adequacy

This set of activities reduces the likelihood by two levels from L4 to L2 of using the MCNP5 software analysis results in a manner that would result in facility design failure.

The documented rationale for Likelihood is L2.

Process Step 3: Determine Risk/Practice Level

Graded Risk Level (RL) Associated SSQAP Recommended Practice Level (PL)					
Likelihood Tier Undesirable event due to software failure	**Consequence Tier** Undesirable Event				
	C4 (Catastrophic)	**C3** (Severe)	**C2** (Moderate)	**C1** (Low)	**C0** (Negligible)
L4 (Very High)	**RL = VH** **PL = P4**	**RL = VH** **PL = P4**	**RL = H** **PL = P3**	**RL = M** **PL = P2**	**RL = L** **PL = P1**
L3 (High)	**RL = VH** **PL = P4**	**RL = H** **PL = P3**	**RL = M** **PL = P2**	**RL = M** **PL = P2**	**RL = L** **PL = P1**
L2 (Moderate)	**RL = H** **PL = P3**	**RL = M** **PL = P2**	**RL = M** **PL = P2**	**RL = L** **PL = P1**	**RL = L** **PL = P1**
L1 (Low)	**RL = M** **PL = P2**	**RL = M** **PL = P2**	**RL = L** **PL = P1**	**RL = L** **PL = P1**	**RL = N** **PL = P0**
L0 (Negligible)	**RL = L** **PL = P1**	**RL = L** **PL = P1**	**RL = L** **PL = P1**	**RL = N** **PL = P0**	**RL = N** **PL = P0**

Legend:
RL values: N = negligible, L = low, M = moderate, H = high, VH = very high
PL values: P0, P1, P2, P3, and P4 are defined in the Guidance to SSQAP Practice Levels. Practice activities related to these practice levels are provided in Table 3-3.

Using the combination (C2, L2) results in a Risk Level of P2

Process Step 3: Determine Risk/Practice Level

P2 PRACTICES

Since this MCNP5 software is acquired, there isn't much this organization can do about some process areas, e.g., technical solution, as well as some other areas.

However, some of the other areas such as verification and validation, configuration management, risk management, project quality planning, can be applied. As stated – additional analysis of software results and verification/validation testing of the MCNP5 for its specific application use is done.

In addition, for P2 areas that should have been covered by the developer, the regulatory agency that distributes the code has supporting evidence for how the process areas/associated practices are covered.

The rationale for each of the P2 process areas and practices in the practice table are documented in the MCNP5 Safety Software Quality Assurance Plan, in which it is also determined that because the application use of MCNP5 may result in loss of the secondary safety barrier, this use of MCNP5 makes MCNP5 safety software (in fact nuclear safety software since it is used in a nuclear facility).

BOTTOM LINE: What's Important?

(1) Always consider software effects in the context of the encompassing system and its application use.

(2) Graded really means determining the appropriate software practices to satisfy an acceptable level of risk that the software might execute in a way that results in a system failure. Not all failures are of equal importance!

(3) Risk level is determined by using a combination of consequence of failure and likelihood of failure for specified applications.

- Remember that consequence determination is at the system level and does not involve potential mitigations for the software failure. Mitigations are considered as part of the likelihood determination.
- The consequence and likelihood levels and associated criteria are organization-specific. Examples have been provided to illustrate the concept.

(4) The identified risk level (there is residual risk due to software) is reduced to an acceptable level by applying appropriate software practices. The CMMI® framework has been used to illustrate how this might be done.

Q&A

Process Step 1: Consequence Tier Levels

Consequence Tier	[#]Risk Categories/Consequences				
	Environment, Safety, & Health*	**Performance**	**Customer & Public Confidence**	**Safeguards & Security**	**Financial**
C4	▪ Catastrophe (death or serious injury) to occupational worker or public ▪ Severe damage to the environment beyond site property boundaries (offsite) ▪ Injury or illness to a member of the public ▪ Impact requiring immediate evacuation or other drastic action to protect the public	*Note: Only the ES&H and Security categories have Tier C4 consequences identified.*	*Note: Only the ES&H and Security categories have Tier C4 consequences identified.*	▪ Compromise of Top Secret Classified information ▪ Loss or theft of Category I quantity of Special Nuclear Materials (SNM)	*Note: Only the ES&H and Security categories have Tier C4 consequences identified.*
C3	▪ Injury or illness to occupational worker ▪ Severe damage to the environment contained within site property boundaries (onsite) ▪ Loss of primary safety barrier ▪ Incorrect classification of a facility, thus resulting in severely reduced safety design ▪ Incorrect decision regarding a safety issue with potentially catastrophic results	▪ Felony or similar level civil liability. ▪ Incorrect product qualification basis (primary source) ▪ Incorrect basis for critical business decision (primary source)	▪ Major loss of public/customer confidence; irreparably destroyed or damaged ▪ International adverse publicity ▪ PII issues + HIPAA	▪ Compromise of classified information ▪ Loss or theft of Category II/III quantity of SNM ▪ Loss of accountability for Category I quantity of SNM ▪ Compromise of the national security posture	Costs > $1M from lawsuits, settlements, lost wages/hours, or fines, etc.
C2	▪ Moderate potential of injury or illness to employees ▪ Loss of secondary safety barrier with no effect on primary safety barrier ▪ Serious regulatory violation ▪ Facility design inadequacy for safety ▪ Incorrect decision regarding a safety issue with potentially serious results	▪ Prevention of acceptable performance of critical functions ▪ A system or subsystem failure that results in a down system, for a long time ▪ Sandia work stoppage ▪ Incorrect product qualification basis (one source) ▪ Incorrect basis for critical business decision (one source) ▪ Serious civil liability	▪ Loss of public/customer confidence ▪ National adverse publicity ▪ Impact requiring action by off-site public ▪ Unauthorized access to PII	▪ Loss of accountability for classified information or access to it ▪ Loss of accountability for Category II/III SNM or access to it ▪ Loss of alarm monitoring for SNM or TS classified information ▪ Loss of video assessment for SNM ▪ Degradation of the national security posture ▪ Compromise of proprietary information or other intellectual property ▪ Loss of, or damage to, physical property valued in excess of allowable limit	Lawsuits, settlements, lost wages/hours, and fines >$100K or ≤$1M
C1	▪ Low potential of injury or illness to employees ▪ Minor damage to the environment contained within site property boundaries (onsite) ▪ Minor regulatory violation	▪ Cost or schedule impact, does not impact the performance of critical functions ▪ Sandia project work stoppage or operations inconvenience ▪ Minor civil liability	▪ Minor public/customer concern ▪ State/local adverse publicity ▪ Adverse publicity or reputation impact within customer/user community	▪ Loss of accountability for physical property ▪ Loss of accountability for proprietary information or other intellectual property ▪ Loss of accountability for access to property protection areas	Lawsuits, settlements, lost wages/hours, or fines >$10K and ≤$100K
C0	▪ Negligible impact to employees or the public ▪ Negligible impact to the environment	▪ Negligible impact to performance requirements or system integrity ▪ Negligible impact to project; potential project inconvenience	▪ Negligible public/customer concern ▪ Adverse publicity (if any) restricted within Sandia	▪ No security implications	Lawsuits, settlements, lost wages/hours, or fines ≤$10K

[#] The bulleted consequences are examples of the typical concerns for each consequence level and each risk category; this is not meant to be a comprehensive list.
[♭] If there is a potential for a radiological exposure, analysis of a potential radiological exposure, or if the software is safety software as per DOE O 414.1D, safety basis knowledgeable personnel involvement isrequired for Tier determination.

Process Step 1: Consequence Level

	Risk Categories/Consequences				
Application Area	**Environment, Safety & Health**	**Performance**	**Public & Customer Confidence**	**Safeguards & Security**	**Financial**
<app1>					
<app2>					
<app3>					
…					
Max Level					
Consequence of Failure Level (Max)					

Note: the worst case "risk" will be a combination of application, consequence level and likelihood level, so it will be necessary to consider the worst case combination, not necessarily just the worst case consequence.

References of Some Interest

APPENDIX A. REFERENCES

A.1. DOE Regulatory Requirements and Guidance

a. 10 CFR 830, "Nuclear Safety Management," January 2001
b. 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," U.S. Department of Energy, June 2005(or latest version)
c. DOE O 414.1D, "Quality Assurance," U.S. Department of Energy, April 2011
d. NNSA Safety Software Handbook, "NNSA Safety Software Quality Assurance Handbook, Part I: Expectations and Assessment Practices," September 2005
e. NNSA Safety Software Handbook, "NNSA Safety Software Quality Assurance Handbook, Part II: Software Safety Engineering Practices," October 2006
f. OMB M-07-16, Safeguarding Against and Responding to Breaches of Personally IdentifiableInformation
g. QC-1 Rev 10, "DOE/NNSA Weapon Quality Policy," U.S. Department of Energy, National Nuclear Security Administration, February 10, 2004

A.2. International and National Standards and Guides

a. ASME NQA-1-2000/2004/2008, "Quality Assurance Requirements for Nuclear Facility Applications," 2000 and 2004/2008 (updated versions no significant changes for software)
b. AUST DEF Guide, "+SAFE – A Safety Extension to CMMI-DEV," Version 1.2, Australian Department of Defence, March 2007
c. CMMI-DEV, "CMMI for Development," V13, CMU/SEI-2010-TR-033, November 2010
d. IEEE12207-0-IEEE/EIA Std 12207.0-1996, "Software life-cycle processes," IEEE Computer Society, March 1998
e. JA1002, Software Reliability Program Standard, Society of Automotive Engineers, January 2004
f. JA1003, Software Reliability Program Implementation Guide, Society of Automotive Engineers, January 2004
g. JA1004, Software Supportability Program Standard, Society of Automotive Engineers, January 2004
h. JA1005, Software Supportability Program Implementation Guide, Society of Automotive Engineers, January 2004
i. JA1006, Software Supportability Program Implementation Guide Concept, Society of Automotive Engineers, January 2004
j. Joint Software System Safety Committee, "Software System Safety Handbook," U.S. Department of Defense, December 1999

A.3. Sandia Corporate and Nuclear Weapons Complex Requirements and Guidance

a. CG100.5, "Corporate Process: Ensure Quality"
b. IM100.2.6 Control PII
c. IM100.3, "Corporate Process: Create, Maintain, and Evaluate Information Technology Resources and Services"
d. IM100.3.5, "Provide Quality Software"
e. IM100.3.5, "Provide Quality Software," Corporate Procedure, Sandia National Laboratories
f. TBP-306, "Software Product Processes," Nuclear Weapons Complex Technical Business Practice, Issue E, Sandia National Laboratories, May 2, 2003
g. DG10235, "Software Product Processes, Design Guide," Issue B, February 2005
h. RPP-113 Software Product Engineering and Qualification,Sandia Realize Product Procedure
i. SAND2004-3142, "Concepts for Tester Software Qualification," July 2004.
j. SS-R89224, Specific Use Specification, Safety Software Inventory Matrix, Sandia National Laboratories
k. SS-R94286, Specific Use Specification, Self-Assessment Instrument for Software Quality
l. SS-R94287, Specific Use Specification, Sandia Safety Software Training Program, Sandia National Laboratories