Software Dedication Using the ASME NQA-1 Approach

3rd NRC Workshop on Vendor Oversight for New Reactor Construction - June 28, 2012 Baltimore, Maryland

Presented by

Norman (Norm) P. Moreau
Principal Consultant
Theseus Professional Services, LLC
nmoreau@theseuspro.com
http://www.theseuspro.com
410-857-0023

THESEUS PROFESSIONAL SERVICES

Topics Covered

- Agree on Software Terms and Uses
- ASME NQA-1 Requirements and Guidance for Software Dedication
- Sample CGD Plan Form
- Sample CGD Plan Detailed Review

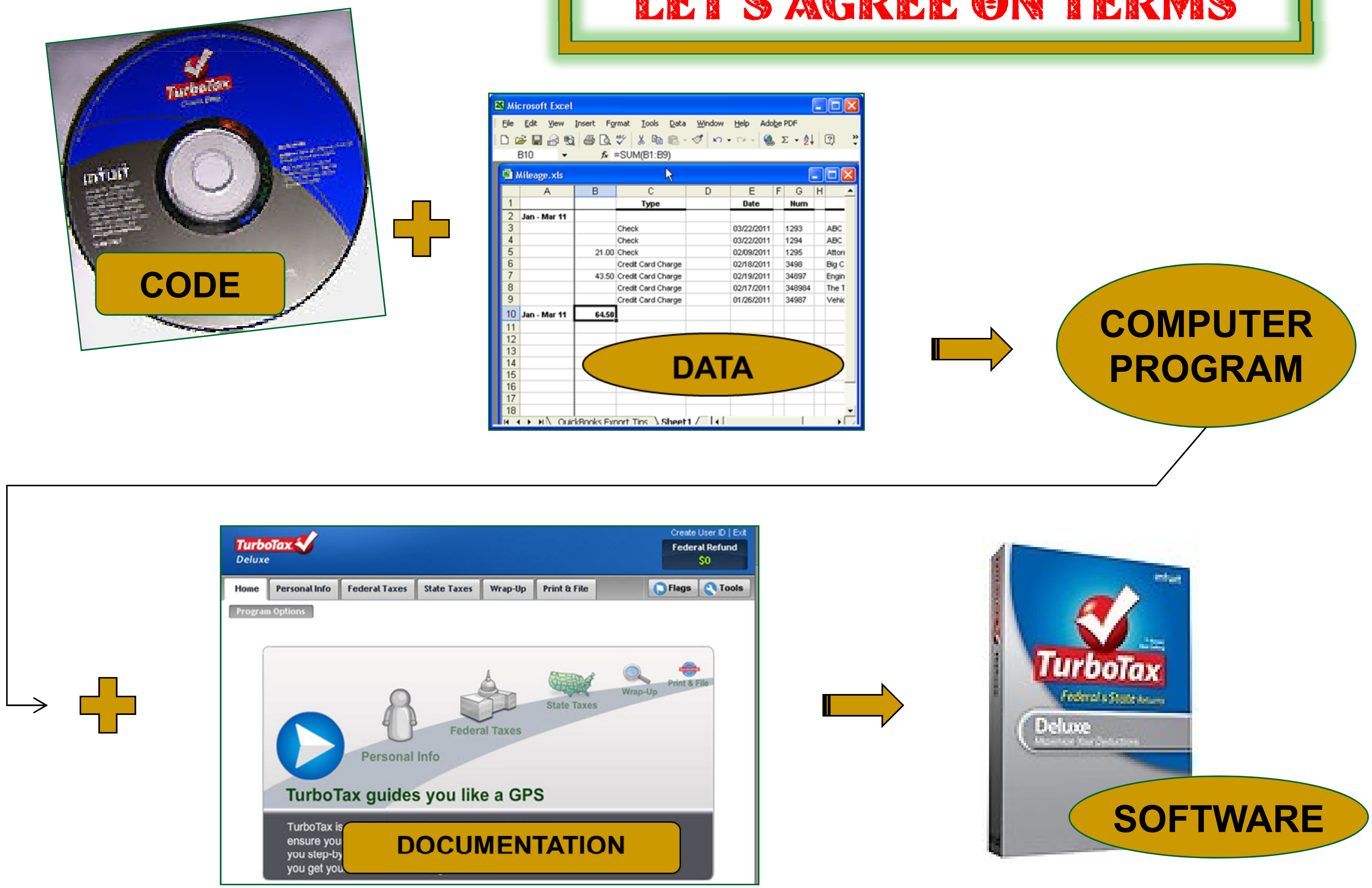
Disclaimer and Thanks

- The views expressed by the speaker do not represent the views or positions of the ASME NQA-1 Committee, the NRC or EPRI.
- They are the views of the speaker only

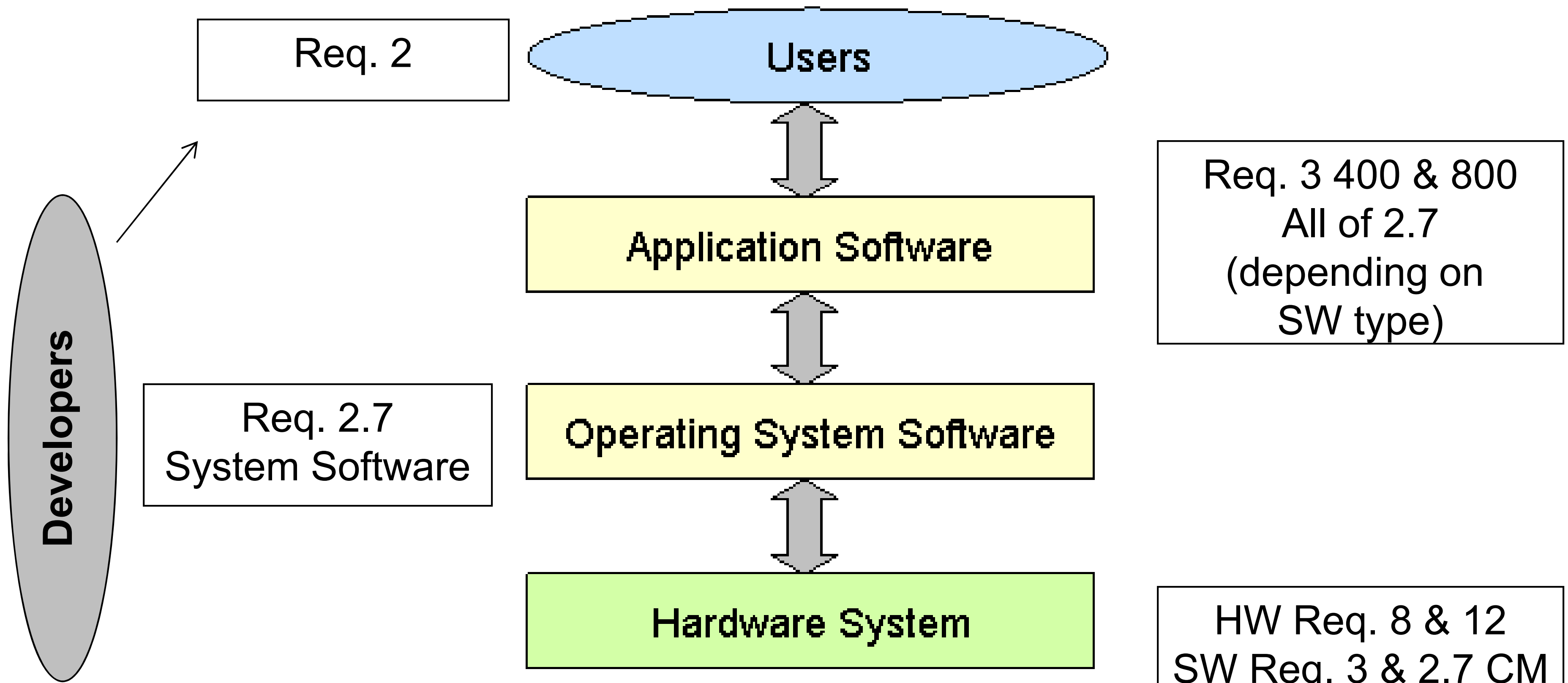
- Josh Kolenc, VP Software Engineering Curtiss Wright Flow Control Corp. (Farris Engineering Services)

  http://fes.cwfc.com/Solutions/spokes/iPRSM.htm
- Ronald C. Schrotke, Chief Technical Authority, Quality Pacific Northwest National Laboratory, ronald.schrotke@pnnl.gov

LET'S AGREE ON TERMS



Where Do Computer Programs Reside & What Part of NQA-1 Applies?



Software Used in the Nuclear Industry

Use:	Design Analysis (Design & Analysis)	Process Control (Digital I&C)	Operations (Mgmt. & Admin)
Ex:	FEA, Code Calc, Structural, Geotechnical, Seismic, Dispersion…	PLC, EPROM, Instrumentation, HMI…	ERP, MRP, e-P&ID, CMMS, e-Doc/e-Record Control Systems…

Most software today is very much like an Egyptian pyramid with millions of bricks piled on top of each other, with no structural integrity, but just done by brute force and thousands of slaves.
Alan Kay

Software Dedication - Requirements

- Changes from NQA-1-2008 to NQA-1a-2009 Part II, Subpart (SP) 2.7 Section 302
  - Requires application of Part I, Requirement 7, Control of Purchased Items and Services and Part II Subpart 2.14, Quality Assurance Requirements for Commercial Grade Items and Services
    - For acquisition of software that has not been previously approved under a program consistent with NQA-1 for use in its intended application.
  - Changes from an evaluation (IAW Subpart 2.7) to a dedication process
  - Eliminates exceptions from the process
  - Includes the identification of Critical Characteristics

Changes in 2009 Addendum

302 Otherwise Acquired Software [NQA-1a-2009]

Part I, Requirement 7, and Part II, Subpart 2.14, Quality Assurance Requirements for Commercial Grade Items and Services, shall be applied to the acquisition software that has not been previously approved under a program consistent with this Standard for use in its intended application (e.g., freeware, shareware, procured commercial off-the-shelf, or otherwise acquired software). The **acquired** software shall be identified and controlled during the dedication process.

The **dedication process** shall be documented and include the following:

(a) **identification of the** capabilities and limitations for intended use **as critical characteristics**

(b) **utilization of** test plans and test cases **as the method of acceptance** to demonstrate the capabilities within the limitations

(c) instructions for use **(e.g., user manual)** within the limits of the **dedicated** capabilities

The **dedication process** shall be documented and the performance of the actions necessary to accept the software shall be reviewed and approved. The resulting documentation and associated computer program(s) shall establish the current baseline.

Subsequent revisions of **accepted** software received from organizations not required to follow this Subpart shall be **dedicated** in accordance with this section.

Software Dedication - Requirements

- NQA-1a-2009 Part II, Subpart 2.14
  - Provides amplified requirements to provide reasonable assurance that a commercial grade item or service will perform its **safety function**.
    - Commercial Grade Item (3 definitions)
      - Nuclear Power Plants
      - Nuclear Facilities Other than Nuclear Power Plants
      - DOE Nuclear Facilities:
        - A structure, system, or component or part thereof, that affects its safety function, that was not designed and manufactured in accordance with the requirements of this Standard.
        - Includes Process Control Systems
    - Application in the context of SP 2.7 includes ALL software (e.g. Operational Control, Design and Analysis, Databases)

Software Dedication - Requirements

- NQA-1a-2009 Part II, Subpart 2.14
  - Technical Evaluation
    - Determine Safety Function
    - Identify Performance Requirements
    - Identify Critical Characteristics
    - Identify Dedication Method
      1. Special Tests, Inspections, and/or Analyses
      2. Commercial Grade Survey of the Supplier
      3. Source Verification
      4. Acceptable Supplier Item or Service Performance Record
    - Determine if replacement is like-for-like or equivalent

Guidance for Dedication of Software

- NQA-1-2012 Non-Mandatory Appendix (NMA)
  - Focused on dedication of Design and Analysis Computer Programs
  - Aligns with each of the Sections of SP 2.14 and provides information where the SP cannot be clearly interpreted as it applies to computer programs
    - Unique Definitions that apply to computer programs
    - Limits application of *Like-for-Like*
    - Omits *Equivalency* unless complete evaluation is possible.
    - Critical Characteristics derived from DOE Guidance document
      - Also adopted, in part, by the EPRI CGD Guidance

Guidance for Dedication of Software

- 4 Categories of Critical Characteristics
  - Identification
    - i.e., version, build date, release name, or part or catalog number
  - Physical
    - physical media (e.g., CD, tapes, downloads, or remote access)
  - Performance/Functional
    - required functionality of the computer program to perform its safety function and the accuracy of its results
  - Dependability (unique to computer programs)
    - Evaluation to develop judgment regarding built-in quality
    - Includes attributes related to the supplier's software development process such as
      - review of the computer program's lifecycle processes and output documentation,
      - review of configuration management activities, testing and V&V activities, and other activities
    - Included in EPRI's TR 106439 as it relates to embedded computer programs
- Table in NMA Guidance includes Critical Characteristics with Acceptance Criteria and Method for each

Guidance for Dedication of Software

- NQA-1-2012 Non-Mandatory Appendix (NMA)
  - Status
    - Approval by the Board on Nuclear Codes and Standards (BNCS)
      - December 2011
    - Mark-up reviewed by NQA-1 Committee
    - Back to editors for publication version

Guidance for Dedication of Software

- Scope Comparison
  - NQA-1
    - Focused on dedication of design and analysis computer programs
  - DOE Environmental Management
    - 80% of content focused on general CGD
    - 20% related to computer programs
  - EPRI
    - Focused on computer programs
    - Includes classification of computer programs into categories
    - Discusses design and analysis, operations, databases, etc.
    - Goes beyond dedication and discusses augmented quality

Commercial Grade Dedication Plan for XYZ Computer Program

This plan was developed to comply with requirements of ASME NQA-1a-2009, Part II, Subpart 2.14

1. TECHNICAL EVALUATION

1.1. COMMERCIAL GRADE ITEM INFORMATION

Computer Program Name.	**Version Identifier.**
Operating System Hardware.	**Operating System Software and Version.**

Part Description:

End use description: (denote if this CGI is for more than one application)

Supplier:

Interfaces:

1.

1.2 SAFETY CLASSIFICATION

1. Is this item designated as Safety-Related? [ ]
2. Is this item designated as Augmented Quality? [ ]
3. Other (specify)? Safety Design and Analysis Software [X]

1.3 COMMERCIAL GRADE ITEM DETERMINATION

Is the item a structure, system or component (safety-related/augmented quality), part thereof, that was not designed and manufactured by an ASME NQA-1 qualified supplier?

Yes [X] (Continue to Section 1.4) No [ ] (The item does not need CGD)

Note: If No, verify if the need for CGD is required to support implementation of ASME NQA-1 for a non-safety related item or service.

Non-safety related driver (specify) ____[ ]

1.4 LIKE-FOR-LIKE REPLACEMENT ITEM

The design of the replacement item is identical to the existing item [ ] Yes [X] No [ ] NA (proceed to 1.6)

1. If "Yes" with a high level of confidence, than no further Technical Evaluation is required and dedication/acceptance shall be performed in accordance with the previously approved CGD Plan for the item. Previously approved Plan – CGI Plan Ref. No.___________________________
2. If "Yes" with a low level of confidence based on review of criteria in Section 2.1, the degree of technical evaluation needs to be established and completed by development of the plan.
3. If "No" and a replacement item continue with Section 1.5.

1.5 EQUIVALENT REPLACEMENT ITEM

Are there changes in design, material, manufacturing process, form, fit, or function that could prevent the replacement item from being interchangeable under the design condition of the original items and performing its required safety function? (ASME NQA-1a-2009, Part II, Subpart 2.14, Section 403) [ ] Yes [X] No

If Yes, then the replacement item is not equivalent and must be rejected or processed as a design change in accordance with ASME NQA-1, Part 1, Requirement 3, Section 600.

If No, than selection and verification of the identified critical characteristics by an appropriate dedication method(s) is required in accordance with this plan.

1.10 FAILURE MODES (See 5. Failure Mode Determination Worksheet Pg 5)	
Part/Component Functional Mode Primary Safety Function [ ] Active [ ] Passive Secondary Safety Function [ ] Active [ ] Passive	Active - Mechanical or Electrical change of state is required to occur for the component to perform its safety function Passive – Change of state is not required for the component to perform its safety function
Host Assembly/System safety Function (as applicable) N/A	
Credible Failure mode(s) and Effect on Safety Function (see page 5, use attachments or references as required) 1. Software aborts prior to successful completion. The analysis results are not available. Conditions causing abort needs to be resolved or other software must be used for analysis. 2. Software fails to execute correct calculational routines. The results from the software are not accurate and may not be detected as being incorrect. 3. Software fails to output correct results from calculational routines. The results from the software are not accurate and may not be detected as being incorrect.	

1.11 ENVIRONMENTAL & NATURAL PHENOMENA EVALUATION	
Environmental Qualification Required [ ] Yes [ ] No	If yes: Environmental Qualification Requirements Limiting Environmental Conditions: Required Safety Functions: Qualification Period:
Natural Phenomena Hazard (NPH) Design Required [ ] Yes [ ] No	If yes: NPH Design Requirements Performance Category: NPH Design Requirements: Required Safety Functions:

iPRSM® Intelligent Pressure Relief System Management Solution

- iPRSM is an engineering application for the <u>design, audit and documentation</u> of both new and existing pressure relief systems.
- Supports the validation of ongoing <u>compliance</u> with standards such as API, ASME, ISO, OSHA as well as internal company standards.
- Functions as a centralized <u>document repository</u> for all data related to pressure relief systems, including process, plant, design, equipment, inspection, maintenance and historic data.
- *Classification? Safety-Related, Augmented Quality, or Non-Safety Related?*

CGI Information

Computer Program Name	Revision Identifier
iPRSM	v1.1.6.12

Operating System Hardware	Operating System Software and Version
Any *x86/x64* architecture based computer system.	Any *x* 86/ *x* 64 architecture system that is able to support Perl and Linux virtual machines.

Part Description
iPRSM is an engineering application for the design, audit, evaluation, and management of pressure relief systems.

Configuration Description
iPRSM requires three external software applications as infrastructure components:

- Perl programming language (requires >= v5.10)
- Apache web server (requires >= v2.2)
- VMG Thermo (requires >= v5)

End Use Description
iPRSM is used in the audit and design of pressure safety systems, not the actual operation of the plant. The application requires that the user has appropriate engineering knowledge.

Interfaces
iPRSM interfaces three external software applications. Although the software is treated as single application, the following software components are required:

- Physical properties thermal package,
- Mail system,
- Spreadsheet import/export.

Safety Function Performed

4.5 Safety Function Performed

[ASME NQA-1a-2009, Part II, Subpart 2.14, Paragraph 401(a)]

iPRSM's safety function is to support the engineering (design, audit, evaluation) of pressure relief systems essential to the safe operation of a nuclear plant.

4.5.1 Effect on Assembly/System Safety Function

Refer to Section 4.8.2.

4.5.2 Safety Function References

- J. Kolenc, H. J. Hoover, A. G. Olekshy, and P. M. Sanders, *System And Method For Protection System Design Support,* U.S. Patent 7565215, Issued July 17, 2009.
- J. Kolenc, H. J. Hoover, A. G. Olekshy, and P. M. Sanders, *System And Method For Protection System Design Support,* U.S. Patent 7617013, Issued November 10, 2009.
- H. J. Hoover, A. G. Olekshy, G. Froehlich, and P. Sorenson, *Developing Engineered Product Support Applications,* In Proceedings of the 1st Software Product Line Conference, pgs 451-476, 2000.
- G. Froenlich, H. J. Hoover, and P. Sorenson, *Realizing Requirements in Product Line Development*
- *using O-O Frameworks,* Volume 6, Number 2, 1999.
- ASME Sec I- 2010 Edition, 2011 Addendum.
- ASME Sec III, Division 1- 2010 Edition, 2011 Addendum.
- ASME Sec VIII, Division 1- 2010 Edition, 2011 Addendum.
- API-520 P1 - Revision / Edition: 8 - Sizing, Selection, and Installation Of Pressure-Relieving
- Devices In Refineries - Part 1 - Sizing And Selection.
- API RP 520- Part 2 Revision / Edition: 5 - Sizing, Selection, and Installation Of Pressure-Relieving
- Devices In Refineries - Part 2 - Installation.
- API Std 521/ISO-23251 - Fifth Edition - Pressure-Relieving and Depressuring Systems.
- Crane - Flow of Fluids - Technical Paper 410.
- AICHE - Guidelines for Pressure Relief and Effluent Handling Systems.

Performance Requirements

- Evaluate (audit) pressure relief scenarios so as to verify their compliance with standards.
- The following points outline how this is performed by iPRSM:
  - Orifice area calculations as per ASME and API.
  - Piping loss calculations as per Crane, DIERS, and multiple valves.
  - Manufacturers valve data, catalogues, and handbooks. The values for the consistency checks required for valve trim is taken from these sources.

Creditable FMEA

4.8.1 Part/Component Functional Mode

iPRSM is neither an active (i.e., mechanical or electrical change of state is required to occur for the component to perform its safety function) or passive (i.e., state is not required for the component to perform its safety function) computer program. Neither is iPRSM plant equipment. iPRSM is pressure relief systems management software that ensures that plants operate under the protection of safe pressure relief systems at all times, but it does not operate or cause any operation of the plant or facility. For these reasons this element is not applicable to iPRSM, since it is not part of a component.

4.8.2 Credible Failure Mode(s) and Effect on Safety Function

The item is used for the design and analysis of pressure relief systems, and requires the user to follow RAGAGEP and the ability to make sound engineering decisions. The following failures would result in a pressure relief system that may be inadequate:

1. Missed workflow steps;
2. Erroneous data;
3. Incomplete data;
4. Wrong math.

However, the final implication on safety is based on a final engineering review and acceptance.
The infrastructure components could affect the functionality of this item. The control of these components is outside the scope of this dedication process. Regardless, the acceptance of the work completed by this item is based on final engineering review and acceptance.

Critical Characteristics & Acceptance Method

Table 3: Identification of Critical Characteristics

#	Critical Characteristic	Acceptance Criteria	Acceptance Method
CC1	Host computer operating environment Identifiers	The host computer environment identifiers must match the purchase specification.	Inspection of the operating system identifiers. *(Method 1)*
CC2	Computer program name and version Identifier	Computer program name and version identifier must match the identifier in the vendor product list.	Inspection of iPRSM's version identifiers. *(Method 1)*
CC3	Support tools name(s) and identifier(s)	The support tool name and identifier must match the product identifier from the specification.	Inspection of the support tool(s) and identifier(s). *(Method 1)*

Table 4: Physical Critical Characteristics

#	Critical Characteristic	Acceptance Criteria	Acceptance Method
CC4	Lifecycle Documentation	The iPRSM lifecycle documentation is contained within: iPRSM-Design mailing list, iPRSM Tasks Queue, iPRSM Handbook, iPRSM source code, iPRSM-related patents, and published academic research papers.	Inspection of lifecycle documents. *(Method 1 & Method 2)*

Table 5: Performance/Functional Critical Characteristics

#	Critical Characteristic	Acceptance Criteria	Acceptance Method
CC5	Accuracy/ Precision/ Tolerance Outputs	**Accuracy:** *not critical* as iPRSM can display any value (up to IEEE standard for Double precision[IEEE-754]). **Precision:** IEEE standard for Double precision. A table of the basis conversions used in iPRSM is contained in the support material for this critical characteristic. **Tolerance:** *Not applicable to this item.*	Inspection and testing. *(Method 1)*

Critical Characteristics & Acceptance Method

Table 5: Performance/Functional Critical Characteristics – *Continued from previous page*

#	Critical Characteristic	Acceptance Criteria	Acceptance Method
CC 6	Environmental Compatibility: Portability	The effort to migrate the computer program to a different program is insignificant provided that a new platform satisfies the requirements of critical characteristic 1.	*This is not applicable to this item as discussed in the acceptance criteria*
CC 7	Functionality: Completeness & Correctness	The completeness of iPRSM is evaluated against ISO 23251 Section 4 Causes for overpressure. Refer to Section 4.6. The functionality correctness critical characteristics for iPRSM are its math and its workflow. The math correctness is based on the methods outlined in Section 4.6. The workflow, as outlined in Figure 2, will fail safe such that it cannot proceed without preconditions being met.	Inspection and testing. *(Method 1)*
CC 8	Functionality: Consistency with appropriate engineering, scientific research, & professional technical approaches	This item is based on RAGAGEP. Refer to Section 4.6.	Inspection and testing. *(Method 1)*

Critical Characteristics & Acceptance Method

Table 6: Dependability Critical Characteristics

#	Critical Characteristic	Acceptance Criteria	Acceptance Method
CC13	Built-in Quality: Adherence to coding practices	Although no formal QA Program was used during the development of iPRSM, the informal Process QA (at time of this CGD document) are listed in Appendix A.	The development team for iPRSM has no documented coding standard, but the process of accepting new code is outlined in Appendix A. A description of an accepted coding standard for iPRSM is being developed as part of the QA Manual. *(Method 2)*
CC14	Built-in Quality: Code Structure (complexity, conciseness)	PRSM is built using the Prothos framework. This framework enforces a specific modularization and complexity decomposition on the implementation of iPRSM. The design is based upon the experience the development team gained from developing a similar product. The Prothos framework and its development has been published in a number of academic publications.	Review of the architecture diagram and the associated academic publications that describe the Prothos framework. *(Method 1)*
CC15	Built-in Quality: Conformance to national codes, standards, and industry-accepted certifications	iPRSM is not implemented to satisfy any industry-accepted certifications, national codes, or standards.	*Not applicable to this item as described in the acceptance criteria.*

Critical Characteristics & Acceptance Method

Table 6: Dependability Critical Characteristics – *Continued from previous page*

#	Critical Characteristic	Acceptance Criteria	Acceptance Method
CC17	Built-in Quality: Internal reviews & verifications	In the absence of a formal QA Program, the development team does not have a documented internal review and verification process. Informally, the process is described in Appendix A.	Review the procedures outlined in Appendix A. A more formalized process is being developed as part of the QA Manual as part of this acceptance process. *(Method 2)*
CC18	Built-in Quality: Testability & thoroughness of testing	iPRSM testing is currently ad hoc. iPRSM contains the ability to conduct impact analysis testing, but a more comprehensive set of test suites is needed. Also, testing of iPRSM's workflow is challenging, and it is tested in an ad hoc fashion by the development team.	A set of formal testing procedures are being developed as part of the QA Manual. *(Method 2)*
CC19	Built-in Quality: Training, knowledge, and proficiency of personnel performing the work	All of the core developers have graduate degrees in Computing Science and they each have more than 20 years of software engineering experience.	The acceptance criteria for this item will be based on a review of the resumé(s) of the development team attesting to their education and experience in software development. *(Method 1)*
CC20	Problem Reporting: Notifications to Customers	Problem reported to customers is captured in the item's mailing list and tasks queue. Communications to customers is handled by the engineering team. Release notes listing changes available online through iPRSM when a user logs into the system.	A more complete communication interface for customers is included as part of the QA Manual. The existing communication is included for inspection(Method *2)*
CC21	Supportability/ Maintainability	iPRSM has been used in support of petrochemical industry for the past 10 years.	Verified by review of the supplier history for iPRSM usage within the petrochemical industry - which is the same computer application, just not processed through the CGD process. *(Method 4)*

Conclusions

- The challenge will be determining <u>when and when not</u> to apply the dedication process to a computer program – Classification and Grading.
- In many cases the dedication can be packaged around <u>existing V&V</u> packages.
- The more <u>complex</u> the computer program, the more comprehensive the dedication will have to be.
- Performance <u>history</u> has to play a role.

Questions or More Information?

Contact Information

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

Nancy M. Kyle
Principal Consultant
Theseus Professional Services, LLC
nancy5895@gmail.com
http://www.theseuspro.com
706-830-3194

If you want to consider participation in ASME NQA-1 Committee activities visit
http://cstools.asme.org/csconnect/CommitteePages.cfm?Committee=O10500000

For an ASME Short Course on NQA-1 Requirements for Computer Software Used in Nuclear Facilities visit
http://catalog.asme.org/Education/ShortCourse/NQA1_Requirements_Computer.cfm

For training specifically on the Commercial Grade Dedication of Software visit
http://theseuspro.com/training_services.php

Reference

- ASME NQA-1 several editions and addendum, *Quality Assurance Requirements for Nuclear Facility Application*. ASME New York
- EPRI, *Generic Qualification/Dedication of Digital Components Screening of Candidate Components* 1006842 EPRI Project Manager R. Torok, December 2002
- EPRI, *Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications* TR-106439 EPRI Project Manager R. C. Torok October 1996
- EPRI, *Evaluating Commercial Digital Equipment for High Integrity Applications A Supplement to EPRI Report TR-106439 TR-107339* Final Report, December 1997 Principal Investigators B. Fink and J. Betlack Project Manager Ray Torok, December 1997
- EPRI, NP-5652, *Utilization of Commercial Grade Items in Nuclear Safety Related Applications,* 1988
- Farris Engineering Services, *iPRSM Commercial Grade Dedication Plan*, Draft Rev. 1.502
- Moreau, NP, Schrotke, RC, Subir, S, *Applying ASME NQA-1 Requirements for Computer Software Used in Nuclear Facilities,* ICONE 18, May 17–21, 2010 Xi'an, China
- NRC, *Review of TRICONEX Corporation Topical Reports 7286-545, "Qualification Summary Report" and 7286-546, "Amendment 1 TO Qualification Summary Report," Revision 1 (TAC NO. MA8283),* December 2001 http://adamswebsearch2.nrc.gov/idmws/doccontent.dll?library=PU_ADAMS^PBNTAD01&ID=004042634
- NRC, 10 CFR Part 21, *Reporting of Defects and Noncompliance,*1992