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.

Norbert Carte

Duane A. Hardesty

George Wilson

U.S. Nuclear Regulatory Commission, Office of Nuclear Reactor Regulation

Roger A. Kisner

Michael D. Muhlheim, Ph. D

Oak Ridge National Laboratory

Thursday, September 14, 2011

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

Purpose

- To discuss
  - the process of developing proposed revisions to NUREG-1537,
  - preliminary results of that development process,
  - concepts for graded and conditional evaluations of updates to digital I&C systems at RTRs, and
  - other issues related to the revision of NUREG-1537 that affect the RTR community.

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

Agenda for Public Meeting September 14, 2011

Time	Topic	Led By
08:00 – 08:10	Opening Remarks	NRC
08:10 – 08:30	Summary of Prior Meeting	NRC
08:30 – 10:00	Proposed Acceptance Criteria Revisions	NRC
10:00 – 10:15	BREAK	
10:15 – 11:15	Proposed Revisions (cont)	NRC
11:15 – 11:45	Invitation for Public Participation	NRC
11:45 – 12:00	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 (I&C Systems).
- Review the digital upgrades in the 1990's (historical perspective).
- Develop a structured process that reviews and updates existing guidance for RTRs and incorporates lessons learned from new digital I&C (DI&C) designs and upgrades.
- Prepare a draft to NUREG-1537.
- Hold additional public workshops.

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

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 analog I&C systems with digital I&C systems, update the guidance for implementing these changes in NUREG-1537,
  - use the currently available guidance for RTRs to provide an initial foundation, and
  - leverage the appropriate experience gained in licensing digital I&C systems and upgrades at NPPs by adapting applicable guidance to RTRs.

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

Digital Systems Have a Potential for Unintended Behaviors and Subtle Failure Modes

- The introduction of software and microprocessors could create new failure mechanisms, such as software errors and electromagnetic interference that either were not considered during the initial plant design or not evaluated in sufficient detail in the safety analysis report.

- These failure mechanisms may cause the reactor to malfunction in a way not previously considered. For example, at one facility, after replacing an analog system with a digital system, spikes that were filtered out in the analog system were not filtered out in the digital system, causing a spurious reactor trip. Capacitors were added to solve the new and unexpected failure mode.

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

There Are Several Unique Characteristics of Digital Technology (1)

- Complexity
  - Finite state machine (digital) vs continuous physical condition (analog)
  - Large number of states and very large number of state transition possibilities characterize all but simplest digital implementations
  - Software execution of function not constrained by physical laws (discontinuous states and unpredictable transitions are possible)
  - High potential for introduction of latent systematic faults

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

There Are Several Unique Characteristics of Digital Technology (2)

- High functional density
  - Multiple functions combined into single module vs specific functions on discrete modules
  - Failure affects multiple functions (one subroutine can service multiple, disparate functions)
- Timing dependencies
  - Sequential (step-by-step) execution of function in recursive loop vs parallel (concurrent) execution of function continuously
  - Deterministic performance difficult to establish both in execution and communication
  - Potential for execution/communication delays and “hung’ performance

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

There Are Several Unique Characteristics of Digital Technology (3)

- Configuration management (CM)
  - High flexible, readily changeable software implementation vs hardwired discrete instrumentation
  - Version control of abstract elements (software, logic) necessary in addition to equipment/part identification
  - Capability to modify in the field or alter functionality remotely requires strict Configuration Management (CM)
- Quality assurance
  - Complex, process-oriented QA for software vs basic, product-oriented QC for hardware
  - Verification and validation complicated by inability to exhaustively test software-based digital systems

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

Some of the Advantages of Digital Technology

- Aging and obsolete analog I&C systems have made the use of digital equipment attractive.
- Analog technology intermixes all noise, distortion, drift, and inaccuracies in the signal path and thus become sources of signal error. In distinction, digital technology represents signals as non-continuous symbols (binary estimates) that are not directly affected by circuit imperfections—noise, distortion, drift, and degradation over time.
- Computers and software are flexible and adaptable.
  - Enhanced features such as automatic self-test and diagnostics.

Recent Guidance on Digital I&C Systems was Developed for NPPs, not RTRs

- 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.
  - Although these new requirements are for NPPs, many lessons learned may be applicable/useful to RTRs.
  - There are issues unique to RTRs such as varied power level and diverse design features that will require a more graded approach (i.e., any new guidance cannot be a “one size fits all” approach).

Requirements of Interest to DI&C Upgrades

Regulations	Title	Text
10CFR50.2	Definitions – Design bases	Design bases means that information which identifies the specific functions to be performed by a structure, system, or component of a facility, and the specific values or ranges of values chosen for controlling parameters as reference bounds for design.
10 CFR 50.34	Contents of applications; technical information.	Contents of applications; technical information. (a) PSAR (b) FSAR (c) Physical Security Plan (d) Safeguards Contingency Plan
10CFR50.36	Technical specifications.	(c) Technical specifications will include items in the following categories: (1) Safety limits, limiting safety system settings, and limiting control settings. (2) Limiting conditions for operation. (3) Surveillance requirements. (4) Design features. (5) Administrative controls. (6) Decommissioning.
10 CFR 50.55a(a)(1)	Codes and standards.	Structures, Systems, and Components must be designed, fabricated, erected, constructed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed.
10 CFR 50.59	Changes, tests and experiments.	10 CFR 50.59(c)(2) list eight evaluation criteria.
10 CFR 50.90	Application for amendment of license, construction permit, or early site permit.	. . . fully describing the changes desired, and following as far as applicable, the form prescribed for original applications.
10 CFR 50, Appendix E, I-V	Emergency Planning and Preparedness for Production and Utilization Facilities	I. Introduction II. PSAR III. FSAR IV. Content of Emergency Plans V. Implementing Procedures VI. Emergency Response Data Systems

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

- An understanding of the design, risk, and regulatory differences is necessary to properly adapt regulations and experience from NPPs to RTRs.
  - Because of the lower thermal power level in RTRs, the decay heat is insufficient to cause cladding damage under any cooling condition. Furthermore, the generally intermittent operation results in a significantly smaller inventory of fission products in the fuel.
  - TRIGA-type RTRs have an inherent reactivity insertion safety feature in their design and generate minimal decay heat that precludes damage to the fuel.
- The much lower public risk associated with RTRs has been one of the bases upon which the NRC has accepted that less stringent and less prescriptive measures provide reasonable assurance for the protection of the public, workers, and the environment. This is consistent with the Atomic Energy Act of 1954, as amended, which states that utilization facilities . . . should be regulated to the minimum extent consistent with protecting the health and safety of the public.

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

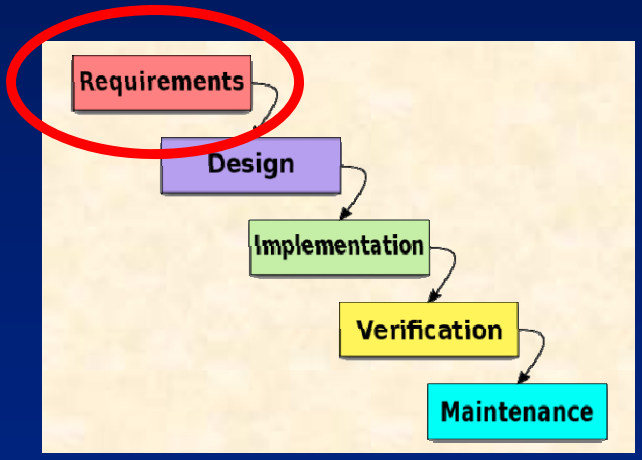
The GA Console and Penn State Reviews Recognized the Level of Risk from RTRs

- 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 reviewers recognized that they were not NPP reviews—this philosophy is being maintained in the update to NUREG-1537.
  - Engineering judgment was used in the reviews because the fuel could not be damaged (i.e., the TRIGAs did not need to meet all of the criteria for NPPs).
  - The initial publication of NUREG-1537 in 1996 captured what was done in the reviews.

The Previous Reviews Noted Deficiencies in the Applications for Digital Upgrades

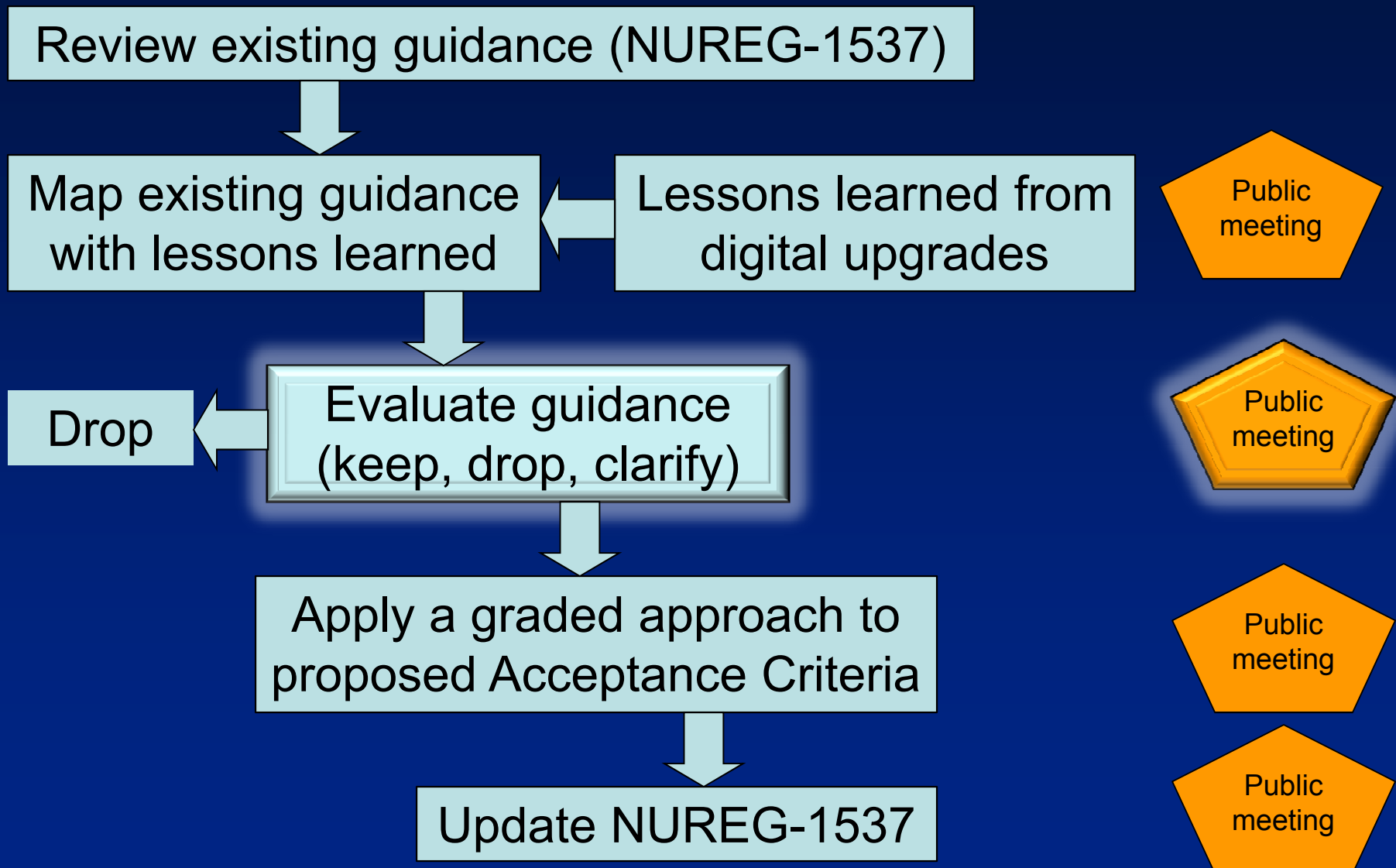
Noted deficiencies (corrected prior to approval)

- 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.



Waterfall model

A Structured Process is Being Used to Modernize Guidance in NUREG-1537



Identification of Lessons Learned

- Assess the similarities and differences between ANSI/ANS 15.15-1978 vs. IEEE Std 603-1991

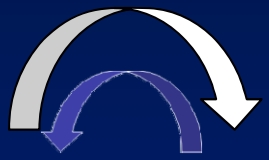
- Identify lessons learned from digital guidance for NPPs (e.g., compare NUREG-1537 vs. NUREG-0800)
  - NUREG-1537 Section 7.3 (RCS) vs NUREG-0800 Section 7.7 (control system)
  - NUREG-1537 Section 7.4 (RPS) vs NUREG-0800 Section 7.2 (RTS)
  - NUREG-1537 Section 7.5 (ESFAS) vs NUREG-0800 Section 7.3 (ESFAS)
  - NUREG-1537 Section 7.6 (console and display) vs NUREG-0800 Section 7.5 (info systems)
  - NUREG-1537 Section 7.7 (rad monitoring) vs NUREG-0800 Section 7.5 (control systems)
  - NUREG-1537 vs NUREG-0800 Section 7.4 (Safe Shutdown Systems)
  - NUREG-1537 vs NUREG-0800 Section 7.6 (Interlocks)
  - NUREG-1537 vs NUREG-0800 Section 7.8 (D3)
  - NUREG-1537 vs NUREG-0800 Section 7.9 (DCS)

- Worksheet for revision to Acceptance Criteria--7.3 RCS
- Worksheet for revision to Acceptance Criteria--7.4 RPS
- Worksheet for revision to Acceptance Criteria--7.5 ESFAS
- Worksheet for revision to Acceptance Criteria--7.6 Control Console and Display
- Worksheet for revision to Acceptance Criteria--7.7 Rad Monitoring Inst

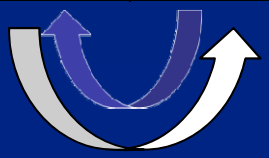
Recent Reviews of Digital Upgrades (GA and Penn State) Followed ANSI/ANS 15.15-1978 (withdrawn). Should the Reviews Follow IEEE Std 603-1991?

- **There are requirements in ANSI/ANS 15.15-1978 that are not in IEEE Std 603-1991**
  - **e.g., fail-safe design vs. single-failure criterion**
- **There are requirements in IEEE Std 603-1991 that are not in ANSI/ANS 15.15-1978**
  - **e.g., Equipment Qualification including qualification and testing of computers and COTS.**
- **There are requirements in IEEE Std 603-1991 that are too restrictive for RTRs**
  - e.g., Clause 5.3 of IEEE Std 603-1991 identifies ANSI/ASME NQA1-1989 as a prescribed QA program.

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

Insights from an Analysis Applied to the RCS shows . . .

- A combined RPS/RCS increases the likelihood of RCS compromising the 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 the failure of the RPS does not lead to greater than negligible risk.
- Need to address the possibility that the RPS/RCS is susceptible to CCFs that could inhibit ability to control while also affecting ability of the protection system.
- Quality hardware and software is necessary to minimize challenges.

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

Insights from an Analysis Applied to the RPS shows . . .

- As expected, the most significant difference is in the criteria 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.

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

Insights from an Analysis Applied to the 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 RTRs compared to NPPs

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

Insights from an Analysis Applied to the 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 (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 and UNNECESSARY criteria on RTRs that were not present in NUREG-1537 (RTRs perform a system check prior to startup and shut down for maintenance). ANSI/ANS 15.15-1978 Clause 5.7.4 already requires audible and visual announcement of any bypass.

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

Insights from an Analysis Applied to the Radiation Monitoring Systems shows . . .

- NUREG-1537 states that "the [Radiation Monitoring] 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." Data communication between the radiation monitoring systems and the RPS should not inhibit the performance of the safety function.

- 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" will be N/A for RTRs.

Prior to Mapping the Lessons Learned, the Acceptance Criteria for RTRs Was Updated

NUREG-1537

- IEEE Std 7-4.3.2-1993, "IEEE Standard Criteria for Digital Computers Systems in Safety Systems of Nuclear Power Generating Stations"
- Regulatory Guide 1.152, Revision 1, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants"
- ANSI/ANS 10.4-1987, "Guidelines for the Verification and Validation of Scientific and Engineering Computer Programs for the Nuclear Industry"
- ANSI/ANS 15.15-1978, "Criteria for the Reactor Safety Systems of Research Reactors"
- ANSI/ANS 15.20 (draft), "Criteria for the Control and Safety Systems for Research Reactors"

Updated Criteria for NUREG-1537

- IEEE Std 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers Systems in Safety Systems of Nuclear Power Generating Stations"
- Regulatory Guide 1.152, Revision 2, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants"
- ANSI/ANS 10.4-2008, "Verification and Validation of Non-Safety-Related Scientific and Engineering Computer Programs for the Nuclear Industry"
- ANSI/ANS 15.15-1978, "Criteria for the Reactor Safety Systems of Research Reactors" (withdrawn)
- ANSI/ANS 15.20 (draft), "Criteria for the Control and Safety Systems for Research Reactors"

The Clauses in IEEE Std 7-4.3.2 and ANSI/ANS 15.15 were Individually Reviewed

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

Updated Criteria For NUREG-1537

- Item 1: range of operation
- Item 2: continuous indication
- Item 3: sensitivity
  .
  .
- IEEE Std 7-4.3.2-2003
- RG 1.152, Rev. 2 (IEEE Std 603-1991)
- ANSI/ANS 15.15-1978
- ANSI/ANS 10.4-2008

Lessons Learned

Expanded Criteria for NUREG-1537

- Item 1: range of operation
- Item 2: continuous indication
- Item 3: sensitivity
  .
  .
- IEEE Std 7-4.3.2-2003, Clause 5.3 Quality
- IEEE Std 7-4.3.2-2003, Clause 5.4 EQ
  .
  .
- IEEE Std 7-4.3.2-2003, Clause 5.15 Reliability
- RG 1.152, Rev. 2 Clause 2.1-2.9
- ANSI/ANS 15.15-1978, Clause 4 Design Basis
- ANSI/ANS 15.15-1978, Clause 5.1 Single Failure
  .
  .
- ANSI/ANS 15.15-1978, Clause 5.7 Bypasses
- ANSI/ANS 10.4-2008

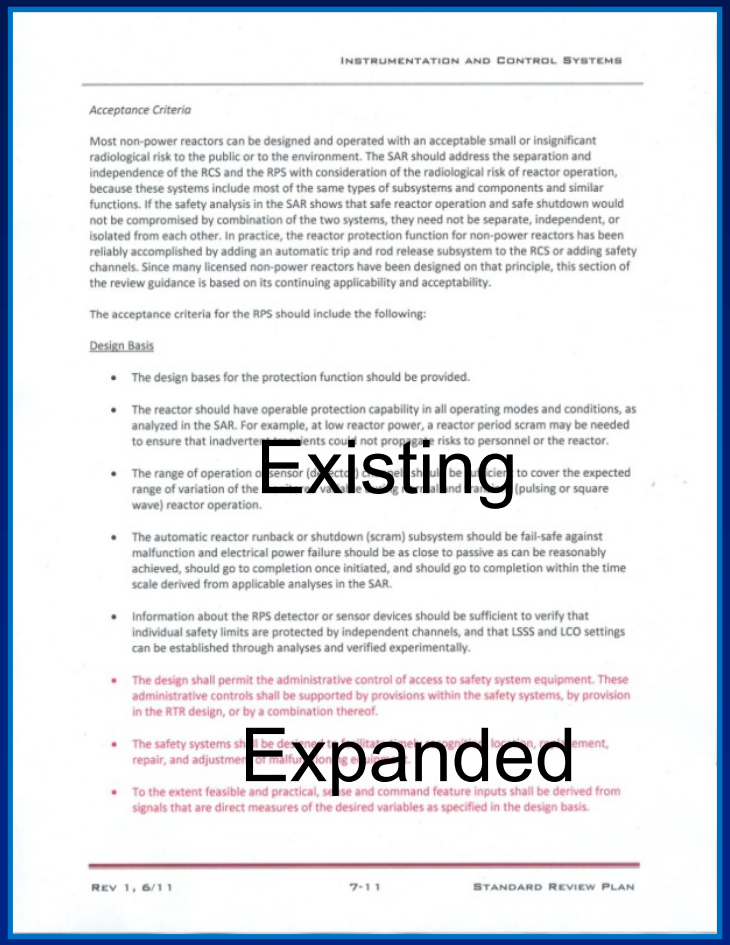
Each Criteria Is Being Individually Evaluated for its Applicability to RTRs

The review of access control should confirm that design features provide the means to control physical access to safety system equipment, including access to test points and means for changing setpoints. Typically such access control includes provisions such as alarms and locks on safety system panel doors, or control of access to rooms in which safety system equipment is located. Review of digital computer-based systems should consider controls over electronic access to safety system software and data. Controls should address access via network connections, and via maintenance equipment.
(Source: ANSI/ANS 15.15, Clause 5.10)
(Source: IEEE Std 603-1991, Clause 5.9)
Comments: NUREG-1537 addresses access control for radiation and experimental areas but not access to I&C components. Access control applies to both analog and digital systems. In addition, access control not only includes physical access to facility but software cyber security. Cyber security for software must be addressed throughout the software life cycle.
Recommendation: KEEP

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

The Collection of Criteria Provides the Basis for the Proposed Acceptance Criteria for the Draft Report

- The revised report will maintain the format and style of NUREG-1537.
- NUREG-1537 will be a stand-alone document. Criteria will be provided in bullet form; standards will primarily be cited as source of additional information.
- A public working group session will be scheduled to evaluate the proposed criteria.



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 [illegible] could not propagate risks to personnel or the reactor.
- The range of operation of sensor (detector) [illegible] should be sufficient to cover the expected range of variation of the [illegible] 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 [illegible] repair, and adjustment [illegible]
- 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

Existing

Expanded

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

Preliminary Results of Proposed of *Acceptance Criteria*

Section	NUREG-1537		Proposed	Drop
	Existing Bullets	Expanded Bullets*	Clarify**	
7.3 RCS	24	2	8	17
7.4 RPS	17	29	22	75
7.5 ESFAS	10	18	12	3
7.6 Control Console and Display	12	3	16	6
7.7 Radiation Monitoring Systems	8	1	15	9
Total	71	53	73	110

*Collected from the review of ANSI/ANS 15.15-1978, IEEE Std 7-4.3.2-2003, and RG 1.152, Rev. 2.
**Based on lessons learned from digital upgrades.

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

RCS

Review Category	Existing Bullets	Expanded Bullets	Proposed
Design Basis	18		3
Effects of Control System Operation/Failures	1		1
Use of Digital Systems	2		1
Environmental Control System	1		
Safe State	1		
Experiment or Experimental Facility	1		
Safety Classification			1
Independence		1	
Potential for Inadvertent Actuation			1
Control of Access		1	
Setpoint Determination/Performance			1
Total	24	2	8

RCS has 8 Proposed Bullets

- Of the 8, 1 is only related to digital systems
  - Guidance for purchase of PLC hardware; embedded and operating systems software, programming tools, and peripheral components
- The other 7 apply to both analog and digital systems
  - Manual and automatic control of process variables
  - EMI/RFI
  - Lightning
  - No reliance on RCS in accident analysis
  - Limit inadvertent actuations and challenges to safety systems
  - High probability of accomplishing safety function in event of AOO
  - Guidance for setpoint analysis methodology and assumptions

Example of Proposed Bullet for the RCS

Proposed Bullet

- Review the electromagnetic environment operating envelopes, design, installation, and test practices that address the effects of electromagnetic interference/radio frequency interference (EMI/RFI), and power surges on I&C systems and components important to safety.

Justification

- *Experience with EMI has indicated that digital electronics may be both a generator of and susceptible to EMI. Interference to a digital input introduces different responses as compared with analog inputs. A digital input, operating in a binary state and expecting a serial sequence, can be spoofed by a burst of interference or blocked for a short period, whereas with an analog input, an interfering pulse may generate a spike simulating a sudden, short-duration temperature or pressure signal. Because of the fundamental differences between analog and digital signal types as well as the differences in internal circuit functioning, specific qualification of digital systems is necessary.*

- *Thus, although NUREG-1537 states that "The RCS should be designed for reliable operation in the normal range of environmental conditions," susceptibility to EMI/RFI should be specifically identified and evaluated.*

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

RPS

Review Category	Existing Bullets	Expanded Bullets	Proposed
Design Basis	5	4	3
Single Failure and Independence	2		2
Testing and Surveillance	4		1
Environmental	1		
Human Factors	3		1
Use of Digital Systems	2	6	11
Quality		2	
Setpoint Determination/Performance		1	
Bypass Permissives		5	
Diversity			1
Data Communications		2	3
Security		9	
Total	17	29	22

RPS has 22 Proposed Bullets

- Of the 22, 15 are only related to digital systems
  - Security vulnerabilities
  - Activities for safety system software (e.g., control, test, documentation)
  - Diversity and defense-in-depth analysis
  - Data communications
- The other 7 apply to both analog and digital systems
  - Timely recognition of malfunctioning equipment
  - EMI/RFI
  - Separation of redundant sensing lines
  - Independence of RPS circuits and safety/nonsafety systems
  - Connections to safety system
  - Testing during operation
  - Consideration of human factors

Example of Proposed Bullet for the RPS

Proposed Bullet

- Redundant instrumentation sensing lines should be routed and protected so that any credible effects (consequences) of any design-basis event that is to be mitigated by signals sensed through those sensing lines should not render any of these redundant sensing lines inoperable unless it can be demonstrated that the protective function is still accomplished. Instrument sensing lines should be routed such that no single failure can cause the failure of more than one redundant sensing line unless it can be demonstrated that the protective function is still accomplished.

Justification

- *Errors can be introduced into sensing and signal lines that are common to multiple systems. Systems utilizing these signals may be redundant safety systems, control systems, or operator displays. Propagation of an erroneous value into these systems can lead to conflicting actions. An example would be that of an erroneous low flux reading, which would be acted on by the control systems to increase reactivity whereas the protection system would see it as a non-threatening condition and not respond. Although not all RTRs would have sensing lines for pressure or chemical sampling, when those are used evolved gases present in the lines have been known to adversely affect readings.*

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

ESFAS

Review Category	Existing Bullets	Expanded Bullets	Proposed
Design Basis	2	5	2
Single Failure and Independence	2	2	1
Quality	1	1	
Testing and Surveillance	2	4	1
Environment	1		
Use of Digital Systems	2	2	3
Completion of Protective Action		1	
Diversity and Defense-in-Depth			1
Setpoint Determination/Performance			1
Control of Access		1	
Repair			1
Identification		1	
Human Factors			1
Reliability			1
Total	18	15	12

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

ESFAS has 12 Proposed Bullets

- Of the 12, 5 are only related to digital systems
  - Environmental qualification of computer-based system
  - EMI/RFI
  - Diversity and defense-in-depth analysis
  - Data communications
  - Effect of software on system reliability
- The other 9 apply to both analog and digital systems
  - Auxiliary features should not degrade safety performance
  - Inputs should be derived from signals that are direct measures
  - Independence between interconnections among division or between systems
  - Setpoint determination methodology should be documented
  - Timely recognition, location, replacement, repair of malfunctioning equipment
  - Human factors should be considered

Example of Proposed Bullet for the ESFAS

Proposed Bullet

- The system timing requirements calculated from design basis events and other criteria should be appropriately allocated to the digital computer portion of the ESFAS and be satisfied in the digital system architectural design. The real-time performance of the ESFAS should include verification that system timing is deterministic or bounded. Time delays within the digital ESFAS and measurement inaccuracies introduced by the digital components should be accounted for in the establishment of the instrumentation setpoints. Timing must be accounted for in system response and verified in testing. Practices should address asynchronous operation of separate modules.

Justification

- *A digital system may exhibit slower (and perhaps faster in some cases) response time from trigger condition to actuation initiation as compared with that of an analog electronic system. The timing difference may allow an increase in process energy (e.g., temperature or pressure) that could increase risk of release or equipment failure. Timing delays may be variable owing to CPU or communication loading or other non-deterministic factors in the system. For this reason, an analysis of timing performance from sensors through actuators including the digital system should be performed. The analysis should be verified by actual testing.*

Control Console and Display

Review Category	Existing Bullets	Expanded Bullets	Proposed
Design Basis	8		6
Design Basis—DI&C			2
Annunciator System	1	1	4
Control of Access	1		
Use of Digital Systems	1	1	2
Safe State	1		
Single Failure			1
BISI			1
Independence		1	
Total	12	3	16

Control Console and Display has 16 Proposed Bullets

- Of the 16, 5 are only related to digital systems
  - The displays and controls should be independent and diverse from the computer-based safety system(s)
  - Communications
  - Timing, quality, and testing
- The other 11 apply to both analog and digital systems
  - HFE principles
  - Manual controls downstream of automatic controls
  - Single-failure criterion to and the physical independence of the electrical power, instrumentation, and control portions of safety-related consoles and display systems
  - Annunciator systems (redundancy, independence, MMI, testability)

Example of Proposed Bullet for the Control Console and Display Systems

Proposed Bullet

- HFE principles and criteria should be applied to the selection and design of the displays and controls. Main Control Room minimum inventory includes the human system interfaces that the operator always needs available to:
  - monitor the status of fission product barriers,
  - perform and confirm a reactor trip,
  - perform and confirm a controlled shutdown of the reactor using the normal or preferred safety means,
  - actuate safety related systems that have the critical safety function of protecting the fission product barriers,
  - analyze failure conditions of the normal human system interfaces (while maintaining the current plant operating condition and power level until the human system interfaces are restored in accordance with applicable regulatory requirements),
  - implement the plant's emergency operating procedures,
  - bring the plant to a safe condition,
  - carry out those operator actions shown to be risk important by the applicant's accident analysis.

Justification

- *Human performance requirements should be described and related to safety criteria. New methods of human interaction are available now that were not prior to modern digital systems. For example, touch screens, which are commonly used in control rooms, can be designed to be clearly understood and reduce the likelihood of operator misoperation. However, without application of good human factors design criteria, the screens can become virtually unreadable and un-navigable.*

Radiation Monitoring Systems

Review Category	Existing Bullets	Expanded Bullets	Proposed
Design Basis	4	1	1
Test and Calibration	2		
Environment	1		
Use of Digital Systems	1		1
Single Failure			1
Display and Recording			11
Human Factors			1
Total	8	1	15

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

Radiation Monitoring Systems has 15 Proposed Bullets

- Of the 15, 1 is only related to digital systems
  - CCF of computer software
- The other 14 apply to both analog and digital systems
  - If signal validation is used, the validity of the indication should be provided as part of the display
  - No single failure should prevent the operators from being presented the information necessary (different from Bullet 2)
  - Display and recording of accident monitoring variables
  - Design of instrumentation to facilitate the recognition, location, replacement, repair, or adjustment of malfunctioning components or modules

Example of Proposed Bullet for the Radiation Monitoring System

Proposed Bullet

- No single failure within either the accident-monitoring instrumentation, its auxiliary supporting features, or its power sources concurrent with failures that are a result of a specific accident should prevent operators from being presented information necessary for them to determine safety status of the plant and to bring the plant to and maintain it in a safe condition following that accident.

Justification

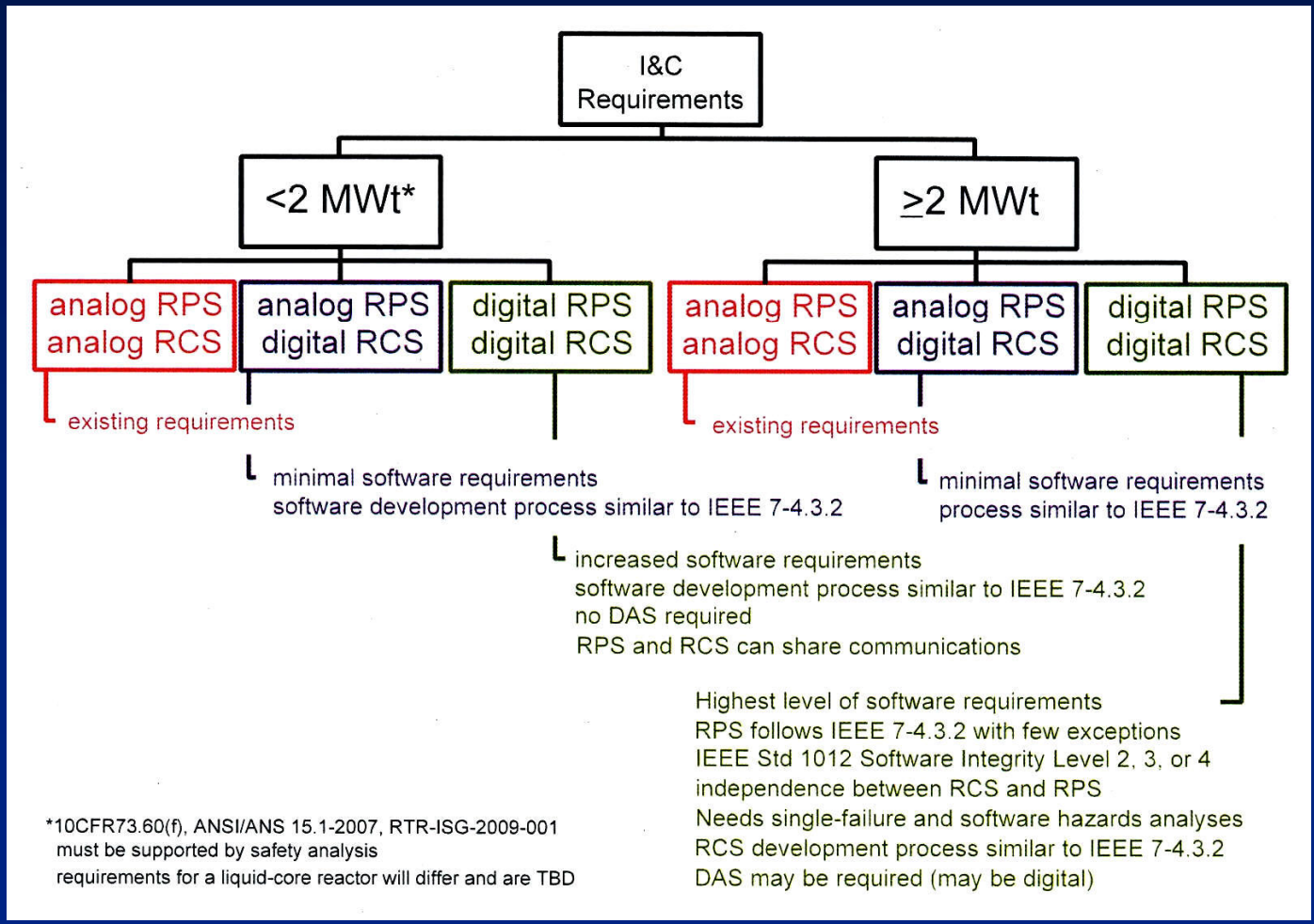
- *Radiation monitoring systems, which provide operators with necessary information to verify functioning of control systems, protection systems, and plant state, should be impervious to single failures. Independent information channels or diverse measurements can be provided to mitigate against the effect of a single failure. This criterion goes beyond the requirement to prevent functioning of the RPS because radiation monitoring systems directly supply operators with information that affects contingency planning.*

The Next Step is to Apply a Graded and Conditional Evaluation to the Proposed Acceptance Criteria

- Graded and conditional evaluations will be applied to the Acceptance Criteria selected from the reviews of NUREG-1537, IEEE Std 7-4.3.2-2003, ANSI/ANS 15.15-1978, RG 1.152, and lessons learned from digital system upgrades and designs.
  - If independence between the RPS and RCS is not required, communications between safety and nonsafety divisions would not be required.
  - If there is only 1 channel, the single-failure criterion would not apply.
- Efforts are underway to determine the software integrity level (SIL) for RTRs and if this SIL applies to all RTRs or there is a different SIL based on a graded approach.
- The need and level of diversity, defense-in-depth, independence, and single-failure criterion is undergoing further review.
  - The GA and Penn State applications maintained an analog scram system.
  - If no redundancy is required, an analysis of diversity and common-cause failure of software is not applicable.

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

A Graded Approach Based on Power Level May Be Used to Separate the Acceptance Criteria



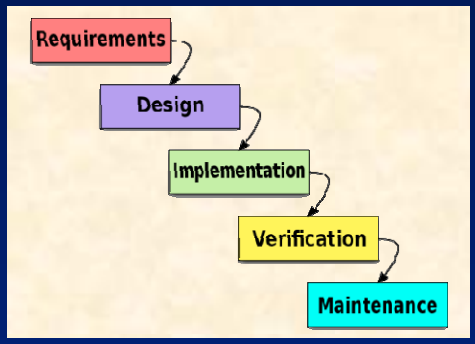
U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Special Topics of Interest in Reviews

- Cyber security
- Experimental system software
- GL 95-02 (Digital Upgrades)

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

- Regulatory Guide 1.152, Rev. 2, presents the waterfall lifecycle phases as a framework for describing specific digital safety system security guidance. The digital safety system development process should address potential security vulnerabilities in each phase of the digital safety system:
  - Concepts;
  - criteria;
  - Design;
  - Implementation;
  - Test;
  - Installation, Checkout, and Acceptance Testing;
  - Operation;
  - Maintenance; and
  - Retirement.



- With respect to control of access, the review should confirm that the data communication system (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.

Cyber Threats are Real

- **Stuxnet** is a computer worm first discovered in June 2009.
- The Stuxnet computer virus had caused problems with the controller handling the centrifuges at the Natanz facilities in Iran.
- Speculation is that the infection may have spread from USB drives (i.e., jumped an air gap)
- The worm initially spreads indiscriminately, but includes a highly specialized malware payload that is designed to target only Siemens Supervisory Control And Data Acquisition (SCADA) systems that are configured to control and monitor specific industrial processes. Stuxnet infects programmable logic controllers (PLCs) by subverting the software application that is used to reprogram these devices.

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

Experimental System Software

- Software for experimental systems should meet the updated guidelines provided in ANSI/ANS 10.4-2008, "Verification and Validation of Non-Safety Related Scientific and Engineering Computer Programs for the Nuclear Industry."

- If a digital experiment system can scram the reactor (e.g., shorting plugs), this is to be evaluated in the GL 95-02 analysis.

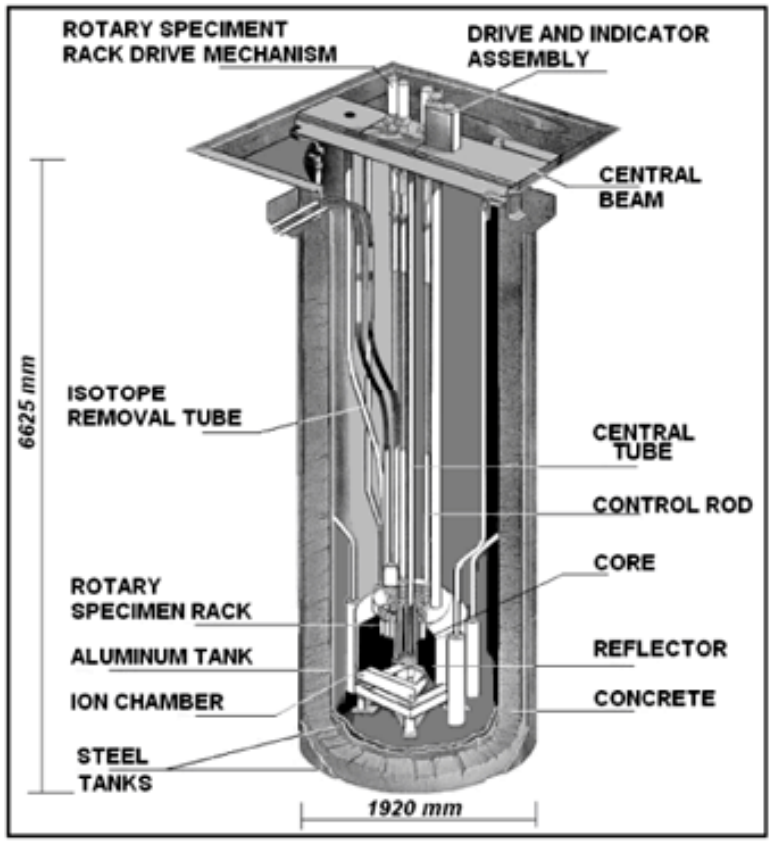


FIG. 1: The pool of the IPR-R1 TRIGA nuclear reactor (courtesy of Dr. A. Z. Mesquita).

Subcommittee for DI&C

- The TRTR Executive Committee is forming two sub-committees,
  - one to work on a new relicensing process for RTRs, and
  - the other for developing regulations and licensing processes for Digital I&C for RTRs.
- The TRTR Executive Committee has asked for 3-5 members from the RTR community to participate in what will likely be monthly meetings at White Flint for about 1-2 years.
- The TRTR Executive Committee is soliciting nominations of individuals to participate on one or both of the committees from the RTR facilities.
  - Please submit nominations for the committees directly to Steve Miller, Chairman of TRTR ("Steve Miller" <sim@simelectronics.com>) no later than Monday 25 July. If you have any questions, please direct them to Steve Miller.

Path Forward

NUREG-1537 Review Issues and Decision Points

- Assess the Existing, Expanded, and Proposed bullets in a Public Workshop
- 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!

This presentation is a publicly available record accessible electronically from the Agencywide Documents Access and Management System (ADAMS) Public Electronic Reading Room on the NRC Web site http://www.nrc.gov/reading-rm/adams.html under accession number MLxxxxxxxxx.

Persons who do not have access to ADAMS or who encounter problems in accessing the documents located in ADAMS should contact the NRC PDR Reference staff at 1-800-397-4209, or 301-415-4737, or send an e-mail to pdr@nrc.gov..

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

Backup Slides

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 should 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

Drop

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.

Norbert Carte

Duane A. Hardesty

George Wilson

U.S. Nuclear Regulatory Commission, Office of Nuclear Reactor Regulation

Roger A. Kisner

Michael D. Muhlheim, Ph. D

Oak Ridge National Laboratory

Wednesday, September 14, 2011

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

Purpose

- To discuss
  - the process of developing proposed revisions to NUREG-1537,
  - preliminary results of that development process,
  - concepts for graded and conditional evaluations of updates to digital I&C systems at RTRs, and
  - other issues related to the revision of NUREG-1537 that affect the RTR community.

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

Agenda for Public Meeting September 14, 2011

Time	Topic	Led By
08:00 – 08:10	Opening Remarks	NRC
08:10 – 08:30	Summary of Prior Meeting	NRC
08:30 – 10:00	Proposed Acceptance Criteria Revisions	NRC
10:00 – 10:15	BREAK	
10:15 – 11:15	Proposed Revisions (cont)	NRC
11:15 – 11:45	Invitation for Public Participation	NRC
11:45 – 12:00	Conclusion/Document Actions	NRC

Participant Input from Last Public Meeting June 23, 2011

- Guidance needed
  - When does 10 CFR 50.59 apply to an upgrade?
  - When is a license amendment needed?
- Focus on RTR not NPP needs
- Be more specific in terminology used (e.g., graded rather than risk-informed, difference rather than gap)
- Minimize effort required by RTR applicants
  - Atomic Energy Act of 1954, as amended, states that utilization facilities . . . should be regulated to the minimum extent consistent with protecting the health and safety of the public
- Don't encourage (or force) RTR applicants to use obsolete (analog) technologies
- Convene separate meeting at TRTR conference
- Further discuss the software versus additional regulation issue

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

NUREG-1537 Revision Process

- Review the objectives for revising NUREG-1537 (I&C Systems).
- Review the digital upgrades in the 1990's (historical perspective).
- Develop a structured process that reviews and updates existing guidance for RTRs and incorporates lessons learned from new digital I&C (DI&C) designs and upgrades.
- Prepare a draft to NUREG-1537.
- Hold additional public meetings.

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 analog I&C systems with digital I&C systems, update the guidance for implementing these changes in NUREG-1537,
  - Use the currently available guidance for RTRs to provide an initial foundation, and
  - Leverage the appropriate experience gained in licensing digital I&C systems and upgrades at NPPs by adapting applicable guidance to RTRs.

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

Digital Systems Have a Potential for Unintended Behaviors and Subtle Failure Modes

- The introduction of software and microprocessors could create new failure mechanisms, such as software errors and electromagnetic interference that either were not considered during the initial plant design or not evaluated in sufficient detail in the safety analysis report.

- These failure mechanisms may cause the reactor to malfunction in a way not previously considered. For example, at one facility, after replacing an analog system with a digital system, spikes that were filtered out in the analog system were not filtered out in the digital system, causing a spurious reactor trip. Capacitors were added to solve the new and unexpected failure mode.

There Are Several Unique Characteristics of Digital Technology (1)

- Complexity
  - Finite state machine (digital) vs continuous physical condition (analog)
  - Large number of states and very large number of state transition possibilities characterize all but simplest digital implementations
  - Software execution of function not constrained by physical laws (discontinuous states and unpredictable transitions are possible)
  - High potential for introduction of latent systematic faults

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

There Are Several Unique Characteristics of Digital Technology (2)

- High functional density
  - Multiple functions combined into single module vs specific functions on discrete modules
  - Failure affects multiple functions (one subroutine can service multiple, disparate functions)
- Timing dependencies
  - Sequential (step-by-step) execution of function in recursive loop vs parallel (concurrent) execution of function continuously
  - Deterministic performance difficult to establish both in execution and communication
  - Potential for execution/communication delays and “hung’ performance

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

There Are Several Unique Characteristics of Digital Technology (3)

- Configuration management (CM)
  - High flexible, readily changeable software implementation vs hardwired discrete instrumentation
  - Version control of abstract elements (software, logic) necessary in addition to equipment/part identification
  - Capability to modify in the field or alter functionality remotely requires strict Configuration Management (CM)
- Quality assurance
  - Complex, process-oriented QA for software vs basic, product-oriented QC for hardware
  - Verification and validation complicated by inability to exhaustively test software-based digital systems

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

Some of the Advantages of Digital Technology

- Aging and obsolete analog I&C systems have made the use of digital equipment attractive.
- Analog technology intermixes all noise, distortion, drift, and inaccuracies in the signal path and thus become sources of signal error. In distinction, digital technology represents signals as non-continuous symbols (binary estimates) that are not directly affected by circuit imperfections—noise, distortion, drift, and degradation over time.
- Computers and software are flexible and adaptable.
  - Enhanced features such as automatic self-test and diagnostics.
- Digital communication between separate modules can include many types of information as compared with the limitations of analog technology.

Recent Guidance on Digital I&C Systems was Developed for NPPs, not RTRs

- 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.
  - Although these new requirements are for NPPs, many lessons learned may be applicable/useful to RTRs.
  - There are issues unique to RTRs such as varied power level and diverse design features that will require a more graded approach (i.e., any new guidance cannot be a “one size fits all” approach).

Partial List of Requirements of Interest to DI&C Upgrades

Regulations	Title	Text
10CFR50.2	Definitions – Design bases	Design bases means that information which identifies the specific functions to be performed by a structure, system, or component of a facility, and the specific values or ranges of values chosen for controlling parameters as reference bounds for design.
10 CFR 50.34	Contents of applications; technical information.	Contents of applications; technical information. (a) PSAR (b) FSAR (c) Physical Security Plan (d) Safeguards Contingency Plan
10CFR50.36	Technical specifications.	(c) Technical specifications will include items in the following categories: (1) Safety limits, limiting safety system settings, and limiting control settings. (2) Limiting conditions for operation. (3) Surveillance requirements. (4) Design features. (5) Administrative controls. (6) Decommissioning.
10 CFR 50.55a(a)(1)	Codes and standards.	Structures, Systems, and Components must be designed, fabricated, erected, constructed, tested, and inspected to quality standards commensurate with the importance of the safety function to be performed.
10 CFR 50.59	Changes, tests and experiments.	10 CFR 50.59(c)(2) list eight evaluation criteria.
10 CFR 50.90	Application for amendment of license, construction permit, or early site permit.	. . . fully describing the changes desired, and following as far as applicable, the form prescribed for original applications.
10 CFR 50, Appendix E, I-V	Emergency Planning and Preparedness for Production and Utilization Facilities	I. Introduction II. PSAR III. FSAR IV. Content of Emergency Plans V. Implementing Procedures VI. Emergency Response Data Systems

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

- An understanding of the design, risk, and regulatory differences is necessary to properly adapt regulations and experience from NPPs to RTRs.
  - Because of the lower thermal power level in RTRs, the decay heat is insufficient to cause cladding damage under any cooling condition. Furthermore, the generally intermittent operation results in a significantly smaller inventory of fission products in the fuel.
  - TRIGA-type RTRs have an inherent reactivity insertion safety feature in their design and generate minimal decay heat that precludes damage to the fuel.
- The much lower public risk associated with RTRs has been one of the bases upon which the NRC has accepted that less stringent and less prescriptive measures provide reasonable assurance for the protection of the public, workers, and the environment. This is consistent with the Atomic Energy Act of 1954, as amended, which states that "utilization facilities . . . should be regulated to the minimum extent consistent with protecting the health and safety of the public."

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

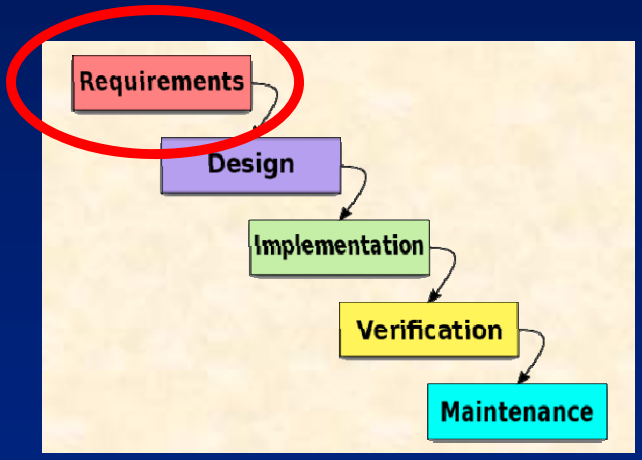
The GA Console and Penn State Reviews Recognized the Level of Risk from RTRs

- 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 reviewers recognized that they were not NPP reviews—this philosophy is being maintained in the update to NUREG-1537.
  - Engineering judgment was used in the reviews because the fuel could not be damaged (i.e., the TRIGAs did not need to meet all of the criteria for NPPs).
  - The initial publication of NUREG-1537 in 1996 captured what was done in the reviews.

The Previous Reviews Noted Deficiencies in the Applications for Digital Upgrades

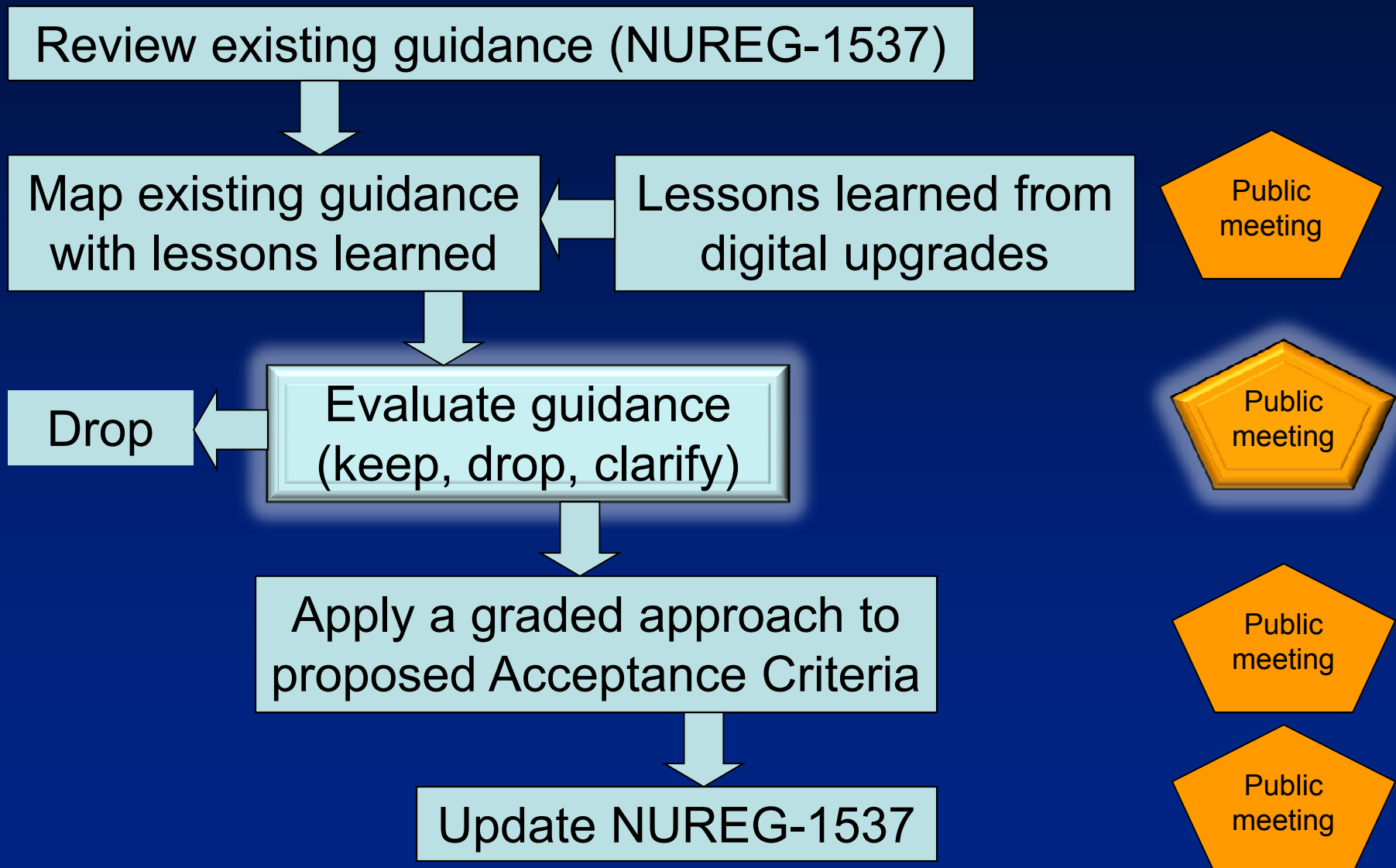
Noted deficiencies (corrected prior to approval)

- 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.



Waterfall model

A Structured Process is Being Used to Modernize Guidance in NUREG-1537



Identification of Lessons Learned

- Assess the similarities and differences between ANSI/ANS 15.15-1978 vs. IEEE Std 603-1991

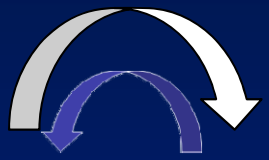
- Identify lessons learned from digital guidance for NPPs (e.g., compare NUREG-1537 vs. NUREG-0800)
  - NUREG-1537 Section 7.3 (RCS) vs NUREG-0800 Section 7.7 (control system)
  - NUREG-1537 Section 7.4 (RPS) vs NUREG-0800 Section 7.2 (RTS)
  - NUREG-1537 Section 7.5 (ESFAS) vs NUREG-0800 Section 7.3 (ESFAS)
  - NUREG-1537 Section 7.6 (console and display) vs NUREG-0800 Section 7.5 (info systems)
  - NUREG-1537 Section 7.7 (rad monitoring) vs NUREG-0800 Section 7.5 (control systems)
  - NUREG-1537 vs NUREG-0800 Section 7.4 (Safe Shutdown Systems)
  - NUREG-1537 vs NUREG-0800 Section 7.6 (Interlocks)
  - NUREG-1537 vs NUREG-0800 Section 7.8 (D3)
  - NUREG-1537 vs NUREG-0800 Section 7.9 (DCS)

- Worksheet for revision to Acceptance Criteria--7.3 RCS
- Worksheet for revision to Acceptance Criteria--7.4 RPS
- Worksheet for revision to Acceptance Criteria--7.5 ESFAS
- Worksheet for revision to Acceptance Criteria--7.6 Control Console and Display
- Worksheet for revision to Acceptance Criteria--7.7 Rad Monitoring Inst

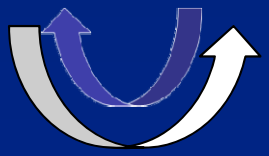
Recent Reviews of Digital Upgrades (GA and Penn State) Followed ANSI/ANS 15.15-1978 (withdrawn). Should the Reviews Follow IEEE Std 603-1991?

- **There are requirements in ANSI/ANS 15.15-1978 that are not in IEEE Std 603-1991**
  - **e.g., fail-safe design vs. single-failure criterion**
- **There are requirements in IEEE Std 603-1991 that are not in ANSI/ANS 15.15-1978**
  - **e.g., Equipment Qualification including qualification and testing of computers and COTS.**
- **There are requirements in IEEE Std 603-1991 that are too restrictive for RTRs**
  - e.g., Clause 5.3 of IEEE Std 603-1991 identifies ANSI/ASME NQA1-1989 as a prescribed QA program.

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

Insights from an Analysis Applied to the RCS shows . . .

- A combined RPS/RCS increases the likelihood of RCS compromising the 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 the failure of the RPS does not lead to greater than negligible risk.
- Need to address the possibility that the RPS/RCS is susceptible to CCFs that could inhibit ability to control while also affecting ability of the protection system.
- Quality hardware and software is necessary to minimize challenges.

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

Insights from an Analysis Applied to the RPS shows . . .

- As expected, the most significant difference is in the criteria 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.

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

Insights from an Analysis Applied to the 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 RTRs compared to NPPs

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

Insights from an Analysis Applied to the 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 (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 and UNNECESSARY criteria on RTRs that were not present in NUREG-1537 (RTRs perform a system check prior to startup and shut down for maintenance). ANSI/ANS 15.15-1978 Clause 5.7.4 already requires audible and visual announcement of any bypass.

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

Insights from an Analysis Applied to the Radiation Monitoring Systems shows . . .

- NUREG-1537 states that "the [Radiation Monitoring] 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." Data communication between the radiation monitoring systems and the RPS should not inhibit the performance of the safety function.

- 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" will be N/A for RTRs.

Prior to Mapping the Lessons Learned, the Acceptance Criteria for RTRs Was Updated

NUREG-1537

- IEEE Std 7-4.3.2-1993, "IEEE Standard Criteria for Digital Computers Systems in Safety Systems of Nuclear Power Generating Stations"
- Regulatory Guide 1.152, Revision 1, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants"
- ANSI/ANS 10.4-1987, "Guidelines for the Verification and Validation of Scientific and Engineering Computer Programs for the Nuclear Industry"
- ANSI/ANS 15.15-1978, "Criteria for the Reactor Safety Systems of Research Reactors"
- ANSI/ANS 15.20 (draft), "Criteria for the Control and Safety Systems for Research Reactors"

Updated Criteria for NUREG-1537

- IEEE Std 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers Systems in Safety Systems of Nuclear Power Generating Stations"
- Regulatory Guide 1.152, Revision 2, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants"
- ANSI/ANS 10.4-2008, "Verification and Validation of Non-Safety-Related Scientific and Engineering Computer Programs for the Nuclear Industry"
- ANSI/ANS 15.15-1978, "Criteria for the Reactor Safety Systems of Research Reactors" (withdrawn)
- ANSI/ANS 15.20 (draft), "Criteria for the Control and Safety Systems for Research Reactors"

The Clauses in IEEE Std 7-4.3.2 and ANSI/ANS 15.15 were Individually Reviewed

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

Updated Criteria For NUREG-1537

- Item 1: range of operation
- Item 2: continuous indication
- Item 3: sensitivity
  .
  .
- IEEE Std 7-4.3.2-2003
- RG 1.152, Rev. 2 (IEEE Std 603-1991)
- ANSI/ANS 15.15-1978
- ANSI/ANS 10.4-2008

Lessons Learned

Expanded Criteria for NUREG-1537

- Item 1: range of operation
- Item 2: continuous indication
- Item 3: sensitivity
  .
  .
- IEEE Std 7-4.3.2-2003, Clause 5.3 Quality
- IEEE Std 7-4.3.2-2003, Clause 5.4 EQ
  .
  .
- IEEE Std 7-4.3.2-2003, Clause 5.15 Reliability
- RG 1.152, Rev. 2 Clause 2.1-2.9
- ANSI/ANS 15.15-1978, Clause 4 Design Basis
- ANSI/ANS 15.15-1978, Clause 5.1 Single Failure
  .
  .
- ANSI/ANS 15.15-1978, Clause 5.7 Bypasses
- ANSI/ANS 10.4-2008

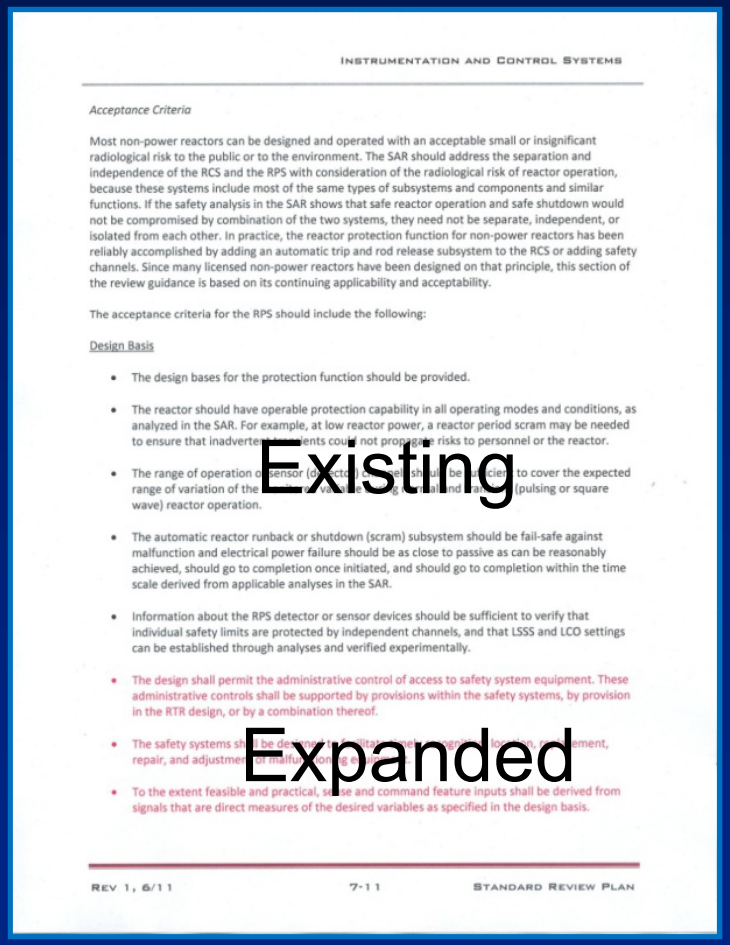
Each Criterion Is Being Individually Evaluated for its Applicability to RTRs

The review of access control should confirm that design features provide the means to control physical access to safety system equipment, including access to test points and means for changing setpoints. Typically such access control includes provisions such as alarms and locks on safety system panel doors, or control of access to rooms in which safety system equipment is located. Review of digital computer-based systems should consider controls over electronic access to safety system software and data. Controls should address access via network connections, and via maintenance equipment.
(Source: ANSI/ANS 15.15, Clause 5.10)
(Source: IEEE Std 603-1991, Clause 5.9)
Comments: NUREG-1537 addresses access control for radiation and experimental areas but not access to I&C components. Access control applies to both analog and digital systems. In addition, access control not only includes physical access to facility but software cyber security. Cyber security for software must be addressed throughout the software life cycle.
Recommendation: KEEP

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

The Collection of Criteria Provides the Basis for the Proposed Acceptance Criteria for the Draft Report

- The revised report will maintain the format and style of NUREG-1537.
- NUREG-1537 will be a stand-alone document. Criteria will be provided in bullet form; standards will primarily be cited as source of additional information.
- A public meeting will be scheduled to evaluate the proposed criteria.



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 [illegible] could not propagate risks to personnel or the reactor.
- The range of operation of sensor (detector) [illegible] should be sufficient to cover the expected range of variation of the [illegible] and [illegible] (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 [illegible] repair, and adjustment [illegible]
- 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

Existing

Expanded

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

Preliminary Results of Proposed of *Acceptance Criteria*

Section	NUREG-1537		Proposed	Drop
	Existing Bullets	Expanded Bullets*	Clarify**	
7.3 RCS	24	2	8	17
7.4 RPS	17	29	22	75
7.5 ESFAS	10	18	12	3
7.6 Control Console and Display	12	3	16	6
7.7 Radiation Monitoring Systems	8	1	15	9
Total	71	53	73	110

*Collected from the review of ANSI/ANS 15.15-1978, IEEE Std 7-4.3.2-2003, and RG 1.152, Rev. 2.
**Based on lessons learned from digital upgrades.

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

RCS

Review Category	Existing Bullets	Expanded Bullets	Proposed
Design Basis	18		3
Effects of Control System Operation/Failures	1		1
Use of Digital Systems	2		1
Environmental Control System	1		
Safe State	1		
Experiment or Experimental Facility	1		
Safety Classification			1
Independence		1	
Potential for Inadvertent Actuation			1
Control of Access		1	
Setpoint Determination/Performance			1
Total	24	2	8

RCS has 8 Proposed Bullets

- Of the 8, 1 is only related to digital systems
  - Guidance for purchase of PLC hardware; embedded and operating systems software, programming tools, and peripheral components
- The other 7 apply to both analog and digital systems
  - Manual and automatic control of process variables
  - EMI/RFI
  - Lightning
  - No reliance on RCS in accident analysis
  - Limit inadvertent actuations and challenges to safety systems
  - High probability of accomplishing safety function in event of AOO
  - Guidance for setpoint analysis methodology and assumptions

Example of Proposed Bullet for the RCS

Proposed Bullet

- Review the electromagnetic environment operating envelopes, design, installation, and test practices that address the effects of electromagnetic interference/radio frequency interference (EMI/RFI), and power surges on I&C systems and components important to safety.

Justification

- *Experience with EMI has indicated that digital electronics may be both a generator of and susceptible to EMI. Interference to a digital input introduces different responses as compared with analog inputs. A digital input, operating in a binary state and expecting a serial sequence, can be spoofed by a burst of interference or blocked for a short period, whereas with an analog input, an interfering pulse may generate a spike simulating a sudden, short-duration temperature or pressure signal. Because of the fundamental differences between analog and digital signal types as well as the differences in internal circuit functioning, specific qualification of digital systems is necessary.*

- *Thus, although NUREG-1537 states that "The RCS should be designed for reliable operation in the normal range of environmental conditions," susceptibility to EMI/RFI should be specifically identified and evaluated.*

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

RPS

Review Category	Existing Bullets	Expanded Bullets	Proposed
Design Basis	5	4	3
Single Failure and Independence	2		2
Testing and Surveillance	4		1
Environmental	1		
Human Factors	3		1
Use of Digital Systems	2	6	11
Quality		2	
Setpoint Determination/Performance		1	
Bypass Permissives		5	
Diversity			1
Data Communications		2	3
Security		9	
Total	17	29	22

RPS has 22 Proposed Bullets

- Of the 22, 15 are only related to digital systems
  - Security vulnerabilities
  - Activities for safety system software (e.g., control, test, documentation)
  - Diversity and defense-in-depth analysis
  - Data communications
- The other 7 apply to both analog and digital systems
  - Timely recognition of malfunctioning equipment
  - EMI/RFI
  - Separation of redundant sensing lines
  - Independence of RPS circuits and safety/nonsafety systems
  - Connections to safety system
  - Testing during operation
  - Consideration of human factors

Example of Proposed Bullet for the RPS

Proposed Bullet

- Redundant instrumentation sensing lines should be routed and protected so that any credible effects (consequences) of any design-basis event that is to be mitigated by signals sensed through those sensing lines should not render any of these redundant sensing lines inoperable unless it can be demonstrated that the protective function is still accomplished. Instrument sensing lines should be routed such that no single failure can cause the failure of more than one redundant sensing line unless it can be demonstrated that the protective function is still accomplished.

Justification

- *Errors can be introduced into sensing and signal lines that are common to multiple systems. Systems utilizing these signals may be redundant safety systems, control systems, or operator displays. Propagation of an erroneous value into these systems can lead to conflicting actions. An example would be that of an erroneous low flux reading, which would be acted on by the control systems to increase reactivity whereas the protection system would see it as a non-threatening condition and not respond. Although not all RTRs would have sensing lines for pressure or chemical sampling, when those are used evolved gases present in the lines have been known to adversely affect readings.*

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

ESFAS

Review Category	Existing Bullets	Expanded Bullets	Proposed
Design Basis	2	5	2
Single Failure and Independence	2	2	1
Quality	1	1	
Testing and Surveillance	2	4	1
Environment	1		
Use of Digital Systems	2	2	3
Completion of Protective Action		1	
Diversity and Defense-in-Depth			1
Setpoint Determination/Performance			1
Control of Access		1	
Repair			1
Identification		1	
Human Factors			1
Reliability			1
Total	18	15	12

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

ESFAS has 12 Proposed Bullets

- Of the 12, 5 are only related to digital systems
  - Environmental qualification of computer-based system
  - EMI/RFI
  - Diversity and defense-in-depth analysis
  - Data communications
  - Effect of software on system reliability
- The other 9 apply to both analog and digital systems
  - Auxiliary features should not degrade safety performance
  - Inputs should be derived from signals that are direct measures
  - Independence between interconnections among division or between systems
  - Setpoint determination methodology should be documented
  - Timely recognition, location, replacement, repair of malfunctioning equipment
  - Human factors should be considered

Example of Proposed Bullet for the ESFAS

Proposed Bullet

- The system timing requirements calculated from design basis events and other criteria should be appropriately allocated to the digital computer portion of the ESFAS and be satisfied in the digital system architectural design. The real-time performance of the ESFAS should include verification that system timing is deterministic or bounded. Time delays within the digital ESFAS and measurement inaccuracies introduced by the digital components should be accounted for in the establishment of the instrumentation setpoints. Timing must be accounted for in system response and verified in testing. Practices should address asynchronous operation of separate modules.

Justification

- *A digital system may exhibit slower (and perhaps faster in some cases) response time from trigger condition to actuation initiation as compared with that of an analog electronic system. The timing difference may allow an increase in process energy (e.g., temperature or pressure) that could increase risk of release or equipment failure. Timing delays may be variable owing to CPU or communication loading or other non-deterministic factors in the system. For this reason, an analysis of timing performance from sensors through actuators including the digital system should be performed. The analysis should be verified by actual testing.*

Control Console and Display

Review Category	Existing Bullets	Expanded Bullets	Proposed
Design Basis	8		6
Design Basis—DI&C			2
Annunciator System	1	1	4
Control of Access	1		
Use of Digital Systems	1	1	2
Safe State	1		
Single Failure			1
BISI			1
Independence		1	
Total	12	3	16

Control Console and Display has 16 Proposed Bullets

- Of the 16, 5 are only related to digital systems
  - The displays and controls should be independent and diverse from the computer-based safety system(s)
  - Communications
  - Timing, quality, and testing
- The other 11 apply to both analog and digital systems
  - HFE principles
  - Manual controls downstream of automatic controls
  - Single-failure criterion to and the physical independence of the electrical power, instrumentation, and control portions of safety-related consoles and display systems
  - Annunciator systems (redundancy, independence, MMI, testability)

Example of Proposed Bullet for the Control Console and Display Systems

Proposed Bullet

- HFE principles and criteria should be applied to the selection and design of the displays and controls. Main Control Room minimum inventory includes the human system interfaces that the operator always needs available to:
  - monitor the status of fission product barriers,
  - perform and confirm a reactor trip,
  - perform and confirm a controlled shutdown of the reactor using the normal or preferred safety means,
  - actuate safety related systems that have the critical safety function of protecting the fission product barriers,
  - analyze failure conditions of the normal human system interfaces (while maintaining the current plant operating condition and power level until the human system interfaces are restored in accordance with applicable regulatory requirements),
  - implement the plant's emergency operating procedures,
  - bring the plant to a safe condition,
  - carry out those operator actions shown to be risk important by the applicant's accident analysis.

Justification

- *Human performance requirements should be described and related to safety criteria. New methods of human interaction are available now that were not prior to modern digital systems. For example, touch screens, which are commonly used in control rooms, can be designed to be clearly understood and reduce the likelihood of operator misoperation. However, without application of good human factors design criteria, the screens can become virtually unreadable and un-navigable.*

Radiation Monitoring Systems

Review Category	Existing Bullets	Expanded Bullets	Proposed
Design Basis	4	1	1
Test and Calibration	2		
Environment	1		
Use of Digital Systems	1		1
Single Failure			1
Display and Recording			11
Human Factors			1
Total	8	1	15

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

Radiation Monitoring Systems has 15 Proposed Bullets

- Of the 15, 1 is only related to digital systems
  - CCF of computer software
- The other 14 apply to both analog and digital systems
  - If signal validation is used, the validity of the indication should be provided as part of the display
  - No single failure should prevent the operators from being presented the information necessary (different from Bullet 2)
  - Display and recording of accident monitoring variables
  - Design of instrumentation to facilitate the recognition, location, replacement, repair, or adjustment of malfunctioning components or modules

Example of Proposed Bullet for the Radiation Monitoring System

Proposed Bullet

- No single failure within either the accident-monitoring instrumentation, its auxiliary supporting features, or its power sources concurrent with failures that are a result of a specific accident should prevent operators from being presented information necessary for them to determine safety status of the plant and to bring the plant to and maintain it in a safe condition following that accident.

Justification

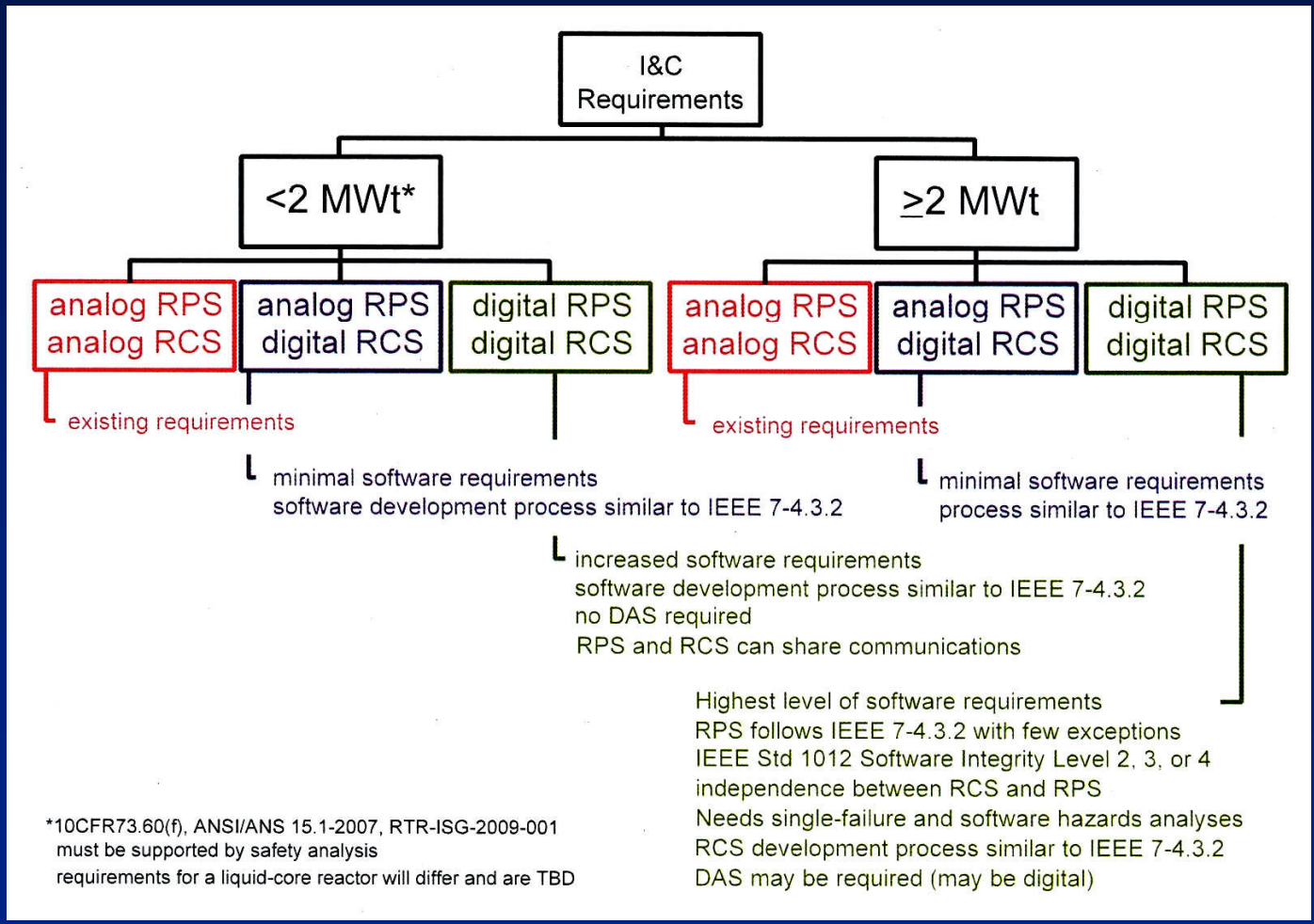
- *Radiation monitoring systems, which provide operators with necessary information to verify functioning of control systems, protection systems, and plant state, should be impervious to single failures. Independent information channels or diverse measurements can be provided to mitigate against the effect of a single failure. This criterion goes beyond the requirement to prevent functioning of the RPS because radiation monitoring systems directly supply operators with information that affects contingency planning.*

The Next Step is to Apply a Graded and Conditional Evaluation to the Proposed Acceptance Criteria

- Graded and conditional evaluations will be applied to the Acceptance Criteria selected from the reviews of NUREG-1537, IEEE Std 7-4.3.2-2003, ANSI/ANS 15.15-1978, RG 1.152, and lessons learned from digital system upgrades and designs.
  - If independence between the RPS and RCS is not required, communications between safety and nonsafety divisions would not be required.
  - If there is only 1 channel, the single-failure criterion would not apply.
- Efforts are underway to determine the software integrity level (SIL) for RTRs and if this SIL applies to all RTRs or there is a different SIL based on a graded approach.
- The need and level of diversity, defense-in-depth, independence, and single-failure criterion is undergoing further review.
  - The GA and Penn State applications maintained an analog scram system.
  - If no redundancy is required, an analysis of diversity and common-cause failure of software is not applicable.

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

A Graded Approach Based on Power Level May Be Used to Separate the Acceptance Criteria



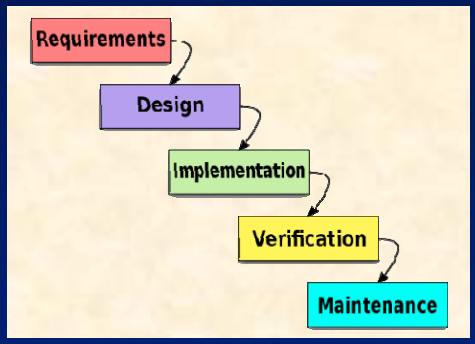
U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Special Topics of Interest in Reviews

- Cyber security
- Experimental system software
- GL 95-02 (Digital Upgrades)

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

- Regulatory Guide 1.152, Rev. 2, presents the waterfall lifecycle phases as a framework for describing specific digital safety system security guidance. The digital safety system development process should address potential security vulnerabilities in each phase of the digital safety system:
  - Concepts;
  - criteria;
  - Design;
  - Implementation;
  - Test;
  - Installation, Checkout, and Acceptance Testing;
  - Operation;
  - Maintenance; and
  - Retirement.



- With respect to control of access, the review should confirm that the data communication system (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.

Cyber Threats are Real

- **Stuxnet** is a computer worm first discovered in June 2009.
- The Stuxnet computer virus had caused problems with the controller handling the centrifuges at the Natanz facilities in Iran.
- Speculation is that the infection may have spread from USB drives (i.e., jumped an air gap)
- The worm initially spreads indiscriminately, but includes a highly specialized malware payload that is designed to target only Siemens Supervisory Control And Data Acquisition (SCADA) systems that are configured to control and monitor specific industrial processes. Stuxnet infects programmable logic controllers (PLCs) by subverting the software application that is used to reprogram these devices.
- While Stuxnet is targeted to Siemens, it or a similar worm could be adapted to other controllers.

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

Experimental System Software

- Software for experimental systems should meet the updated guidelines provided in ANSI/ANS 10.4-2008, "Verification and Validation of Non-Safety Related Scientific and Engineering Computer Programs for the Nuclear Industry."

- If a digital experiment system can scram the reactor (e.g., shorting plugs), this is to be evaluated in the GL 95-02 analysis.

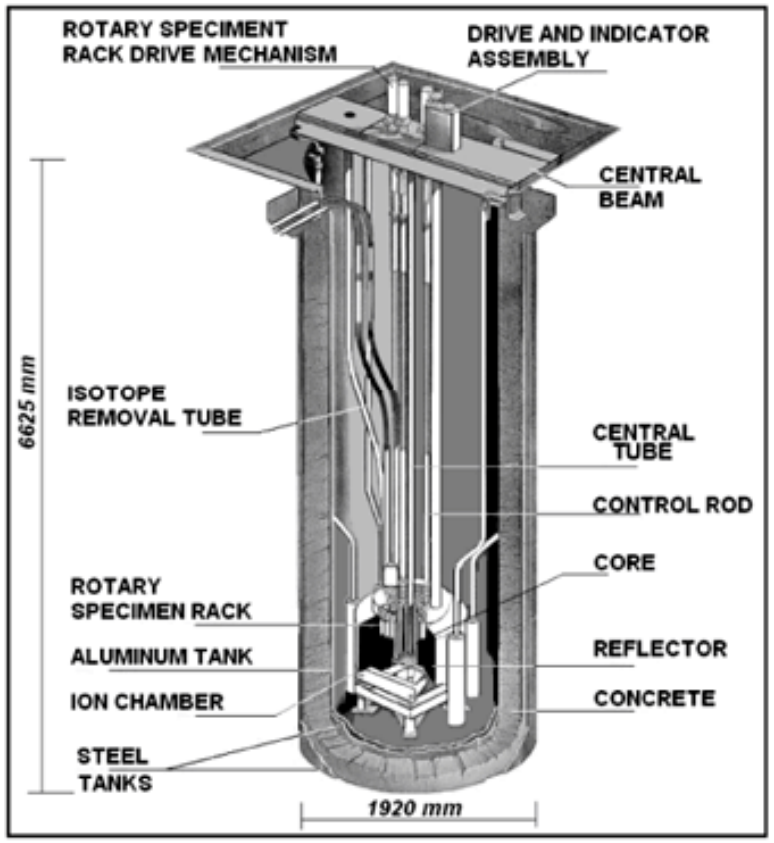


FIG. 1: The pool of the IPR-R1 TRIGA nuclear reactor (courtesy of Dr. A. Z. Mesquita).

Subcommittee for DI&C

- The TRTR Executive Committee is forming two sub-committees,
  - one to work on a new relicensing process for RTRs, and
  - the other for developing regulations and licensing processes for Digital I&C for RTRs.
- The TRTR Executive Committee has asked for 3-5 members from the RTR community to participate in what will likely be monthly meetings at White Flint for about 1-2 years.
- The TRTR Executive Committee is soliciting nominations of individuals to participate on one or both of the committees from the RTR facilities.
  - Please submit nominations for the committees directly to Steve Miller, Chairman of TRTR ("Steve Miller" <sim@simelectronics.com>). If you have any questions, please direct them to Steve Miller.

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

Path Forward

NUREG-1537 Review Issues and Decision Points

- Assess the Existing, Expanded, and Proposed bullets in a future public meeting.
- Discuss the options for a graded approach 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!

This presentation is a publicly available record accessible electronically from the Agencywide Documents Access and Management System (ADAMS) Public Electronic Reading Room on the NRC Web site http://www.nrc.gov/reading-rm/adams.html under accession number ML11249A229.

Persons who do not have access to ADAMS or who encounter problems in accessing the documents located in ADAMS should contact the NRC PDR Reference staff at 1-800-397-4209, or 301-415-4737, or send an e-mail to pdr@nrc.gov..

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

Backup Slides

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

Partial List of Requirements Applicable to the Review of Research and Test Reactors

Document	Topic
10CFR50.2	Definitions – Design bases
10 CFR 50.34	Contents of applications; technical information.
10CFR50.36	Technical specifications.
10 CFR 50.55a(a)(1)	Codes and standards.
10 CFR 50.59	Changes, tests and experiments.
10 CFR 50.90	Application for amendment of license, construction permit, or early site permit.
10 CFR 50, Appendix E, I-V	Emergency Planning and Preparedness for Production and Utilization Facilities
10 CFR 73.60(f)	Additional requirements for physical protection at non-power reactors

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

Partial List of Sources for Review of Research and Test Reactors

Document	Topic
NUREG-1537	Guidelines for Preparing and Reviewing Applications for the Licensing of Non-Power Reactors. Part 1: Format and Content; Part 2: Standard Review Plan and Acceptance Criteria
ANSI/ANS 15.1-2007	Identifies and establishes the content of technical specifications for RTRs. Areas addressed: Definitions, Safety Limits, Limiting Safety System Settings, Limiting Conditions for Operation, Surveillance Requirements, Design Features, and Administrative Controls.
RTR-ISG-2009-001	Interim Staff Guidance on Streamlined Review Process for License Renewal for RTRs
IEEE Std 7-4.3.2	IEEE Standard Criteria for Digital Computers in Safety Systems of NPPs
NUREG 0800	Standard Review Plan for the Review of Safety Analysis Reports for NPPs: LWR Edition
ANSI/ANS 15.15-1978 (Withdrawn)	This standard documents the criteria from which appropriate specific design requirements may be established for the reactor safety system of an individual research reactor.
IEEE Std 603-1991	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	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
R G 1.152, Revision 2	Criteria for Digital Computers in Safety Systems of Nuclear Power Plants
ANSI/ANS 10.4-2008	V&V of Non-Safety-Related Scientific and Engineering Computer Programs
ANSI/ANS 15.20 (draft)	Criteria for the Control and Safety Systems for Research Reactors
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 10CFR50.59

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 should 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.

Each Criterion Is Being Individually Evaluated for its Applicability to RTRs—Example of a "DROP"

- The capability of a safety system to accomplish its safety function shall be retained while sense and command features equipment is in maintenance bypass. The review of bypass and removal from operations should be coordinated with the organization responsible for reviewing technical specification format and content to confirm that the provisions for this bypass are consistent with the required actions of the proposed plant technical specifications.
  (Source: IEEE Std 603-1991, Clause 6.7)
  Comments: Maintenance bypass may not be used at an RTR. Research reactors are operated continuously, with scheduled shutdowns for refueling, changing samples in the flux trap, and performing any corrective or preventive maintenance, etc. Before startup after maintenance, tests are performed to assure operability. For example, channel tests of sensor operability and channels not included elsewhere in the technical specifications that are identified in the SAR, the ventilation system, and electrical system are typically tested quarterly and before startup after maintenance.
  Recommendation: DROP .