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

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

Michael D. Muhlheim, Ph.D.

Oak Ridge National Laboratory

September 25, 2012

Agenda for Public Meeting September 25, 2012

Time	Topic	Led By
03:00 – 03:05	Opening Remarks	NRC
03:05 – 03:15	Summary of Prior Meetings	NRC
03:15 – 04:15	Discuss Comments on RCS Draft	NRC
04:15 – 04:25	BREAK	
04:25 – 05:15	Proposed Revisions (continued)	NRC
05:15 – 05:25	Invitation for Public Participation	NRC
05:25 – 05:30	Conclusion/Document Actions	NRC

NRC's Objective—To Update and Enhance the Available Guidance on Reviewing Digital I&C Systems for NPRs

- Objective
  - Update the guidance in NUREG-1537 to ensure the quality and uniformity of reviews
    - increase clarity of guidance for upgrading existing analog I&C systems with digital I&C systems
    - reflect applicable current positions on nonpower reactor I&C systems
    - maintain consistency with the Atomic Energy Act of 1954, as amended
- Approach
  - Adapt the currently available guidance for NPRs to provide an initial foundation, and
  - Review the experience gained in licensing digital I&C systems and upgrades at NPPs and use it for adapting applicable guidance for NPRs.

Purpose of Today's Public Meeting (September 25, 2012)

- To discuss
  - the proposed draft of the NUREG-1537*
    - Part 1—Format and Content
    - Part 2—Acceptance Criteria
  - other issues related to the revision of NUREG-1537 that affect the NPR community

*The proposed draft Sections for Chapter 7 will be reviewed

Participant Input from the June 23, 2011 Public Meeting (ML112092676)

- Guidance is needed on when 10CFR50.59 applies to an upgrade and when a license amendment request needed
- Minimize effort required by NPR applicants
- Focus on NPR not NPP needs
- Risk-informed and gap imply a PRA and deficiency. More appropriate terms are graded-approach and differences
- Don’t encourage (or force) NPR applicants to use obsolete (analog) technologies by making digital more onerous
- Convene separate meeting at TRTR conference

Participant Input from the September 14, 2011 Public Meeting (ML11249A229)

- Provide slides and Acceptance Criteria "bullets" in advance of meeting
- Number the "bullets"
- IEEE Std 7-4.3.2-2003 specifies SIL Level 4 in IEEE Std 1012-1998. What SIL Level is applicable for NPRs?
- Explain the breakpoint for the graded approach
- EMI/RFI is listed as "digital" in control console and display systems but "digital/analog" in RCS, RPS, and ESFAS
  – EMI/RFI is applicable to both digital and analog I&C systems (sensitivities to EMI/RFI and consequences of failure are different)

Participant Input from the June 21, 2012 Public Meeting (ML121390143)

- Rather than repeat guidance and criteria in each section, move this to one section (e.g., the front end of Ch. 7)
- Explain the breakpoint for the graded approach; separation by power level would be beneficial
- Consider providing a yes/no table that identifies the guidance for the different types of facilities based on power level
- Consider adding more "If required by the SAR analysis."

Participant Input from Public Comments

- Insufficient time for comments
- Text in Part 1 should not be repeated in Part 2
- Provide the regulatory basis
- Description and analysis of software should be in a separate Section
- GL 95-02 should be replaced with RIS 2002-22
- Numerous comments were on existing text

Current NUREG-1537

- What it covers
  - – The traditional control panels, with their assorted gauges, indicating lights, control switches, annunciators, etc.
  - – Application of IEEE Std 7-4.3.2-1993 and RG 1.152, Rev. 1 to all hardware and software in all systems

Updated NUREG-1537

- Developments from maturity of review process
  - How the systems function, operate, and interact with other systems (high-level functions)
  - Human Factors Engineering
  - Fundamental differences between analog and digital introduce new or increased susceptibilities

- New Acceptance Criteria for digital I&C
  - Communications within and between systems
  - Software requirements, development, and implementation
  - EMI/RFI (increased sensitivity)
  - Cyber security

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

This goal of this update to NUREG-1537 is to clarify NRC guidance for complying with existing requirements for nonpower reactors.

Few Explicit Requirements for NPRs

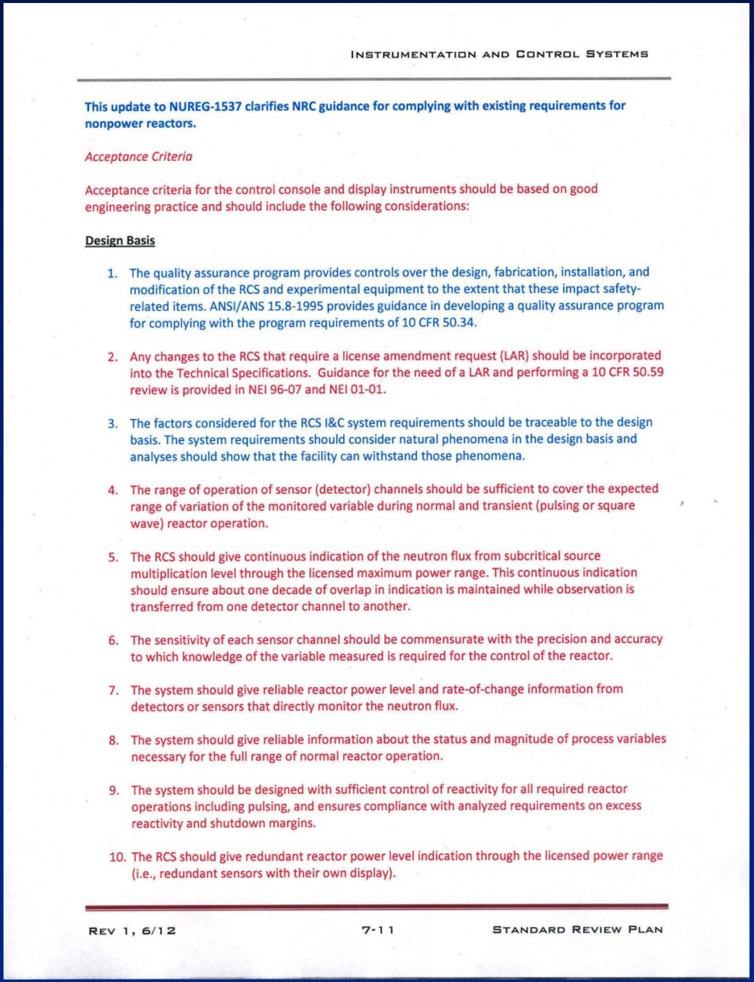
- Regulatory Basis
  - – Explicit—10CFR50.34, 55(a); 10CFR20
  - – Derived—the regulations state that the principle design criteria must be in the SAR, but not what these criteria are. The actual criteria and plant specific events are the derived regulatory basis
- Regulatory Basis is applicable to ALL facilities
  - – Difference in size of NPRs is 4 x 10^6 (5W to 20MW)
  - – Difference in size of NPPs is 2–3 times.

NUREG-1537 Provides Guidance to Meet Regulatory Basis

- Level of detail in Regulatory Basis
  - General
    - General requirements are more flexible to change
    - NRC can be as specific as necessary in the application of general requirements and must be consistent in its application
  - Specific
    - specific requirements are difficult to change (e.g., rulemaking is required to change 10CFR50.49, EQ)
    - detailed requirements constrain NRC and licensees
- Solution
  - Because explicit requirements are typically not detailed, Acceptance Criteria are used to provide detailed guidance

The Update to NUREG-1537 Will Enhance the Quality and Uniformity of Reviews

- The updated report will preserve the current format and style of NUREG-1537
  - Format and Content will be provided in Part 1
  - Acceptance Criteria will be provided in Part 2
- Goal is to ensure clarity and to maintain consistency with the AEA of 1954, as amended



INSTRUMENTATION AND CONTROL SYSTEMS

This update to NUREG-1537 clarifies NRC guidance for complying with existing requirements for nonpower reactors.

Acceptance Criteria

Acceptance criteria for the control console and display instruments should be based on good engineering practice and should include the following considerations:

Design Basis

1. The quality assurance program provides controls over the design, fabrication, installation, and modification of the RCS and experimental equipment to the extent that these impact safety-related items. ANSI/ANS 15.8-1995 provides guidance in developing a quality assurance program for complying with the program requirements of 10 CFR 50.34.
2. Any changes to the RCS that require a license amendment request (LAR) should be incorporated into the Technical Specifications. Guidance for the need of a LAR and performing a 10 CFR 50.59 review is provided in NEI 96-07 and NEI 01-01.
3. The factors considered for the RCS I&C system requirements should be traceable to the design basis. The system requirements should consider natural phenomena in the design basis and analyses should show that the facility can withstand those phenomena.
4. The range of operation of sensor (detector) channels should be sufficient to cover the expected range of variation of the monitored variable during normal and transient (pulsing or square wave) reactor operation.
5. The RCS should give continuous indication of the neutron flux from subcritical source multiplication level through the licensed maximum power range. This continuous indication should ensure about one decade of overlap in indication is maintained while observation is transferred from one detector channel to another.
6. The sensitivity of each sensor channel should be commensurate with the precision and accuracy to which knowledge of the variable measured is required for the control of the reactor.
7. The system should give reliable reactor power level and rate-of-change information from detectors or sensors that directly monitor the neutron flux.
8. The system should give reliable information about the status and magnitude of process variables necessary for the full range of normal reactor operation.
9. The system should be designed with sufficient control of reactivity for all required reactor operations including pulsing, and ensures compliance with analyzed requirements on excess reactivity and shutdown margins.
10. The RCS should give redundant reactor power level indication through the licensed power range (i.e., redundant sensors with their own display).

REV 1, 6/12 7-11 STANDARD REVIEW PLAN

The Update is a Stand-Alone Document

NUREG-1537

- 298 pages
  - 40 pages text (Part 1 and 2)
  - 32 pages Penn State and GA SE reviews
  - 166 pages cited or implied standards
  - 60 pages guidance on 50.59 review

NUREG-1537 (Update)

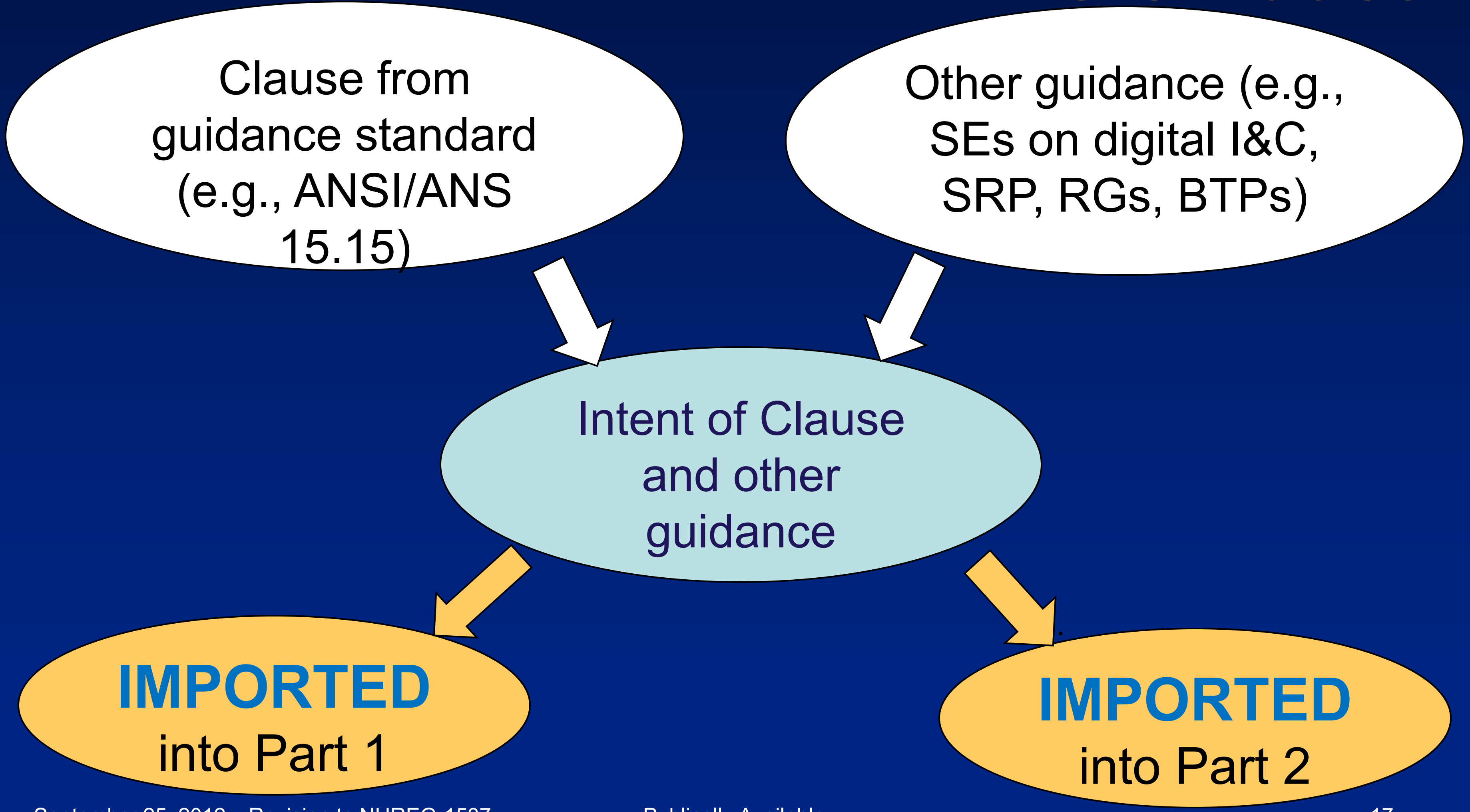
- 347 pages
  - 105 pages text (Part 1 and 2)
  - 24 pages cited standards
  - 178 pages guidance on 50.59 review

- NUREG-0800
  - ~ 427 pages in SRP
  - ~1273 pages guidance
  - ~5000 pages Standards

Background for Developing Proposed Acceptance Criteria

- **UNCHANGED**
  - **Red text provides existing text or acceptance criterion from NUREG-1537 (any modification to existing criterion is in blue).**
- **IMPORTED**
  - **Derived from expanding existing guidance documents to the clause level (e.g., ANSI/ANS 15.15-1978, Clause XX) and importing the intent of the clause.**
- **CLARIFICATION**
  - **Derived from Format and Content in Part 1 or Evaluation Findings in Part 2 without a corresponding Acceptance Criteria.**
- **NEW**
  - **Guidance based on lessons learned from digital I&C upgrades, industry standards, etc.**

Example of How Imported Acceptance Criteria (AC) Were Added



Clause from guidance standard (e.g., ANSI/ANS 15.15)

Other guidance (e.g., SEs on digital I&C, SRP, RGs, BTPs)

Intent of Clause and other guidance

IMPORTED into Part 1

IMPORTED into Part 2

Example of How Clarifying Acceptance Criteria (AC) Were Added

- Area of Review (Part 2)

  Radiation measurements at a reactor facility may be used for reactor diagnostic or safety purposes.

- If the radiation measurements are used for safety purposes, the basis for display characteristics should be based on an analysis of the system functions required to respond to an accident and the tasks required of the operator to implement those functions.

  Acceptance Criteria

  Verify that the display characteristics for accident monitoring variables were established based on results of an analysis of the system functions required for accident response and the operator-executed tasks required for those functions during design basis accidents.

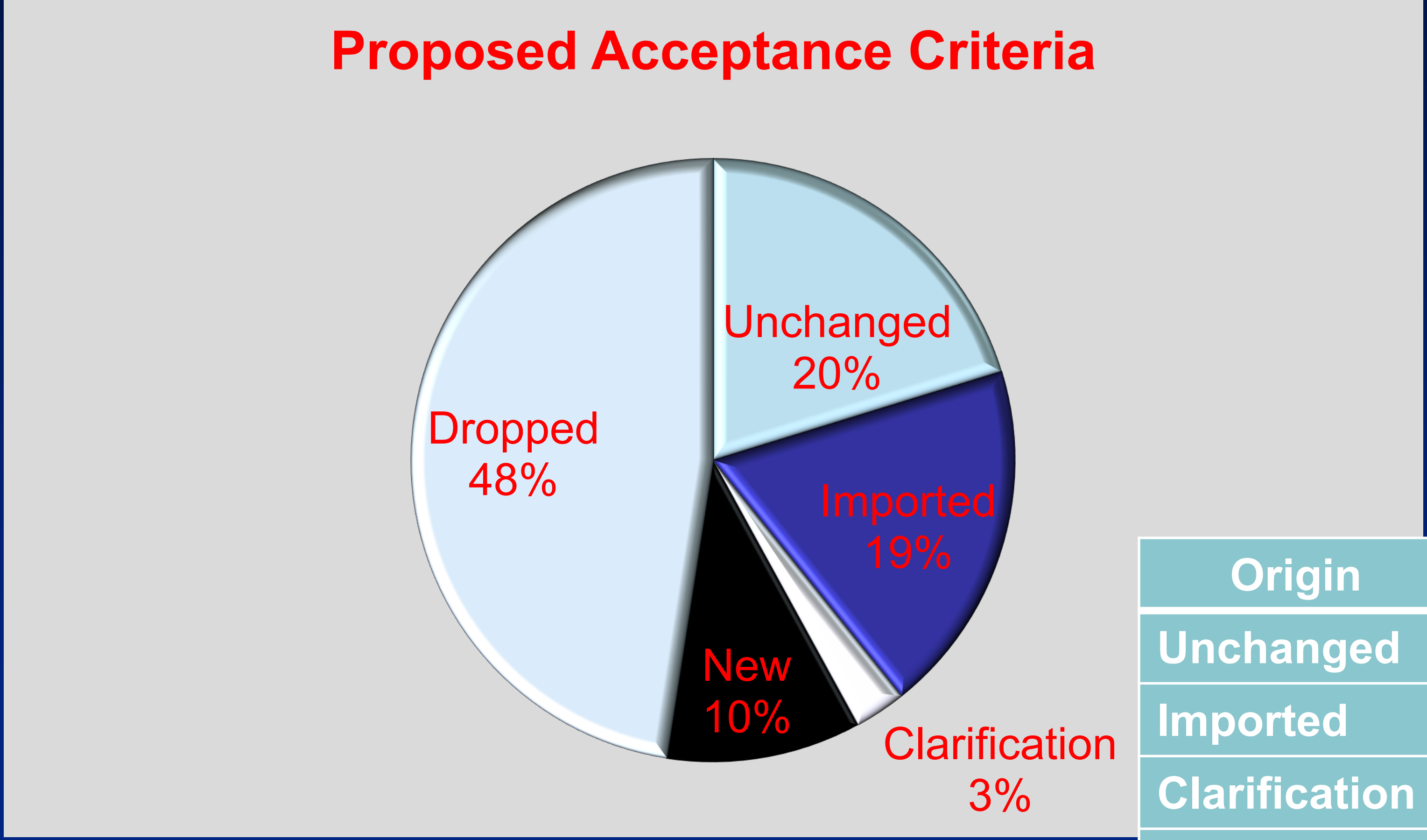
Example for How NEW Acceptance Criteria Were Added

- Unchanged
  - Sensitivity of sensor channel commensurate with precision and accuracy of variable measured
- Imported
  - Administrative controls for changing setpoints
- New
  - Setpoints based on documented analysis
  - Margin exists between setpoints and safety limits

Example of a “Drop”

- The system design, installation, testing and maintenance of the Lightning Protection System should be addressed. The secondary effects of lightning discharges to safety-related I&C systems. [Low-level power surges and EMI/RFI are addressed in RG 1.180].
- (Bases: RG 1.204, IEEE Std. 665-1995, IEEE Std. 666-1991, IEEE Std. 1050-1996, IEEE Std. C62.23-1995)
- Comments: The design and installation of lightning protection systems is to assure that electrical transients resulting from lightning phenomena do not render I&C systems important to safety inoperable or cause spurious operation of such systems. NUREG-1537, Section 8.1 (AC bullet #4) states that “electrical power circuits should be isolated sufficiently to avoid electromagnetic interference with safety-related instrumentation and control functions.” In general NPRs are designed for fail-safe shutdown by a reactor scram in the event of the loss of offsite electrical services. **NUREG-1537 already states this in Ch. 7 and Ch. 8.**
- Recommendation: __DROP____

Proposed Acceptance Criteria

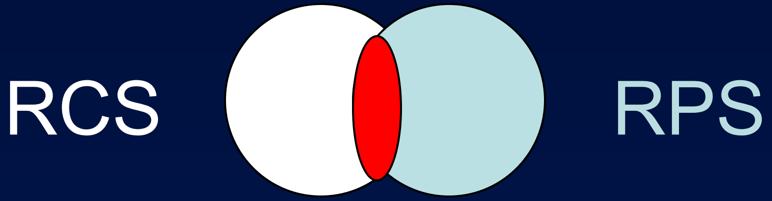


Origin	Number
Unchanged	66
Imported	62
Clarification	9
New	34
Dropped	154

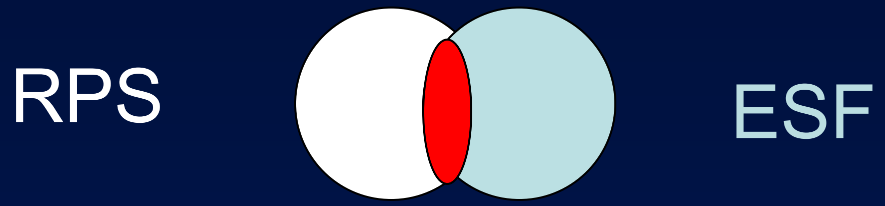
Summary of Revisions to Guidance

- Because NUREG-1537 already addresses the following design criteria, few Acceptance Criteria were added for these topics:
  - Independence
  - Diversity
  - Quality
  - Redundancy
  - Testability

- New or Imported guidance that was added for digital I&C systems include:
  - Determinism (timing)
  - Software



- At first glance, it may appear that there is duplication in the Acceptance Criteria. Consider the independence of the RCS and RPS:
  - The RCS “view” for independence is between nonsafety/safety
  - The RPS “view” is between channels (i.e., within the RPS)
- Example of why independence is reviewed in both RCS and RPS Sections
  - The RPS must be able to operate properly given a failure of the RCS
  - The isolation devices between the RPS and RCS are based on certain assumptions. Thus, the properties of the isolation devices (e.g., voltage) on the RCS side need to match the input assumptions to RPS.
  - If a modification is being implemented that only affects the RCS, the review should confirm that the modification does not violate the design basis of the RPS.



Duplication of Guidance Was Removed if Appropriate

- 8 AC for RPS software:
  - Development (1)
  - Implementation (5)
  - Requirements specifications (1)
  - Reliability goals (1)
- 3 AC for ESF software:
  - Development (1)
  - Requirements specifications (1)
  - Reliability goals (1)

Most of the Guidance for Digital Systems Was Imported (i.e., Already Existed)

- Software has 8 AC (7 Imported, 1 New)
  - Requirements specifications (NEW)
  - Development
  - Implementation
    - V&V
    - Configuration management
    - Software risk management
    - Identification (software– hardware match)
    - Testing
  - Reliability measures

Section 7.6, Control Console and Display Systems

- Alarms and Annunciators
  - Clearly show status (UNCHANGED)
  - Failures properly evaluated (NEW)
  - Are reliable and do not introduce a credible CCF (CLARIFYING)
  - Tests include annunciators (NEW)
  - Alarms for which no automatic control is provided should be reviewed for quality and reliability (NEW)

Section 7.7, Radiation Monitoring Systems

- Display and recording
  - Display characteristics based on accident response (CLARIFYING)
  - Operators should be able to easily discern information for use under accident conditions (NEW)
  - Means are provided to monitor and access the magnitude of any radioactive releases (NEW)
  - If information is essential it should be continuously displayed (NEW)
  - Signals from effluent radioactivity monitors and meteorology monitors are recorded for future use (NEW)

50.59 Review

- Guidance for a “50.59” review is in a new Section—Section 7.2.6 in Part 1
- EPRI TR-102348, Rev. 1/NEI 01-01 (EPRI 1002833), provides suitable guidance both for designing a digital replacement and for determining whether it can be implemented under 10 CFR 50.59 without prior staff approval
- Although not all digital equipment replacement usage will automatically result in an unreviewed safety question, it is likely that digital modifications to safety-significant systems such as the RPS or ESF actuation system will require staff review

If Approved for an NPP it is Approved for an NPR

- If a simple component (no digital communication) has been approved for use under an Appendix B program for a nuclear power plant, it is good enough to be used at an NPR and screened out under a 50.59 review. However, the 8 questions in 10CFR50.59 must still be answered to address if the replacement introduces a new failure mode. (The simple components use must be consistent with the original use.)

Items that Require Input from Stakeholders

- ANSI/ANS 15.15-1978 (withdrawn)
- Offsite radiation monitors
- Restructure with systems and topics
  - Sections 7.3–7.7 will still cover systems
  - Proposed Appendix would cover the following topics:
    - Use of digital systems
    - Access control
    - Cyber security

We Want Your Comments

- We appreciate the comments
  - Sometimes what is clear to us is not clear to stakeholders
  - Some of the Acceptance Criteria are more appropriately placed in a different design criteria “bin”
  - Coverage of generic information

Path Forward

- Make Chapter 7 an ISG
- Address stakeholder comments
  - 75 day comment period
- Update NUREG-1537
  - Incorporate ISGs for License renewal and Licensing of isotope production facilities

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 **ML12261A328**.

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..

Backup Slides

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

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 research reactors. 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 7-4.3.2-2003	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 3	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
RIS 2002-22	NRC Regulatory Issue Summary 2002-22 Use of EPRI/NEI Joint Task Force Report, “Guideline on Licensing Digital Upgrades: EPRI TR-102348, Revision 1, NEI 01-01: A Revision of EPRI TR-102348 to Reflect Changes to the 10 CFR 50.59 Rule”

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

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

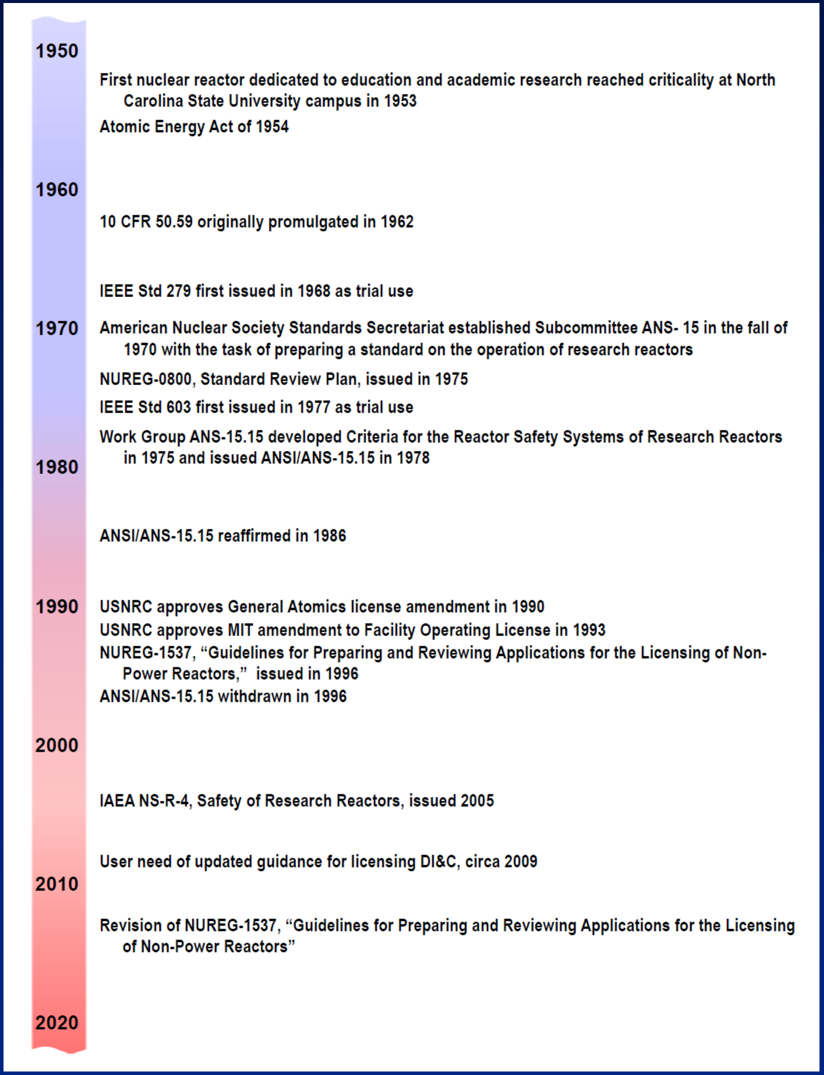
V&V Activity	Software Integrity Level			
	1	2	3	4
Component V&V test plan and test procedure generation	🟦	X	X	X
Concept documentation Evaluation	🟦	X	X	X
Configuration management Assessment	🟩	🟩	X	X
Contract verification			🟨	X
Criticality analysis	X	X	X	X
Hardware/software/user requirements allocation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

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

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

Origin of NUREG-1537 and Licensing Reviews for NPRs

- GA and Penn State submitted applications to install new digital I&C systems (circa 1990)
- NUREG-1537 was not available for currently licensed NPRs
- The GA and Penn State reviews were based on power reactor guidelines
- NUREG-1537, written after the fact, reflects lessons learned in the GA and Penn State reviews (published 1996)



First nuclear reactor dedicated to education and academic research reached criticality at North Carolina State University campus in 1953

Atomic Energy Act of 1954

10 CFR 50.59 originally promulgated in 1962

IEEE Std 279 first issued in 1968 as trial use

American Nuclear Society Standards Secretariat established Subcommittee ANS- 15 in the fall of 1970 with the task of preparing a standard on the operation of research reactors

NUREG-0800, Standard Review Plan, issued in 1975

IEEE Std 603 first issued in 1977 as trial use

Work Group ANS-15.15 developed Criteria for the Reactor Safety Systems of Research Reactors in 1975 and issued ANSI/ANS-15.15 in 1978

ANSI/ANS-15.15 reaffirmed in 1986

USNRC approves General Atomics license amendment in 1990

USNRC approves MIT amendment to Facility Operating License in 1993

NUREG-1537, "Guidelines for Preparing and Reviewing Applications for the Licensing of Non-Power Reactors," issued in 1996

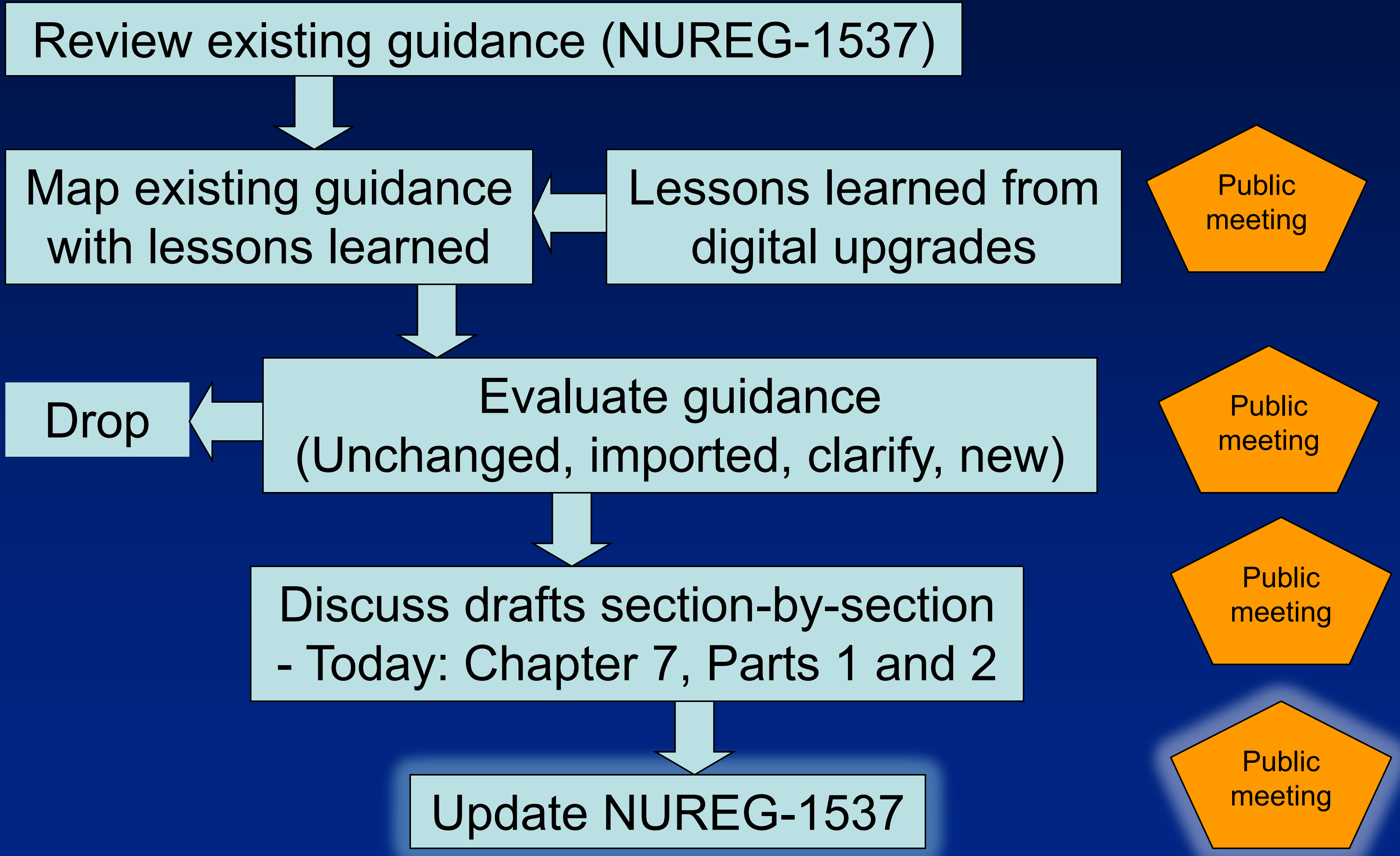
ANSI/ANS-15.15 withdrawn in 1996

IAEA NS-R-4, Safety of Research Reactors, issued 2005

User need of updated guidance for licensing DI&C, circa 2009

Revision of NUREG-1537, "Guidelines for Preparing and Reviewing Applications for the Licensing of Non-Power Reactors"

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



Review existing guidance (NUREG-1537)

Map existing guidance with lessons learned

Lessons learned from digital upgrades

Public meeting

Evaluate guidance (Unchanged, imported, clarify, new)

Drop

Public meeting

Discuss drafts section-by-section - Today: Chapter 7, Parts 1 and 2

Public meeting

Update NUREG-1537

Public meeting

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

Results of Proposed of *Acceptance Criteria*

Section	NUREG-1537		Proposed		
	Unchanged	Imported	Clarify	New	Dropped
7.3 Reactor Control System	24	5	1	4	24
7.4 Reactor Protection System	14	21	4	10	86
7.5 ESFAS	9	18	0	7	8
7.6 Control Console and Display	11	11	0	7	17
7.7 Radiation Monitoring Systems	8	7	4	6	20
Total	66	62	9	34	155

Distribution of AC

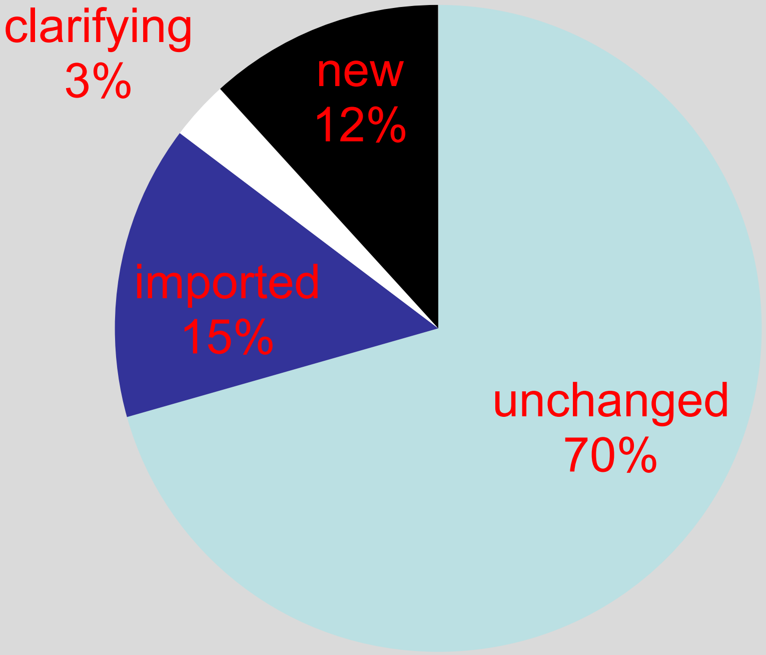
	RCS	RPS	ESF	Console	RMS
Design basis	19	13	9	10	7
Design criteria					
Single failure		2	2		2
Independence	2	4	2	2	1
Equipment qualification		2	1		
Prioritization of functions		1		1	
Fail-safe design	1		1		
Effects of Control System failures	2				
Setpoints		4	2		
Operational bypass		2	3		
Maintenance bypass	2	2			
Completion of protective actions			1		
Surveillance	3	3	4	3	3
Classification and identification		1	1		
Human factors considerations		3	1	1	1
Display and recording					5
Annunciators				5	
Quality	2	2	2	1	1
Use of digital systems	1	8	3	4	4
Access control	1	1	1	1	
Cyber security	1	1	1	1	1
	34	**49**	**34**	**29**	**25**

Distribution of NEW AC

	RCS	RPS	ESF	Console	RMS
Design basis	2	2	3	4	1
Design criteria					
Single failure					
Independence		1			
Equipment qualification		2	1		
Prioritization of functions					
Fail-safe design					
Effects of Control System failures	1				
Setpoints		2	1		
Operational bypass					
Maintenance bypass		1			
Completion of protective actions					
Surveillance					
Classification and identification					
Human factors considerations			1		1
Display and recording					4
Annunciators				3	
Quality	1	1	1		
Use of digital systems		1			
Access control					
Cyber security					
	4	**10**	**7**	**7**	**6**

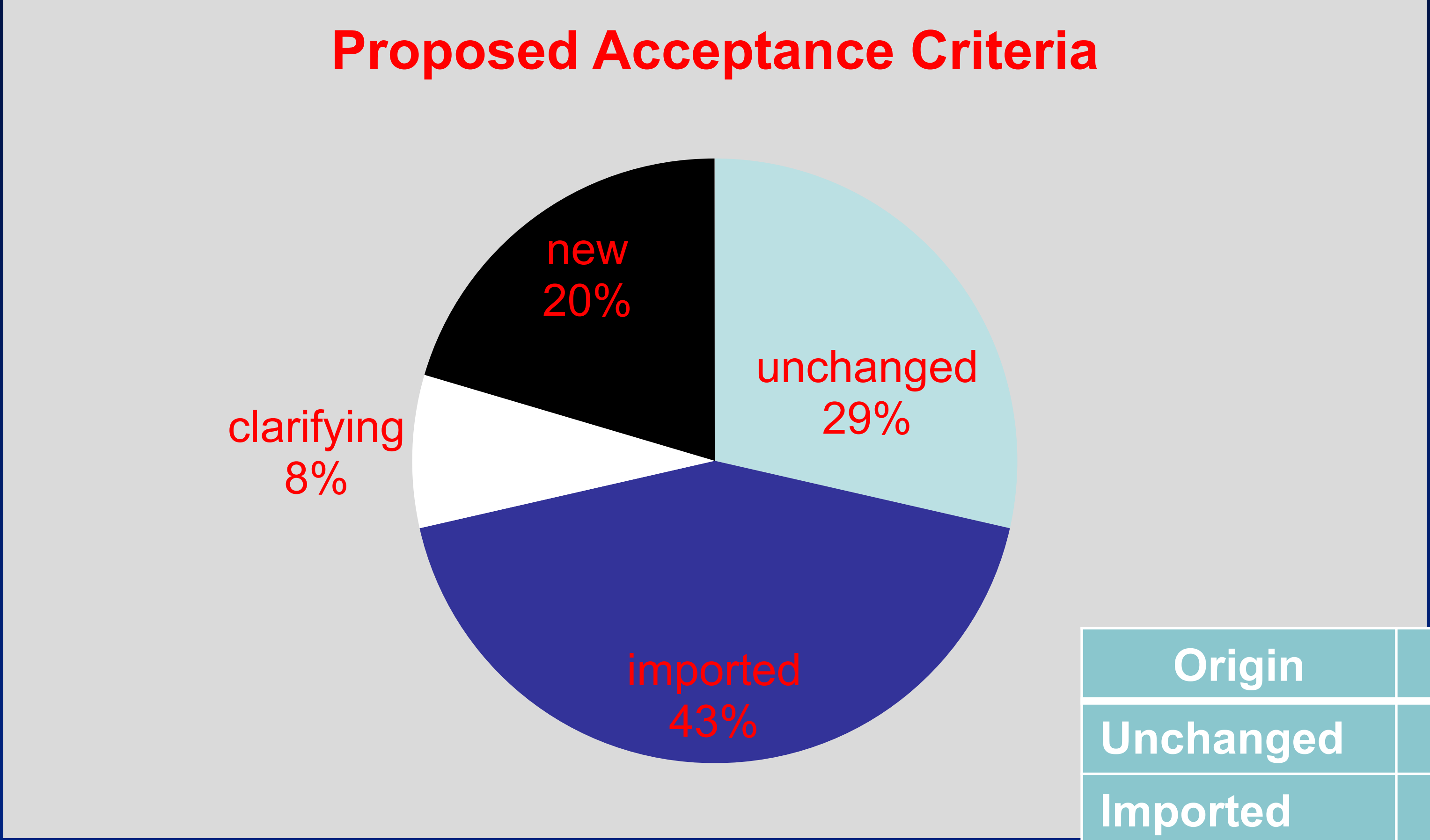
RCS

Proposed Acceptance Criteria



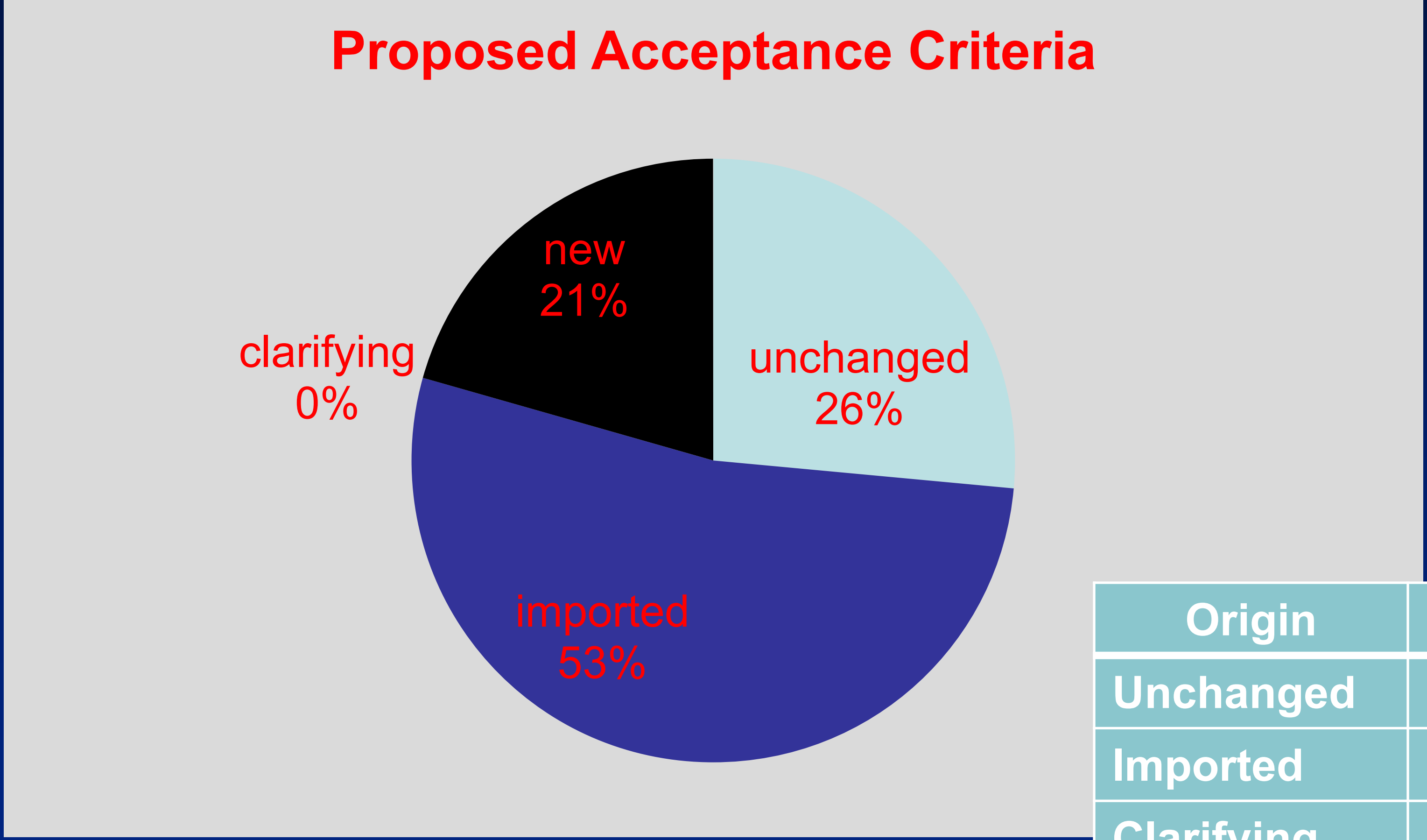
Origin	Number
Unchanged	24
Imported	5
Clarifying	1
New	4

RPS



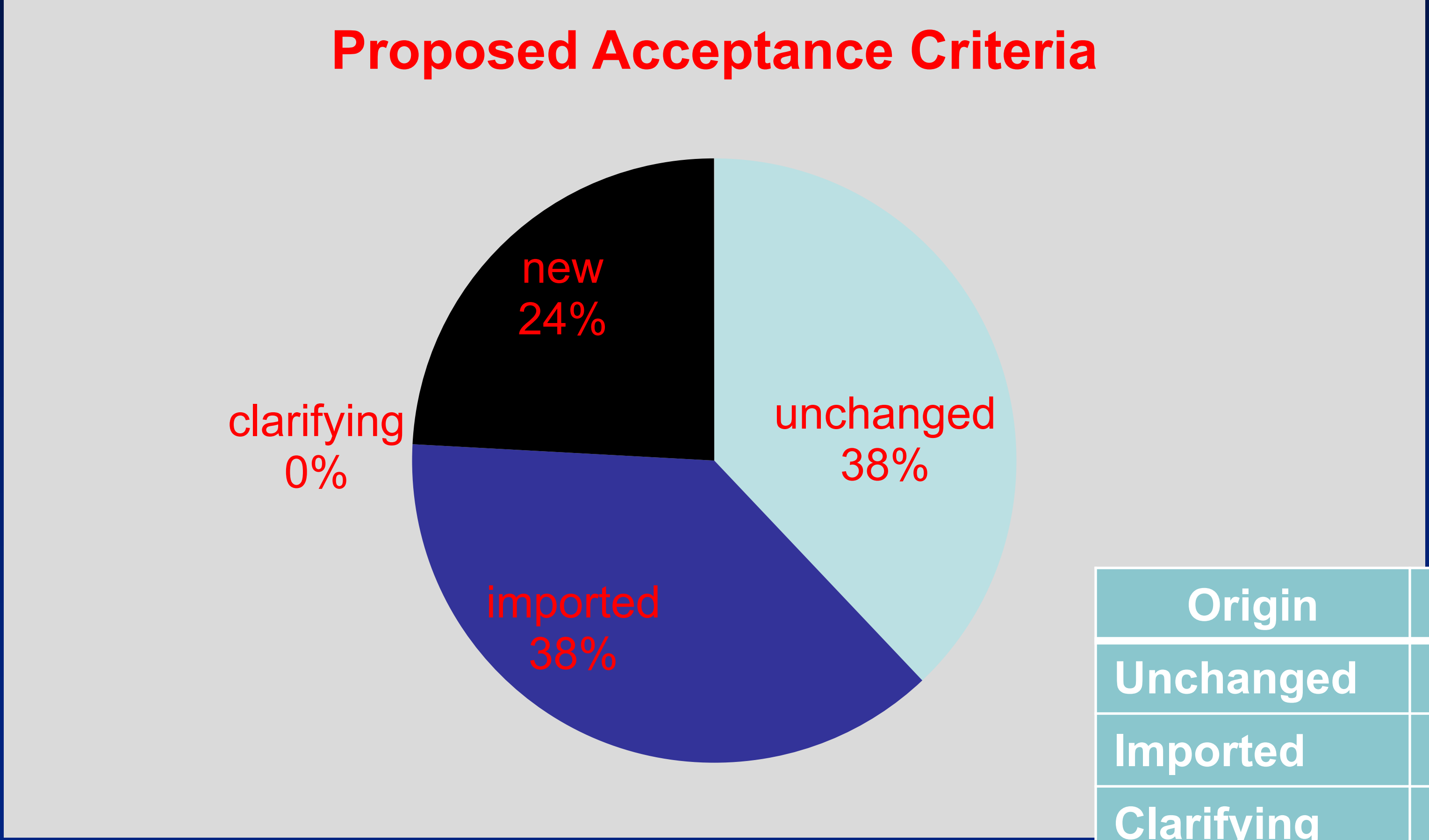
Origin	Number
Unchanged	14
Imported	21
Clarifying	4
New	10

ESF



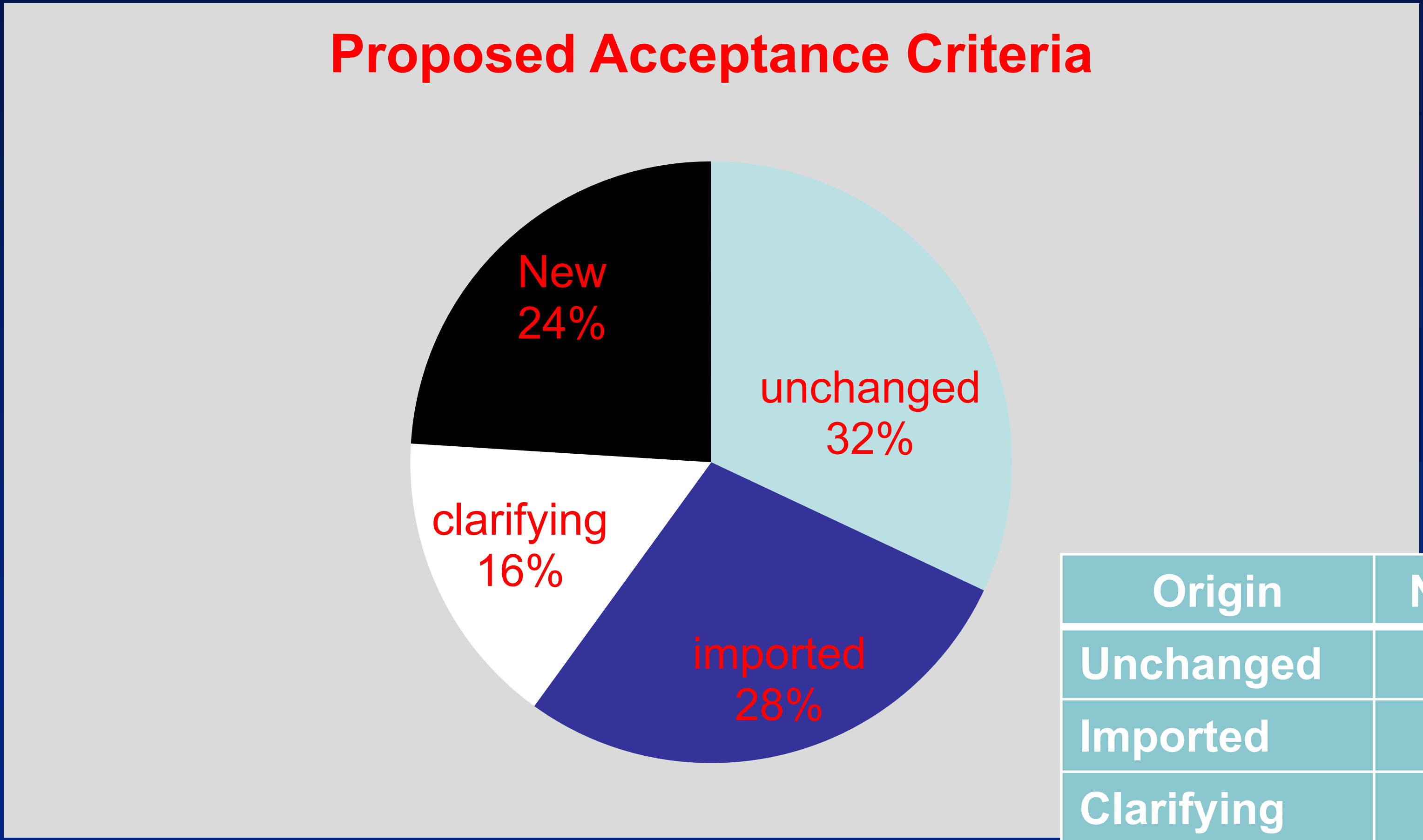
Origin	Number
Unchanged	9
Imported	18
Clarifying	0
New	7

Control Console and Display



Origin	Number
Unchanged	11
Imported	11
Clarifying	0
New	7

Radiation Monitoring Systems



Origin	Number
Unchanged	8
Imported	7
Clarifying	4
New	6

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

Reactor Control System

Review Category	Unchanged	Imported	Clarifying	New
Design Basis	16		1	2
Independence		2		
Fail Safe	1			
Effects of Control System Operation/Failures	1			1
Operational Bypass	2			
Surveillance	3			
Quality		1		1
Use of Digital Systems	1			
Access Control		1		
Cyber Security		1		
Total	24	5	1	4

RCS has 4 Proposed New Acceptance Criteria

- Verify that all interfaces between the RCS and RPS have been properly identified and addressed, thereby preserving the reliability, redundancy, and independence requirements of the RPS.
- Verify that the control system includes the necessary features for manual and automatic control of process variables within prescribed normal operating limits. Functionality, which is included beyond the necessary minimum, should be reviewed to verify that unintended consequences of any added feature have been considered.
- Verify that any mitigation of the Maximum Hypothetical Accident or potential accidents analyzed in Chapter 13 of the SAR do not rely on the operability of the reactor control system function to assure safety.
- Verify that the licensee’s QA program provides controls over the design, fabrication, installation, and modification of the RPS and experimental equipment to the extent that these impact safety-related items. For RTRs, the licensee may use the guidance of ANSI/ANS 15.8-1995, as endorsed by RG 2.5, in developing a quality assurance program for complying with the program requirements of 10 CFR 50.34, subsections (a)(7) and (b)(6)(ii).

RPS

Review Category	Unchanged	Imported	Clarifying	New
Design Basis	7	2	2	2
Single Failure	1		1	
Independence	1	2		1
Equipment Qualification				2
Prioritization of Functions		1		
Setpoints	1	1		2
Operational Bypass		2		
Maintenance Bypass		1		1
Surveillance	2	1		
Classification and Identification		1		
Human Factors	2		1	
Quality		1		1
Use of Digital Systems		7		1
Access Control		1		
Cyber Security		1		
Total	14	21	4	10

September 25, 2012 – Revision to NUREG-1537 Publically Available 52

RPS has 10 Proposed New AC

- Verify 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.
- Verify that system timing requirements calculated from the maximum hypothetical accidents and other criteria have been allocated to the digital computer portion of the system as appropriate, and have been satisfied in the digital system architectural design. In addition, verify that the installed systems perform as predicted and appropriate measurement and analysis techniques have been used to compensate for the uncertainties introduced by certain design and implementation practices, such as the use of interrupts.
- Verify that the protocol selected for the data communications meet the performance requirements of all supported systems. This review should also include verification that data communications for the RPS system timing is deterministic or bounded. Verify the protocol implementations conform to validated protocol specifications by formally generated test procedures and test data vectors and that the implementations themselves were constructed using a formal design process that ensures consistency between the product and the validated specification. Verify that no unexpected performance deficits exist that could adversely affect the proposed RPS architecture.
- Verify that the specifications on the I&C are within the bounds of the normal range of environmental conditions.
- Verify that the effects of EMI/RFI and power surges on safety-related I&C systems, including computer-based digital systems are adequately addressed.
- Verify that the setpoints for an actuation of the RPS are based on a documented analysis methodology that identifies assumptions and accounts for uncertainties, such as environmental allowances and measurement / computational errors associated with each element of the instrument channel. The analysis parameters and assumptions should be consistent with the safety analysis, system design basis, technical specifications, facility's design, and expected maintenance practices.
- Verify that an adequate margin exists between setpoints and safety limits, such that the system initiates protective actions before safety limits are exceeded.
- If the safety analysis shows that the RPS/RCS should be separate systems, verify that the licensee has shown that there are barriers isolating the RPS and RCS systems or that the combined system is a safety-related system. Any isolation devices should assure that credible failures in the connected nonsafety or redundant channels will not prevent the safety systems from meeting their required functions.
- Verify that the licensee's QA program provides controls over the design, fabrication, installation, and modification of the RPS and experimental equipment to the extent that these impact safety-related items.
- Verify that the functional characteristics for the software requirements specifications are properly (and precisely) described for each requirement.

ESFAS

Review Category	Unchanged	Imported	Clarifying	New
Design Basis	3	3		3
Single Failure	1	1		
Independence		2		
Equipment Qualification				1
Fail Safe	1			
Setpoints		1		1
Operational Bypass		3		
Completion of Protective Actions		1		
Surveillance	2	2		
Classification and Identification		1		
Human Factors				1
Quality	1			1
Use of Digital Systems	1	2		
Access Control		1		
Cyber Security		1		
Total	9	18	0	7

ESFAS has 7 Proposed New AC

- Verify that the ESF inputs are derived from signals that are direct measures of the desired variables as specified in the design basis or that the indirect parameters are a valid representation of the desired parameters.
- Verify that any auxiliary features that are part of the ESF actuation systems by association do not inhibit the performance of the safety function of the ESF actuation systems.
- Verify that the system timing requirements calculated from design basis accidents and other criteria are appropriately allocated to the digital computer portion of the ESF actuation systems and be satisfied in the digital system architectural design. The real-time performance of the ESF actuation systems should include verification that system timing is deterministic or bounded. Time delays within the digital ESF actuation systems and measurement inaccuracies introduced by the digital components should be accounted for in the establishment of the instrumentation setpoints. Timing should be accounted for in system response and verified in testing. Practices should address asynchronous operation of separate modules.
- Verify that the effects of EMI/RFI and power surges on safety-related I&C systems, including computer-based digital systems are adequately addressed.
- Verify that the setpoints for an ESF actuation are based on a documented analysis methodology that identifies assumptions and accounts for uncertainties, such as environmental allowances and measurement / computational errors associated with each element of the instrument channel. The analysis parameters and assumptions should be consistent with the safety analysis, system design basis, technical specifications, facility design, and expected maintenance practices.
- Verify that human factors were considered at the initial stages and throughout the design process to assure that the functions allocated in whole or in part to the operator(s) can be successfully accomplished to meet the safety system design goals.
- Verify that the quality assurance program provides controls over the design, fabrication, installation, and modification of the ESF actuation systems and experimental equipment to the extent that these impact safety-related items.

Control Console and Display

Review Category	Unchanged	Imported	Clarifying	New
Design Basis	4	2		4
Independence	1	1		
Prioritization of Functions		1		
Surveillance	2	1		
Human Factors	1			
Annunciators	1	1		3
Quality		1		
Use of Digital Systems	1	3		
Access Control	1			
Cyber Security		1		
Total	11	11	0	7

Control Console and Display has 7 Proposed New AC

- Verify that the displays and controls provided for manual system-level actuation and control of safety equipment should be functional under conditions which may require manual actions.
- Verify that any remote shutdown stations or monitors are secure and that their failure does not prevent safe reactor shutdown.
- Verify that those manual controls that are connected to safety equipment are connected downstream of digital I&C safety system outputs (i.e., as close to the actuation device without any intervening logic).
- Verify that the functional characteristics of the display and control digital components are sufficient to provide operators with the information needed to place and maintain a facility in a shutdown condition.
- Verify that hardware and software failures were evaluated in assessing the reliability of annunciators used to support normal and emergency operations.
- Verify that the system/channel surveillance tests include the annunciators and displays and that the tests satisfy the technical specification requirements.
- Verify that those alarms for which no automatic control is provided meet same the requirements of the control console, display instruments, and equipment.

Radiation Monitoring Systems

Review Category	Unchanged	Imported	Clarifying	New
Design Basis	4		2	1
Single Failure	1		1	
Independence		1		
Surveillance	2	1		
Human Factors				1
Display and Recording			1	4
Quality		1		
Use of Digital Systems	1	3		
Access Control				
Cyber Security		1		
Total	8	7	4	6

Radiation Monitoring Systems has 6 Proposed New AC

- Verify that the applicant properly developed and maintains the display criteria documentation for the accident monitoring variables.
- Verify that the selection, type, location, and display of radiation monitoring system variables were determined considering human factors analyses.
- Verify that those accident monitoring variables associated with fuel failures or breach of a fission product barrier are uniquely identified with a characteristic designation so that the operator can easily discern information intended for use under accident conditions.
- Verify that variables monitored used in determining and continuously assessing the magnitude of radioactive material release.
- Verify that the displays essential for operator action provide direct or immediate trend or rate information. Trend information essential for operator action should be being continuously available on dedicated trend displays and selectively available on other displays that provide redundancy. Those essential display systems should have the capability of providing at least 30 minutes of data and have recording capability.
- Verify that those measured variables that pertain to accomplishing or maintaining critical safety functions, those needed for manual control, those needed for determining fuel breach magnitude, and those that can be used in determining the magnitude of radioactive release are recorded for future use. Data recording may be continuously updated, stored in electronic memory, and displayed on demand with the capability for at least 30 minutes of pre-event and 12 hours of post-event logging .