U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Public Meeting to Discuss the Revision to NUREG-1537

Leroy A. Hardin
U.S. Nuclear Regulatory Commission, Office of Research

Al Adams, Jr. Duane A. Hardesty
U.S. Nuclear Regulatory Commission, Office of Nuclear Reactor Regulation

Roger A. Kisner Michael D. Muhlheim, Ph. D
Oak Ridge National Laboratory

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Purpose

- To discuss
  - the revision to NUREG-1537,
  - concepts for graded, risk-informed evaluations of RTR systems, and
  - to facilitate discussion of other issues related to this revision that affects the RTR community.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Agenda for Public Meeting
June 23, 2011

Time	Topic	Led By
01:00 – 01:05	Opening Remarks	NRC
01:05 – 03:00	NUREG-1537 Revision Process	NRC
03:00 – 03:30	Decision Points Discussion	NRC
03:30 – 03:50	Invitation for Public Participation	NRC
03:50 – 04:00	Conclusion/Document Actions	NRC

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

NUREG-1537 Revision Process

- Review the objectives for revising NUREG-1537
- Review the digital upgrades in the 1990's (historical perspective)
- Assess the similarities and differences between ANSI/ANS 15.15-1978 (withdrawn) vs. IEEE Std 603-1991
- Identify the similarities and differences between guidance for RTRs and NPPs (i.e., NUREG-1537 vs. NUREG-0800)
- Evaluate the applicability of those differences to RTRs
- Prepare a draft to NUREG-1537, Part 2
- Hold public workshops on the methodology, applicability, and draft report

Objective—To Update and Enhance the Available Guidance on Reviewing Digital I&C Systems for RTRs

- NRC's objective,
  - because non-power reactor licensees have expressed interest in upgrading their existing I&C systems with digital systems, the guidance for implementing these changes requires NUREG-1537, Part 2 to be updated,
  - the currently available guidance for RTRs will be used to provide an initial foundation,
  - because the guidance in licensing digital I&C systems at NPPs cannot just be adopted for RTRs, applicable information and guidance will be adapted and used to leverage the experience gained in licensing digital I&C at NPPs, and
  - areas that are not specifically addressed or are unique to RTRs will be covered by the new enhancements developed in this effort.

- While new requirements, Regulatory Guides (RGs), Interim Staff Guidance (ISG), and industry standards have been or are being developed for licensing digital I&C systems for NPPs, this guidance was not developed for RTRs.
  - these new requirements for NPPs, which have evolved since 1996, contain sections and requirements that do not apply to RTRs, and
  - there are issues unique to RTRs such as varied power level and diverse design features that will require a more graded, risk-informed approach.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

The Two Reviews in the 1990's of Digital Upgrades for RTRs Focused on the Same Topics as that for NPPs While Recognizing the Differences

- To assess hardware and systems the staff considered the following:
  - environmental qualification to determine if temperature or humidity would adversely affect the equipment;
  - seismic qualification of equipment to determine if relay contact chatter could prevent a scram;
  - electromagnetic interference to determine if it could prevent a scram;
  - the effect on the system if a power supply fails or is subjected to line fluctuations;
  - failure modes to determine the probability of failure to scram;
  - independence, redundancy, and diversity of the system; and
  - the testing and operating history of the system.

- To assess software, the staff reviewed the V&V plan by considering the following:
  - the independence of the software verifier from the designer,
  - the functional description of the software and the validation testing performed,
  - the process by which the developer corrected development discrepancies,
  - the design approach to develop software specifications that are reliable and testable,
  - a step- by- step software development plan, and
  - a task analysis for the design of the operator interface.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

History of Digital Upgrades in RTRs

*****GA Console for GA TRIGA Reactor*****
*****Penn State Breazeale Reactor*****

Hardware

- ANSI/ANS 15.15-1978
  - Environment
  - Seismic
  - EMI
  - Power supplies
  - FMEA
  - Independence
  - Redundancy
  - Diversity
- Hardwired scram circuit

Software

- IEEE Std 7-4.3.2-1982 (Intent)
  - Software development (software quality metrics)
  - V&V and Independent V&V
  - Configuration management
- Not covered
  - Qualification of existing commercial computers
  - Use of software tools
  - Risk Management

GA Console Review

Differences between NPP and RTR requirements

- The safety channels provide inputs to the Non-Class 1E Data Acquisition Computer (DAC) through isolators. The isolators used have not been tested for maximum credible faults which the staff requires for power plant use, but have been tested by the manufacturer to standard commercial criteria.

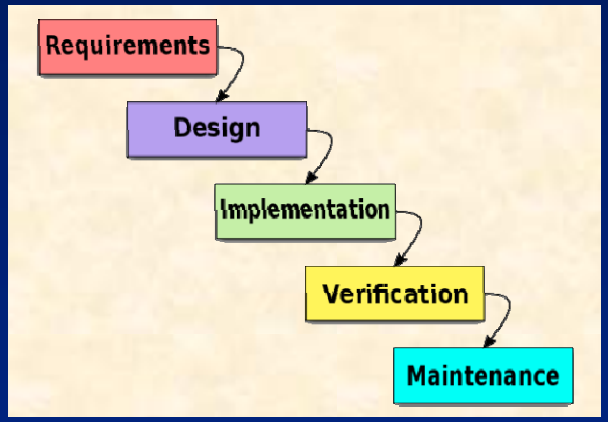
- The DAC is then connected via redundant high speed serial data trunks to the Non-Class 1E Control System Computer (CSC) which interfaces with the operator by controls, a keyboard, and CRT displays. Because the non-safety CSC communicates with the safety channels, this bi-directional communication between a safety system and a non-safety system would not meet the independence requirements of an NPP. The staff concluded that requiring mono-directional communication was not necessary for the current application of the GA Console.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

GA Console Review (continued)

Noted deficiencies (corrected prior to approval)

- Documentation was found to be lacking in several areas with the most significant being the lack of a functional requirements specification.
- A step-by-step plan, such as described in IEEE Std 7-4.3.2, was not developed for the software.
- There was not a formal task analysis to support the design of the operator interface; the initial specifications and descriptions were vague.



U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Penn State Breazeale Reactor Review

- Conclusion of review was a 10 CFR 50.59-type conclusion
  - no significant increase in the probability or consequences of accidents previously evaluated,
  - no new or different kind of accident from any accident previously evaluated,
  - does not involve a significant reduction in the margin of safety, and
  - does not involve a significant hazards consideration.
- The conclusion in the SER is similar to one that is generated when applying for a digital system upgrade for an NPP under 10 CFR 50.59
- A difference is that in a 10 CFR 50.59 submittal today, software faults as a source of common-cause failure must be assessed (Ref. IN 2010-10).

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

The GA Console and Penn State Reviews Recognized the Level of Risk from RTRs

- Because of the specific design features of a TRIGA reactor and the requirements of the Atomic Energy Act (AEA), the reviews reflected the level of risk and the differences between NPPs and RTRs
- The reviews recognized that they were not NPP reviews and this philosophy is being maintained in the update to NUREG-1537, Part 2
  - Engineering judgment was used in the reviews because the fuel could not be damaged (i.e., the TRIGAs did not need to meet the requirements for NPPs)
  - The update to NUREG-1537 in 1996 captured what was done in the reviews

The Update to NUREG-1537 Must Account for the Differences Between NPPs and RTRs

- All reactors (power and non-power) are licensed under Title 10 of the Code of Federal Regulations and in accordance with the Atomic Energy Act of 1954, as amended. The Atomic Energy Act states that utilization facilities for research and development should be regulated to the minimum extent consistent with protecting the health and safety of the public.

- Some understanding of their design, risk, and regulatory differences is necessary to properly adapt regulations and experience from NPPs to RTRs.
  - The licensed thermal power levels of RTRs are several orders of magnitude lower than NPPs. In addition, the generally intermittent operation of RTRs results in a significantly smaller inventory of fission products in the fuel.
  - The lower power RTRs also have less tendency to melt following a LOCA or core uncovery—in many non-power reactors, the decay heat is insufficient to cause cladding damage under any cooling condition.
  - TRIGA-type RTRs have an inherent reactivity insertion safety feature in their design and generate minimal decay heat that precludes damage to the fuel.

- Overall, the public risk associated with RTRs is much less than that of NPPs. These factors have been some of the bases upon which the NRC has determined that less stringent and less prescriptive measures are required to adequately protect the safety of the public, workers, and the environment. (ML003706367).

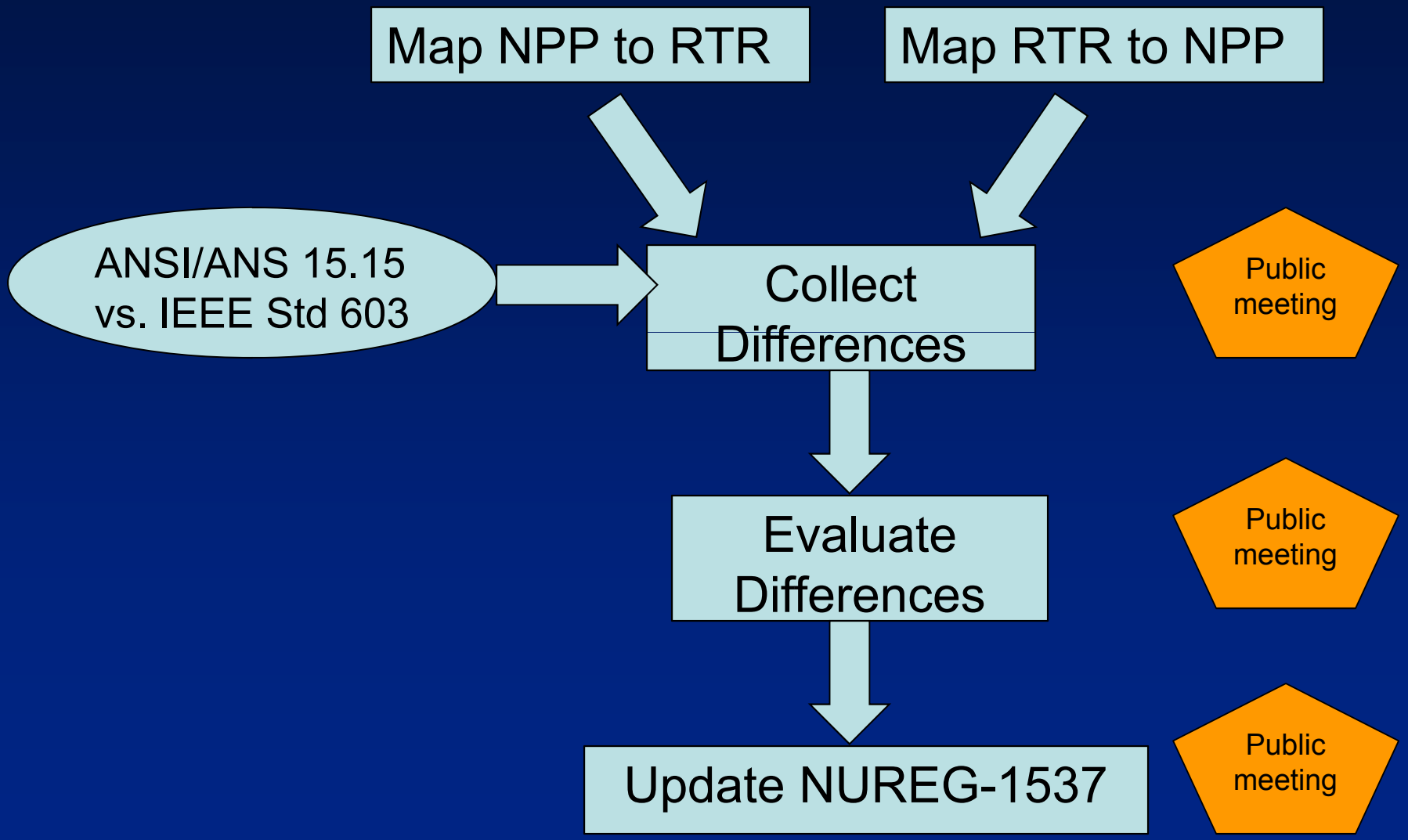
U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Updating NUREG-1537 Will Remove the Regulatory UncertaintyAssociated With Upgrading an I&C System at RTRs

- Why update NUREG-1537?
  - The guidance references have all been superseded
  - More types of reactors (beyond TRIGAs) are looking to update to digital I&C systems
- How will the NUREG be updated?
  - The current format in NUREG-1537 will be maintained
  - Standards will be used as references for additional information

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

A Structured Process Will be Used to Identify and Evaluate Differences



Identifying the Differences Between the Guidance and Standards for Digital I&C in NPPs and RTRs and Evaluating the Applicability of those differences to RTRs will be Used to Update NUREG-1537, Part 2

Difference → Difference Resolution → Draft NUREG

- RTR
  - ANSI/ANS 15.15 (guidance)
  - RG 1.152, Rev. 1
  - IEEE Std 7-4.3.2-1993
  - GL 95-02
  - ANSI/ANS 10.4-1987
  - Specific acceptance criteria

⟺ ⟺ ⟺

- NPP
  - IEEE Std 603-1991 (required)
  - RG 1.152, Rev. 2
  - IEEE Std 7-4.3.2-2003
  - GL 95-02
  - IEEE/EIA 12207.0-1996
  - ISGs
  - BTPs, RGs, and SECYs

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

The Recent Reviews of Digital Upgrades Followed ANSI/ANS 15.15-1978. Should Future Reviews Follow IEEE Std 603?

- The primary review criteria for the hardware for digital upgrades was ANSI/ANS 15.15-1978, which has been withdrawn
- The primary review criteria for the software for digital upgrades was IEEE Std 7-4.3.2, which requires the application of IEEE Std 603
- ANSI/ANS 15.15-1978 is similar to IEEE Std 603-1991 in form and function
- A comparison between ANSI/ANS 15.15-1978 and IEEE Std 603-1991 was made to answer this question
- Prior to the publication of a revised NUREG-1537, IEEE Std 603-2009 will be reviewed for differences and applicability of those differences

ANSI/ANS-15.15-1978(R1988) (discontinued)	IEEE Std 603-1991	IEEE Std 7-4.3.2-2003 additional requirements
5.1 Single Failure 5.1.1 Statement of the Criterion: The reactor safety system (RSS) design shall provide a level of reliability and redundancy such that the RSS can, as a minimum, perform the required protective actions in the presence of any single failure within the RSS concurrent with: (1) the occurrence of all failures caused by the single failure and (2) all failures caused by the Design Basis Event. Specifically the protective actions required are: (a) those for each safety interlock. (b) the intended automatic detection of each Design Basis Event and the immediate execution of the safety shutdown of the reactor. (c) the manual execution of safety shutdown of the reactor. 5.1.2 Application: Except as provided below, the single failure criterion stated above shall be applied to the design of the RSS for each research reactor. (1) A probabilistic assessment of the RSS may be used to eliminate certain postulated failures from consideration on the basis that such failures are shown not to be credible. (2) For negligible-risk research reactors, compliance with the single failure criterion for protective actions (a) and (b) of 5.1.1 is not mandatory. (3) For pulse reactors, compliance with the single failure criterion for protective action (b) in 5.1.1 is not mandatory for those portions of the RSS which function only for reactivity excursion-type events. A pulse reactor is a reactor that has been specially designed with an inherent shutdown mechanism sufficient to allow the reactor to accept large reactivity insertions without exceeding any safety limit. (4) If trustworthy failure rate data are available, reliability analysis may be used to demonstrate that the RSS satisfies such sufficient reliability goals that exemption from compliance with the single failure criterion for protective actions (a) and (b) in 5.1.1 is justified. The minimum level of reliability considered generally acceptable for this purpose is that equivalent to 95% confidence that operation without the needed protective action for a Design Basis Event will occur no more often than once in the operating life of the research reactor and 95 % confidence that such a failure of the RSS will be detected prior to or during the startup for the next day of operation. (5) As an alternative to compliance with the single failure criterion for protective actions (a) and (b) in 5.1.1, the RSS may include methods that promptly detect unsafe failures and alert the reactor operator, provided that: (a) the composite reliability of the basic portion of the RSS and its associated fault detection method is comparable to that which would be attained by direct compliance. (b) the fault detection methods do not introduce a credible common failure mode. (c) written administrative controls are provided which include appropriate specific actions to be taken when a failure is detected.	5.1 Single-Failure Criterion. The safety systems shall perform all safety functions required for a design basis event in the presence of: (1) any single detectable failure within the safety systems concurrent with all identifiable but non-detectable failures; (2) all failures caused by the single failure; and (3) all failures and spurious system actions that cause or are caused by the design basis event requiring the safety functions. The single-failure criterion applies to the safety systems whether control is by automatic or manual means. IEEE Std 379-1988 provides guidance on the application of the single-failure criterion. This criterion does not invoke coincidence (or multiple-channel) logic within a safety group; however, the application of coincidence logic may evolve from other criteria or considerations to maximize plant availability or reliability. An evaluation has been performed and documented in other standards to show that certain fluid system failures need not be considered in the application of this criterion. The performance of a probable assessment of the safety systems may be used to demonstrate that certain postulated failures need not be considered in the application of the criterion. A probable assessment is intended to eliminate consideration of events and failures that are not credible; it shall not be used in lieu of the single-failure criterion. IEEE Std 352-1987 and IEEE Std 577-1976 provide guidance for reliability analysis. Where reasonable indication exists that a design that meets the single-failure criterion may not satisfy all the reliability requirements specified in 4.9 of the design basis, a probable assessment of the safety system shall be performed. The assessment shall not be limited to single failures. If the assessment shows that the design basis requirements are not met, design features shall be provided or corrective modifications shall be made to ensure that the system meets the specified reliability requirements.	None

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Example of Requirements in ANSI/ANS 15.15-1978 that are not in IEEE Std 603-1991

ANSI/ANS 15.15-1978	IEEE Std 603-1991
4. Design Basis. For each mode of operation of the research reactor, the design basis shall address and discuss in appropriate detail at least the following items: – (14) Beyond those normally provided, any quality assurance requirements needed to accommodate any unusual or unique aspects of the design of the Reactor Safety System (RSS). – (15) The administrative controls necessary to satisfy the requirements of this standard in conjunction with the physical features of the RSS.	Safety system requirements at NPPs must meet 10 CFR 50, Appendix B. The only administrative controls allowed are those that can be used for control of access.
5.2 Redundancy. The following types of redundancy shall be considered. To the extent advantageous and practical, the indicated order of preference shall be incorporated: – Functional diversity - monitoring different reactor variables related to the Design Basis Event. – Equipment diversity - monitoring the same reactor variable using equipment with different principles of operation. – Simple redundancy - monitoring the same reactor variable using duplicate equipment.	Although IEEE Std 603-1991 notes that "Redundancy can be accomplished by the use of identical equipment, equipment diversity, or functional diversity," this is not a requirement but a note to a definition.
5.4 Fail-Safe Design. A design objective shall be that no malfunction within the system, caused solely by the variations of external conditions within the ranges detailed in the design basis, will result in an unsafe failure. (A-5.4 Fail-Safe Design, states that for the vast majority of research reactors where auxiliary power is either minimal or not available, this should continue to be an objective in the design of the RSS.)	The single failure criterion for electric power in Clause 8.1 (IEEE Std 308) is more restrictive.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Examples of Requirements in IEEE Std 603-1991 that are not in ANSI/ANS 15.15-1978

4.11 Equipment Protective Provisions

5.4 Equipment Qualification*

5.5 System Integrity*

5.8 Information Displays

5.10 Repair

5.12 Auxiliary Features

5.13 Multi-Unit Stations

5.14 Human Factors Considerations

*Additional requirements are provided in IEEE Std 7-4.3.2

5.15 Reliability*

6.1 Automatic Control

6.3 Interaction Between the Sense and Command Features and Other Systems

6.4 Derivation of System Inputs

6.5 Capability for Testing and Calibration

7.1 Automatic Control

7.2 Manual Control

8.1 Electrical Power Sources

8.2 Non-electrical Power Sources

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Examples of Requirements in IEEE Std 603-1991 that are too Restrictive for RTRs (i.e., Fail to Meet the AEA of 1954)

ANSI/ANS 15.15-1978	IEEE Std 603-1991
<u>Quality</u> • The QA requirements for the reactor safety systems are to be satisfied through the overall quality assurances program approved for the reactor facility. Guidance is provided in ANSI/ANS 15.8; this standard does not specifically address software.	• IEEE Std 603-1991 implies an NQA-1 program – Clause 5.3 states that "Components and modules shall be of a quality that is consistent with minimum maintenance requirements and low failure rates. Safety system equipment shall be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program (ANSI/ASME NQA1-1989)." • Additional guidance for digital systems is provided in IEEE Std 7-4.3.2-2003, which states that "Hardware quality is addressed in IEEE Std 603-1998. Software quality is addressed in IEEE/EIA Std 12207.0-1996 and supporting standards."
<u>Single Failure Criterion</u> Section 5.1.2 does not require compliance with the single failure criterion in specific cases.	Clause 5.1 requires the safety systems to perform all safety functions in the presence of a single failure.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Should Future Reviews Follow IEEE Std 603?

- ANSI/ANS 15.15-1978 contains less restrictive requirements than IEEE Std 603, in keeping with the intent of the AEA
- The similarities and differences between ANSI/ANS 15.15-1978 and IEEE Std 603-1991 (and -2009) will be reviewed for applicability and appropriateness for inclusion in NUREG-1537

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

The Differences Between RTR and NPP Requirements Were Identified to take Advantage of the Maturity and Lessons Learned in Digital Upgrades at NPPs

- Two types of analyses were performed to identify the differences between the review guidance for RTRs and NPPs (i.e., NUREG-1537 and NUREG-0800)

  1. Determine what review guidance and lessons learned from NPPs can be adapted to RTRs

  2. Determine if requirements for NPPs are addressed in the review guidance for RTRs and are needed or appropriate

Determine What Review Guidance and Lessons Learned from NPPs Can be Adapted to RTRs

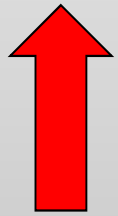
- The first difference analysis started with the currently available review guidance for RTRs as a foundation (i.e., NUREG-1537, Part 2), and determined what guidance and lessons learned for NPPs could be adapted for use at RTRs.
  - That is, the acceptance criteria for NPPs were mapped to the acceptance criteria for RTRs for comparable systems.

- Areas (topics) in NUREG-0800 are already addressed in NUREG-1537. This review is looking for differences, not making a judgment on the appropriateness of those differences (this will be done later).

NUREG-1537	NUREG-0800
7.3, Reactor Control System	7.7, Control Systems
7.4, Reactor Protection System	7.2, Reactor Trip System
7.5, Engineered Safety Features Actuation Systems	7.3, Engineered Safety Features Actuation Systems
7.6, Control Console and Display Instruments	7.5, Information Systems Important to Safety
7.7, Radiation Monitoring Systems	7.5, Information Systems Important to Safety
(addressed in NUREG-1537 section 7.4)	7.4, Safe Shutdown Systems
(addressed in NUREG-1537 section 7.4)	7.6, Interlock Systems Important to Safety
(addressed in NUREG-1537 section 7.4)	7.8, Diverse Instrumentation and Control Systems
(addressed in NUREG-1537 section 7.4)	7.9, Data Communications Systems

Example Difference Analysis for NUREG-1537, Section 7.4 (RPS) and NUREG-0800, Section 7.2 (RTS)

- The mapping was done in a tabular form to facilitate comparison between the requirements
- Similar guidance was laid side by side allowing similarities and differences to be readily apparent
- The identification of the differences were used as input for evaluating the appropriateness of those differences (i.e., our Difference Resolution phase)

NUREG-1537, Section 7.4, RPS	NUREG-0800, Section 7.2, RTS	Comments, differences in NUREG-1537, Overbearing in -0800
The automatic reactor runback or shutdown (scram) subsystem should be fail-safe against malfunction and electrical power failure should be as close to passive as can be reasonably achieved, should go to completion once initiated, and should go to completion within the time scale derived from applicable analyses in the SAR.	IEEE Std 603-1991, Section 4.2 The safety functions and corresponding protective actions of the execute features for each design basis event. IEEE Std 603-1991, Section 4.5 describes the minimum criteria under which manual initiation and control of protective actions may be allowed. Manual actuation relies on minimum equipment and, once initiated, proceeds to completion unless the operator deliberately intervenes. Failure in the automatic initiation portion of a system-level function does not prevent the manual initiation of the function. IEEE Std 603-1991, Section 4.8 The conditions having the potential for functional degradation of safety system performance and for which provisions shall be incorporated to retain the capability for performing the safety functions (for example, missiles, pipe breaks, fires, loss of ventilation, spurious operation of fire suppression systems, operator error, failure in non-safety-related systems). IEEE Std 603-1991, Section 4.10 The critical points in time or the plant conditions, after the onset of a design basis event, including: 4.10.1 The point in time or plant conditions for which the protective actions of the safety system shall be initiated. 4.10.2 The point in time or plant conditions that define the proper completion of the safety function. 4.10.3 The points in time or the plant conditions that require automatic control of protective actions. 4.10.4 The point in time or the plant conditions that allow returning a safety system to normal. IEEE Std 603-1991, Section 4.12 Any other special design basis that may be imposed on the system design (example: diversity, interlocks, regulatory agency criteria). IEEE Std 603-1991, Subsection 5.1 Single-Failure Criterion. The safety systems shall perform all safety functions required for a design basis event in the presence of: (1) any single detectable failure within the safety systems concurrent with all identifiable but non-detectable failures; (2) all failures caused by the single failure; and (3) all failures and spurious system actions that cause or	difference—partial compliance with Section 4.5. Implicit—the requirement appears to meet the intent of Section 4.10. difference—the requirement does not satisfy the diversity of Section 4.12 but does assume it is fail-safe.  **differences noted**

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Determine if the Requirements for NPPs are Addressed in the Review Guidance for RTRs

- The second difference analysis starts with the primary requirements for NPPs (i.e., NUREG-0800) and determines if these are addressed in the guidance for RTRs
  - That is, the acceptance criteria for RTRs were mapped to the acceptance criteria for NPPs for comparable systems.

NUREG-1537	NUREG-0800
7.3, Reactor Control System	7.7, Control Systems
7.4, Reactor Protection System	7.2, Reactor Trip System
7.5, Engineered Safety Features Actuation Systems	7.3, Engineered Safety Features Actuation Systems
7.6, Control Console and Display Instruments	7.5, Information Systems Important to Safety
7.7, Radiation Monitoring Systems	7.5, Information Systems Important to Safety
(addressed in NUREG-1537 section 7.4)	7.4, Safe Shutdown Systems
(addressed in NUREG-1537 section 7.4)	7.6, Interlock Systems Important to Safety
(addressed in NUREG-1537 section 7.4)	7.8, Diverse Instrumentation and Control Systems
(addressed in NUREG-1537 section 7.4)	7.9, Data Communications Systems

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Mapping the Requirements for RTRs onto those for NPPs Will Identify Potential Differences

Difference → Difference Resolution → Draft NUREG

- A table similar to Table 7-1 in NUREG-0800 was created—the GDC were replaced with the clauses in IEEE Std 603-1991. (includes RGs, BTPs, SECY 93-087)
- It was noted if the criteria were addressed for RTRs or if the differences created a difference in the requirements
- This table was compared to the previous difference analysis to ensure any potential differences were identified

	Control (7.3)	RPS (7.4)	ESFAS (7.5)	Safe S/D (---)	Interlock (---)	D3 (---)	DCS (---)	Console & display (7.6)	Rad monitor (7.7)
IEEE Std 603-1991, Section 4. Safety System Designation									
4.1, Design Basis Events	X	X	X						
4.2, Safety Functions and Corresponding Protective Actions	X	X	X						
4.3, Permissive Conditions for Each Operating Bypass Capability	diff	diff	diff						
4.4, Variables Required to be Monitored for Protective Action	X	X	X					X	
4.5, The Minimum Criteria for Each Action Controlled by Manual Means	X	diff	diff					X	
4.6, Spatially Dependent Variables	diff	diff	diff						
4.7, Range of Conditions for Safety System Performance	X	X	X						
4.8, Functional Degradation of Safety Functions	X	X	X			X			
4.9, Reliability	X	X	diff						
4.10, The Critical Points in Time or the Plant Conditions	X	X	X						
4.11, Equipment Protective Provisions	X	X	X						
4.12, Other Special Design Basis	X	diff	diff						
IEEE Std 603-1991, Section 5. Safety System Criteria									
5.1, single-failure criterion	X	X	diff	X	diff		diff		
5.2, completion of protective action	N/A*	X	Diff						
5.3, quality	diff	diff	X		diff		Diff		
5.4, equipment qualification	X	X	X	Diff			Diff		
5.5, system integrity	X	X	X	Diff					
5.6, independence	X	X	X	X	Diff	Diff	diff	X	X
5.7, capability for test and calibration	X	X	X	Diff	diff		diff	X	

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Difference Analysis for RCS shows . . .

- Combined RPS/RCS increases likelihood of RCS compromising function of RPS
  - Analog failures fail parts of a system whereas a digital RPS/RCS could fail the entire protection/control system
  - Interdependencies of digital systems are much more complex than for analog systems
  - Because of the compression of function the loss of a digital system can be more wide-spread than that of an analog system
- Need conformation that failure of RPS does not lead to greater than negligible risk
- Is the RPS/RCS susceptible to CCFs that could inhibit ability to control while also affecting ability of protection system
- Quality necessary to minimize challenges

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Difference Analysis for RPS shows . . .

- As expected, the most significant difference is in the requirements for software. NUREG-1537 identifies IEEE Std 7-4.3.2-1993 as applicable and leaves specific application to the licensees. However, IEEE Std 7-4.3.2-2003 (current version) states that it is to be used in conjunction with the following standards:
  - IEEE Std 603-1998, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations.
  - IEEE Std 1012-1998, IEEE Standard for Software Verification and Validation.
  - IEEE Std 1042-1987 (R1993), IEEE Guide to Software Configuration Management.
  - IEEE/EIA Std 12207.0-1996 IEEE/EIA Standard—Industry Implementation of International Standard ISO/IEC 12207: 1995 (ISO/IEC 12207), Standard for Information Technology—Software life cycle processes.
- It is the application of these standards that invoke criteria beyond those necessary to ensure worker and public safety at RTRs

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Difference Analysis for ESFAS shows . . .

- Very similar to RPS
- Added consideration is requirement for post-accident actuation and monitoring functionality for NPPs
  - Post accident conditions are significantly less severe for NPRs compared to NPPs

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Difference Analysis for Control Console and Display Information shows . . .

- The guidance for periodic testing is not specifically required for RTRs, only that the system be testable.
- Although NUREG-1537 states that reactor operation for RTRs should be prevented and not authorized without use of a key or combination input at the control console, the security phases of the software are not addressed. In addition, the control of access is a small part of cyber security.
- A remote shutdown panel is not required for RTRs.
- The guidance for single failure of the control console and display information is not addressed in NUREG-1537.
- The addition of Bypass and Inoperable Status Indication (BISI) panels (IEEE 603, Clauses 5.6.3 and 6.3) would impose NEW requirements on RTRs that were not present in NUREG-1537.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Difference Analysis for Radiation Monitoring Systems shows . . .

- The systems should be designed not to fail or operate in a mode that would prevent the RPS from performing its safety function, or prevent safe reactor shutdown. (IEEE Std 603-1991, Clause 4.8, 5.6.3; IEEE Std 7-4.3.2-2003, Clause 5.6) It is standard practice that a nonsafety system should not affect the operation of a safety system. Software, including software common-cause failure, should be specifically addressed because it would be new to RTRs.

- Most of the guidance provided in RG 1.97, “Criteria for Accident Monitoring Instrumentation in Nuclear Power Plants,” SRP BTP 7-10, “Guidance on the Application of RG 1.97,” and RG 1.118, “Periodic Testing of Electric Power and Protection Systems,” will be N/A for RTRs or is already addressed.

- A basis should be provided for Emergency Operating Procedures (EOP) action points that accounts for measurement uncertainties (Regulatory Guide 1.105).

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Difference Resolution: The difference Analyses Identify differences Whereas the difference Resolution Evaluates the Justification of those differences

—difference is justified => no change to requirements
—difference is not justified => add to requirements
—difference is partially justified => risk-informed

NPP review philosophy – provide a reason why this requirement does not apply to NPPs
verses
RTR review philosophy – provide a reason why this requirement should apply to RTRs

Each Difference Is Being Individually Evaluated for its Applicability to RTRs

difference → **Difference Resolution** → Draft NUREG

Example of Difference Resolution Evaluation

•The design shall permit the administrative control of access to safety system equipment. These administrative controls shall be supported by provisions within the safety systems, by provision in the RTR design, or by a combination thereof.

(Bases: IEEE Std 603-1991, Clause 5.9)

(Bases: ANSI/ANS 15.15, Clause 5.10)

Is there justification for the difference between regulations for RTRs and NPPs? __X___Yes _____No

If yes, why? The degree of control of access depends on the potential risk. _____

If the difference should be filled, is it the same for all RTRs? ____Yes _X___No

If the difference should be filled, is it _X_ a must have? ___ needs evaluation? ___ needs modification?

Comments: Admin control for access not only includes physical access to facility but software cyber security. Cyber security for software must be addressed throughout the software life cycle._____

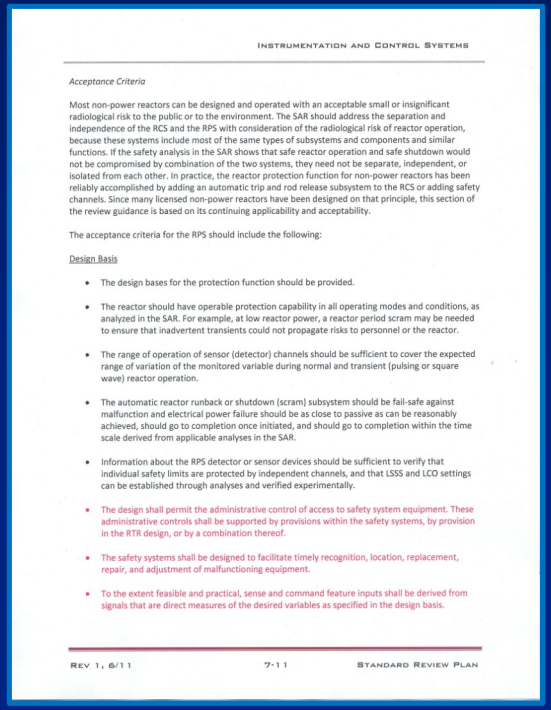
Recommendation: __ADD_____

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Collection of Favorable Difference Resolution Evaluations Provide Review Basis and Acceptance Criteria for Draft Report

Difference → Difference Resolution → **Draft NUREG**

- Revised report maintains format and style of NUREG-1537
- Little reliance on standards; standards only cited as source of additional information
- A public working group session will be scheduled to evaluate the basis and justification how these differences may be addressed



INSTRUMENTATION AND CONTROL SYSTEMS

Acceptance Criteria

Most non-power reactors can be designed and operated with an acceptable small or insignificant radiological risk to the public or to the environment. The SAR should address the separation and independence of the RCS and the RPS with consideration of the radiological risk of reactor operation, because these systems include most of the same types of subsystems and components and similar functions. If the safety analysis in the SAR shows that safe reactor operation and safe shutdown would not be compromised by combination of the two systems, they need not be separate, independent, or isolated from each other. In practice, the reactor protection function for non-power reactors has been reliably accomplished by adding an automatic trip and rod release subsystem to the RCS or adding safety channels. Since many licensed non-power reactors have been designed on that principle, this section of the review guidance is based on its continuing applicability and acceptability.

The acceptance criteria for the RPS should include the following:

Design Basis

- The design bases for the protection function should be provided.
- The reactor should have operable protection capability in all operating modes and conditions, as analyzed in the SAR. For example, at low reactor power, a reactor period scram may be needed to ensure that inadvertent transients could not propagate risks to personnel or the reactor.
- The range of operation of sensor (detector) channels should be sufficient to cover the expected range of variation of the monitored variable during normal and transient (pulsing or square wave) reactor operation.
- The automatic reactor runback or shutdown (scram) subsystem should be fail-safe against malfunction and electrical power failure should be as close to passive as can be reasonably achieved, should go to completion once initiated, and should go to completion within the time scale derived from applicable analyses in the SAR.
- Information about the RPS detector or sensor devices should be sufficient to verify that individual safety limits are protected by independent channels, and that LSSS and LCO settings can be established through analyses and verified experimentally.
- The design shall permit the administrative control of access to safety system equipment. These administrative controls shall be supported by provisions within the safety systems, by provision in the RTR design, or by a combination thereof.
- The safety systems shall be designed to facilitate timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment.
- To the extent feasible and practical, sense and command feature inputs shall be derived from signals that are direct measures of the desired variables as specified in the design basis.

REV 1, 6/11 7-11 STANDARD REVIEW PLAN

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Other Topics of Interest in Difference Analysis

- Diversity
- Cyber security
- Experimental system software
- GL 95-02

Lessons Learned—Based on Operating History, Diversity is an Important Requirement that should be Maintained (Redundancy Is Not Diversity)

- **Failure to Scram (**"Survey of Non-Power Reactors," ML003706367**).**

- **Event Description:**
  - The TRIGA had completed a routine 14 minute run at 15 watts power to perform core excess reactivity measurements. An attempt was made to manually scram the reactor using the scram button at the end of the run. When the manual scram button did not work, the operator's next step was to turn off power to the scram circuit using the reactor three-position key switch. As the operator touched the switch, the switch moved from a position between OPERATE and RESET to the OPERATE position. The operator then tried the manual scram button and the reactor scrammed.
- **Cause of Event:**
  - The licensee determined that a buildup of dirt prevented the three position switch from returning to the OPERATE position. When the switch is in the RESET position, the scram bus is disabled.
  - However, the console is designed so that magnet power is cut off when the switch is in the RESET position. This switch dates to original console installation in 1967. The switch operated properly during preoperational testing before start-up.
  - Upon further investigation, the licensee discovered that the wiring of the scram circuit was different from that shown in the Instrument Maintenance Manual provided by the reactor vendor. The licensee's investigation led to a conclusion that the location of a jumper was probably modified during initial installation of the reactor console in 1967. This modification bypassed the design feature that cut off magnet power when the three-position switch is in the RESET position.
- **Licensee Corrective Actions:**
  - The licensee took a number of corrective actions. The three position switch was removed, cleaned, and relubricated, which restored proper operation, and the switch was reinstalled in the console. The reactor console wiring was restored to its as-designed condition. A physical, electronic check of the wiring in the scram circuitry and other non-scram related circuits was performed to demonstrate that the wiring in the console is as designed. The reactor startup procedure was rewritten to test that the magnet power is cut off when the three position switch is placed in the RESET position. The reactor console was subject to routine startup checks and the semiannual console check procedure. The reactor vendor was contacted to obtain check out procedures to confirm that all suggested surveillances are done before reactor operation.
- **NRC Actions:**
  - The NRC performed a reactive inspection and issued two violations characterized as a Severity Level III problem; no civil penalty was imposed. NRC issued Information Notice 98-14.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

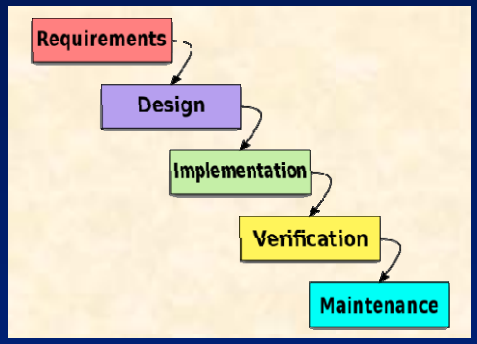
Manual Operator Actions Can be Credited for Diversity

- BTP 7-19 states that "When an independent and diverse method is needed as a backup to an automated system used to accomplish a required safety function as a result of the D3 assessment identifying a potential CCF, the backup function can be accomplished via either an automated system, or manual operator actions performed from the MCR. The preferred independent and diverse backup method is generally an automated system."

- The operator as a diverse means to shutdown the reactor highlights the need why the information the operator receives needs to be correct.

Cyber Security Must Be Addressed in Each Phase of the Lifecycle for Software (More than Now, Less than NPPs)

- Cyber security is not addressed in NUREG-1537. NUREG-0800 Appendix 7.1-D, "Guidance for Evaluation of the Application of IEEE Std 7-4.3.2," addresses cyber security in each phase of the software lifecycle phases:
  - Concepts
  - Requirements
  - Design
  - Implementation
  - Test
  - Installation, Checkout, and Acceptance Testing
  - Operation
  - Maintenance
  - Retirement.



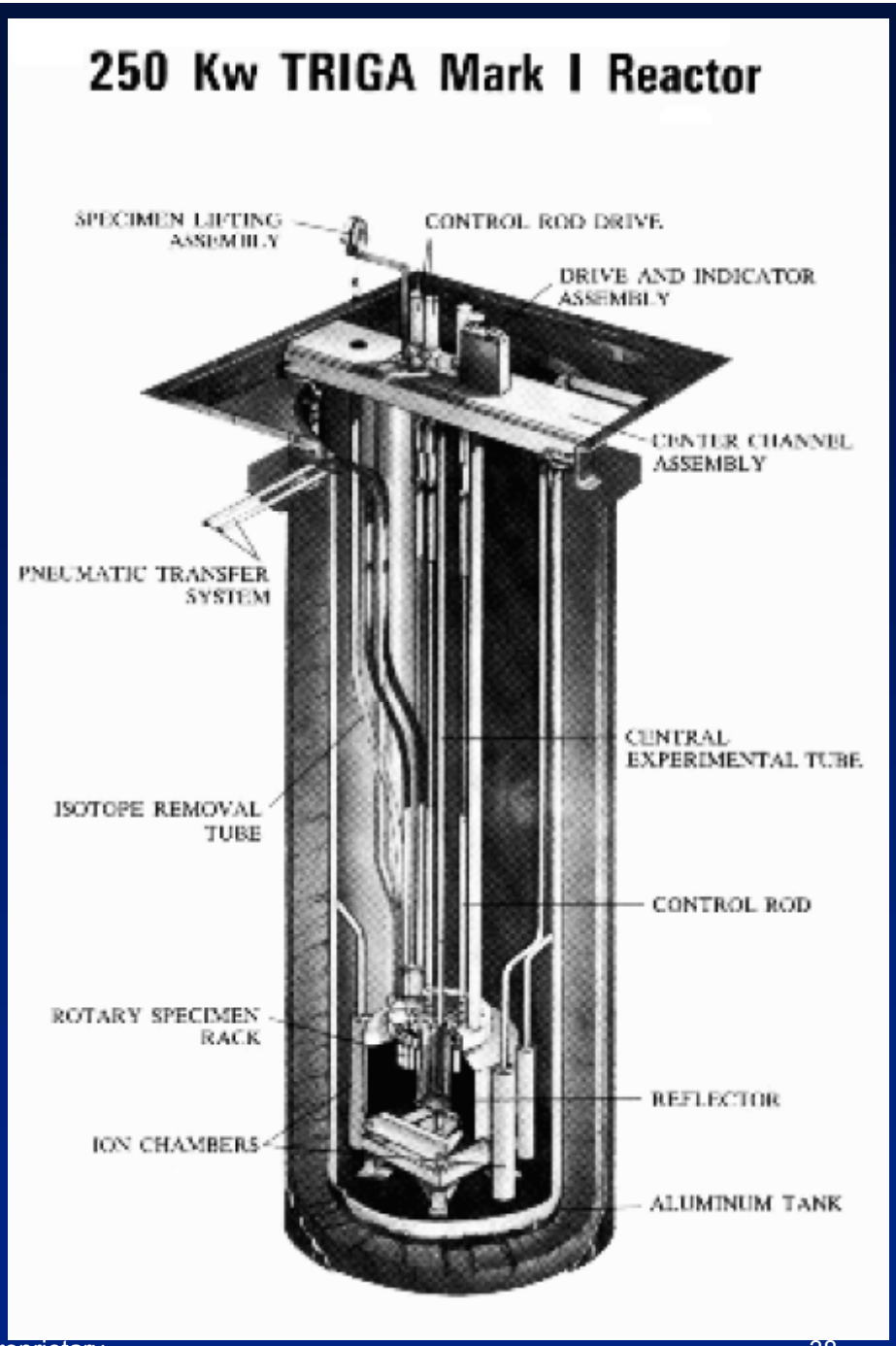
- With respect to control of access, NUREG-0800 Appendix 7.1-A states that the review should confirm that the DCS does not present an electronic path by which unauthorized personnel can change plant software or display erroneous plant status information to the operators. Computers or equipment outside the control of the plant staff may be connected to non-safety DCS (e.g., connections to remote data displays off site). In such cases, the connections should be through gateways that prevent unauthorized transactions originating from off site. Remote access to safety systems should not be implemented.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Experimental System Software

- Software for experimental systems should still meet the guidelines of ANSI/ANS 10.4-1987, “Guidelines for the Verification and Validation of Scientific and Engineering Computer Programs for the Nuclear Industry," that apply to non-power reactor systems

- If a digital experiment system can scram the reactor, this is to be evaluated in the difference analysis (e.g., shorting plugs)



U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

RTRs Should Consult GL 95-02 in Evaluating its Digital Upgrade

- NUREG-1537 states that for I&C systems that are being upgraded to systems based on digital technology, the applicant should consult NRC Generic Letter 95-02, "Use of NUMARC/EPRI Report TR-102348, Guideline on Licensing Digital Upgrades, in Determining the Acceptability of Performing Analog-to-Digital Replacements Under 10 CFR 50.59."

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

GL 95-02, Which Provides Guidance for a 10 CFR 50.59 Review, Has Been Superseded

- GL 95-02 endorses EPRI TR-102348.
- RIS 2002-22 endorses EPRI 1002833, which updates EPRI TR-102348.
- IN 2010-10 indicates that **software CCF** must be addressed for upgrades to systems that are "highly" safety significant, **even if applicant answers NO** to all 8 questions in 10 CFR 50.59(c)(2).
- **In practical terms, any digital upgrade that involves software will be reviewed by NRC.**

10 CFR 50.59 Process

- Applicability
  - Does the proposed change require review and/or approval?
- Screening
  - Determine if a 10 CFR 50.59 evaluation is required.
- Evaluation
  - Apply the eight evaluation criteria of 10 CFR 50.59(c)(2) to determine if a license amendment must be obtained from the NRC.
- Documentation
  - Document and report the activities implemented under 10 CFR 50.59.

There Are Eight Evaluation Criteria in 10 CFR 50.59(c)(2)

- 10 CFR 50.59(c)(2) list eight evaluation criteria.

  1. Does the Activity Result in More Than a Minimal Increase in the Frequency of Occurrence of an Accident?
  2. Does the Activity Result in More Than a Minimal Increase in the Likelihood of Occurrence of a Malfunction of an SSC Important to Safety?
  3. Does the Activity Result in More Than a Minimal Increase in the Consequences of an Accident?
  4. Does the Activity Result in More Than a Minimal Increase in the Consequences of a Malfunction?
  5. Does the Activity Create a Possibility for an Accident of a Different Type?
  6. Does the Activity Create a Possibility for a Malfunction of an SSC Important to Safety with a Different Result?
  7. Does the Activity Result in a Design Basis Limit for a Fission Product Barrier Being Exceeded or Altered?
  8. Does the Activity Result in a Departure from a Method of Evaluation Described in the UFSAR Used in Establishing the Design Bases or in the Safety Analyses?

- **If the evaluation shows that the proposed change meets one of the criteria, the licensee must submit the proposed design change in a license amendment request (LAR).**

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Issue Summary

- EPRI TR-102348/NEI 01-01 serves as a road map through existing regulatory requirements for the design and implementation of digital upgrades to I&C systems for NPPs.
- The report also provides supplemental guidance on the use of NEI 96-07 for digital upgrades to I&C systems. **Supplemental guidance is offered in EPRI TR-102348, Rev. 1 because the new 10 CFR 50.59 rule uses criteria that can be difficult to apply to software-based systems for which there is minimal precedent.**
  - Although 50.59 submittals provide useful examples for the screening process, each licensee must conduct its own 10 CFR 50.59 screening evaluation specific to the plant under consideration, and the design must conform to the applicable regulatory framework.
  - It is the staff's position that there are no established consensus methods for accurately *quantifying* the reliability and dependability of digital equipment.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Use of a Graded, Risk-Informed Evaluations of RTR Systems

- Software
- Power level

Less Stringent and Less Prescriptive Measures Are Sufficient at RTRs (Compared to NPPs) to Adequately Protect Safety

RTR (and NPP) Requirement for use of IEEE 7-4.3.2

- IEEE 7-4.3.2-2003, Section 5.3.3, "Verification and Validation (V&V)," states:
  - *The software V&V effort shall be performed in accordance with IEEE Std 1012-1998. The IEEE Std 1012-1998 V&V requirements for the highest integrity level (level 4) apply to systems developed using this standard.*
- IEEE Std 1012-2004, states that Software Integrity Level 4 software
  - *. . . must execute correctly or grave consequences (loss of life, loss of system, economic or social loss) will occur. No mitigation is possible.*

Description (from IEEE Std 1012-2004)	Level
Software element must execute correctly or grave consequences (loss of life, loss of system, economic or social loss) will occur. No mitigation is possible.	4
Software element must execute correctly or the intended use (mission) of the system/software will not be realized, causing serious consequences (permanent injury, major system degradation, economic or social impact). Partial to complete mitigation is possible.	3
Software element must execute correctly or an intended function will not be realized, causing minor consequences. Complete mitigation possible.	2
Software element must execute correctly or intended function will not be realized, causing negligible consequences. Mitigation not required.	1

Difference Evaluation

- Even unmitigated consequences from an accident at an RTR does not result in serious (level 3) or grave (level 4) consequences

V&V Activity Based on IEEE Std 1012-2004 Software Integrity Levels

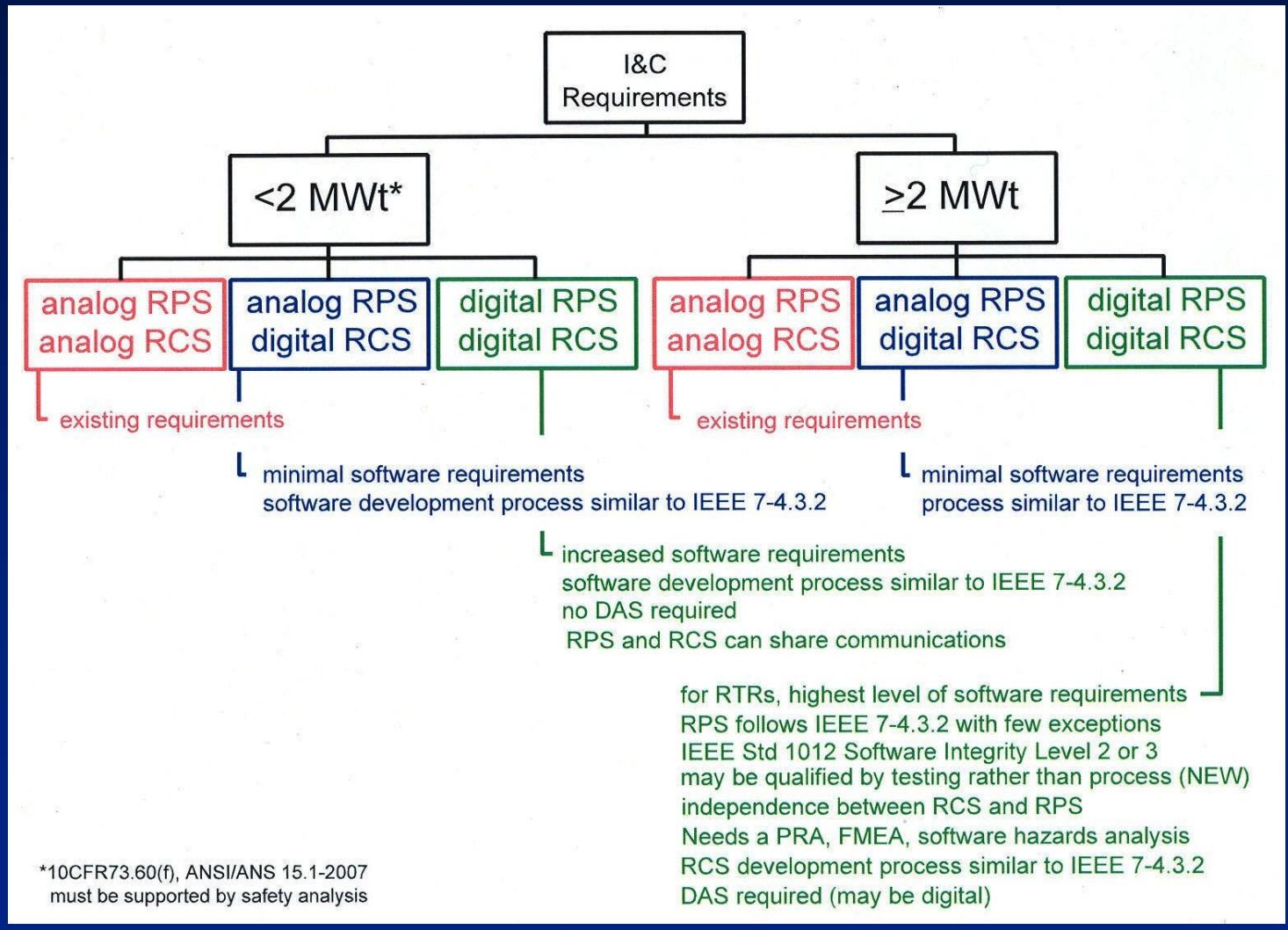
U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

V&V Activity	Software Integrity Level			
	1	2	3	4
Component V&V test plan and test procedure generation		X	X	X
Concept documentation Evaluation		X	X	X
Configuration management Assessment			X	X
Contract verification				X
Criticality analysis	X	X	X	X
Hardware/software/user requirements allocation analysis				X
Hazard analysis			X	X
Identify improvement opportunities in the conduct of V&V	X	X	X	X
Installation checkout			X	X
Installation configuration audit			X	X
Integration V&V test case, design, execution, plan, and procedure generation	X	X	X	X
Interface analysis		X	X	X
Interface with organizational and supporting processes			X	X
Management and technical review support			X	X
Management review of the V&V effort	X	X	X	X
Migration assessment			X	X
New constraints evaluation		X	X	X
Operating procedures evaluation			X	X
Planning the interface between the V&V effort and supplier	X	X	X	X
Proposed/baseline change assessment		X	X	X
Retirement assessment			X	X
Risk analysis			X	X
Scoping the V&V effort	X	X	X	X
Security analysis			X	X
Software design and requirements evaluations	X	X	X	X
SVVP generation and revision	X	X	X	X
Source code and source code documentation evaluation		X	X	X
System requirements review	X	X	X	X
System V&V test case, design, execution, plan, and procedure generation	X	X	X	X
Task iteration	X	X	X	X
Traceability analysis		X	X	X
V&V final report generation	X	X	X	X

- IEEE Std 7-4.3.2-2003 requires that the software shall be Software Integrity Level 4.
- The yellow boxes show that there is not much difference between Software Integrity Level 3 and Software Integrity Level 4
- The blue boxes show that there are appreciable differences between Software Integrity Level 1 and Software Integrity Level 2
- The green boxes show that there are significant differences between Software Integrity Levels 1/2 and Software Integrity Levels 3/4
- The inherent safety, low temperatures, low source terms, and low consequences would deem Software Integrity Level 1 or 2 to be appropriate for RTRs.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Proposed Risk-Informed Update to NUREG-1537, Part 2 Maintains Current Level of Regulatory Oversight



U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

NUREG-1537 Review Issues and Decision Points

- Assess the differences identified and create difference Analysis Resolution tables. These tables will be comprised of the
  - Comparison of ANSI/ANS 15.15-1978 to IEEE Std 603-1991
  - Mapping of NUREG-0800 onto NUREG-1537
  - Mapping of NUREG-1537 onto NUREG-0800
- Discuss the risk-informing options with NRR I&C Branch
- Discuss the format, content, and style of updated draft in another public meeting

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Thank you for coming!