Status of I&C ISG

Interim Staff Guidance for Chapter 7, Instrumentation and Control Systems, of NUREG-1537

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Comments on draft ISG

- The ISG was published for comments in the Federal Register from Nov. 16, 2015 to Feb. 1, 2016.
- Comments were received from 15 individuals and organizations.
  - Anonymous commenter
  - Ohio State University – A. Kauffman and S. White
  - Penn State University – J. Turso and M. Trump
  - Purdue University – C. Townsend
  - Reed College - M. Krahenbuhl
  - Shine Medical Technologies – J. Barteime
  - TRTR – J. Jenkins
  - National Institute of Standards and Technology – T. Newton
  - University of California Irvine – G. Miller
  - University of Florida – D. Cronin
  - University of Massachusetts at Lowell – L. Bobek
  - University of Texas at Austin – P. Whaley
  - US Geological Survey – T. DeBey

Comments on draft ISG (Continued)

- We appreciate the stakeholder comments that were provided on the draft ISG to replace Chapter 7 of NUREG-1537.
- The comments have been beneficial in revising the draft and will result in a more useful document.

Highlights of comments and actions

- Access control, cyber security, and digital upgrades, addressed in Subsections 7.3-7.7 in the draft ISG, will be combined in Section 7.2.
- Design criteria will be renumbered with a 1-to-1 mapping between Part 1 and Part 2 (e.g., 7.3-1).
- Applicable Regulatory basis will be better identified:
  - 10CFR50, Domestic Licensing of Production and Utilization Facilities
  - 10CFR55, Operators' Licenses
  - 10CFR73, Physical Protection of Plants and Materials

Highlights (continued)

- Unanalyzed failure modes have occurred in digital upgrades, including the replacement of "simple" monitors.
  - Guidance for 50.59 reviews is being further considered.
- The current ISG allows a graded approach based on safety evaluations.
  - Each licensee is responsible to identify the criterion applicable to their facility based on their safety evaluations.
  - This will be clarified in the revised ISG.

Contents of ISG

- The current ISG does not address counterfeit parts, which will be addressed in the updated report.
- The majority of the criterion in the draft ISG are derived from the existing guidance contained in NUREG-1537
  - ANSI/ANS 15.15,
  - IEEE Std 7-4.3.2,
  - RG 1.152,
  - etc.

Contents of ISG (Continued)

- A small number of criterion were added as guidance to support the Evaluation Findings.
- For example, four (4) criterion were added to Section 7.3 (RCS) to support the following Evaluation Findings:
  - The RCS is designed to maintain planned control for the full range of normal reactor operations.
  - The RCS was designed so that any single malfunction in its components would not prevent the RPS from performing necessary functions, or would not prevent achieving a safe shutdown condition of the reactor.
  - There is reasonable confidence that the RCS will function as designed.

Example Design Criterion

Number	Design Criterion
7.3-16	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.
7.3-18	Verify that the RCS 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.
7.3-23	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 RCS function to assure safety.
7.3-30	Verify that the licensee's QA 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. 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).

Commission Direction

- SRM to SECY-15-0106 (ML16156A614)
  - Commission disapproved staff rulemaking recommendation (IEEE 603)
  - Develop plan to modernize I&C regulatory infrastructure
  - Stakeholder interaction
  - "to reach a common understanding of the digital I&C regulatory challenges, priorities, and potential solutions to address them"
  - continue meaningful interaction through implementation of the plan

Integrated Action Plan

- Largely focused on Power Reactors
  - But, affects Non-power facilities
- Near-Term Topics (generally within 2 years)
- Prioritize and implement the regulatory activities needed to provide near-term regulatory clarity and support industry confidence to perform DI&C upgrades
- Position on Common Cause Failure
- Incorporating DI&C using the 10 CFR 50.59 Process
- Commercial Grade Dedication of Digital Equipment

IAP – 50.59 Process

- Per NEI 96-07 Rev. 1 as endorsed by RG 1.187
  - Applicability
    - TS Changes require a LAR
    - Excludes changes controlled by other more specific requirements
  - Screening
    - Is the activity a change to the facility or procedures as described in the FSAR (as updated)?
    - Is the change a adverse?
    - Is the activity a test or experiment not described in the FSAR (as updated)?
  - Evaluation
    - Address the eight questions in 10 CFR 50.59 (c)(2)

IAP – Commercial Grade Dedication of Digital Equipment

- Evaluation of third-party certification of digital hardware and software
  - Independent, third-party certification has been effective in some other industries.
  - The use of this process either alone or in conjunction with the CGD process could reduce the scope of digital systems reviews that the staff need to complete
- NRC will need to evaluate this concept and any policy implications that it may have

IAP – Modernization of the I&C Regulatory Infrastructure

- Assessment for Modernization of the I&C Regulatory Infrastructure.
  - Objectives
    - Provide near-term regulatory clarity
    - Support industry confidence to perform DI&C upgrades
    - Broadly evaluate current I&C regulatory infrastructure
    - (licensing review experiences, research efforts, operating experience, other safety-critical industries, & international perspectives)
    - identify and prioritize the improvements to modernize the regulatory infrastructure over the longer term in light of evolving approaches to I&C.

U.S.NRC

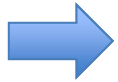
United States Nuclear Regulatory Commission

Protecting People and the Environment

QUESTIONS ?

Number of criteria for review by reference in NUREG-1537 (2-96)

Citation	Number of criteria for review
Average number of individual criteria in each subsection	13
ANSI/ANS 10.4-1987	26
ANSI/ANS 15.15-1978	35
ANSI/ANS 15.20 (draft)	44
ANSI/ANS 15.8-1976 (RG 2.5)	44
ANSI/ANS 15.4-1988	7
IEEE 7-4.3.2-1993	14
IEEE 279/603 (RG 2.2)	49
RG 1.152, Rev. 1	17
Criteria listed in Part 1 or Part 2	9
GL 95-02	2
NUMARC/EPRI TR-102348	Many
RG 2.2	5
Total per section	265+



Gaps in criteria based on advances in technology

Criteria No.	Criteria
7.3-18	the RCS should include the necessary features for manual and automatic control
7.3-22	mitigation of the MHA or potential accidents analyzed in Chapter 13 should not rely on the operability of the RCS to assure safety
7.4-12	a single failure should not cause the failure of more than one sensing line unless it can be shown that the protective function would still be accomplished
7.4-14	redundant safety system channels (or divisions) should be independent
7.4-19	safety system setpoints should be based on a documented analysis methodology
7.5-13	safety system setpoints should be based on a documented analysis methodology
7.6-8	any remote shutdown stations or monitors should be secure and their failure would not prevent safe shutdown of the reactor
7.6-9	manual controls that are connected to safety equipment should be connected downstream of digital I&C safety system outputs
7.6-10	the displays and controls should provide the operator with sufficient information to place and maintain a facility in a shutdown condition
7.6-12	data transmittal to remote displays should be protected by one-way communication
7.6-20	hardware and software failures should be included in assessing the reliability of annunciators used to support normal and emergency operations
7.6-22	system/channel surveillance tests should include annunciators and displays
7.6-23	alarms without automatic control should meet the same requirements of the control console, display instruments, and equipment