As of: 2/5/16 1:33 PM
Received: February 01, 2016
Status: Pending_Post
Tracking No. 1k0-8npt-2ond
Comments Due: February 01, 2016
Submission Type: Web

PUBLIC SUBMISSION

Docket: NRC-2012-0167
Draft NUREG for Comment

Comment On: NRC-2012-0167-0011
Preparing and Reviewing Licensing Applications for Instrumentation and Control Systems for Non-power Reactors; Draft NUREG for Comment

Document: NRC-2012-0167-DRAFT-0015
Comment on FR Doc # 2015-29029

(6)

Submitter Information

Name: Mark Trump
Address:
101 Breazeale Reactor
The Pennsylvania State University
University Park, PA, 16802-2304
Email: mat16@psu.edu

11/16/2015
80 FR 70850

General Comment

See attached file(s)

Attachments

Final PSU comments on Draft ISG NUREG 1537 Docket ID NRC–2012–0167

PENNSTATE

MARK A. TRUMP
Associate Director for Operations
Radiation Science and Engineering Center
The Pennsylvania State University
101 Breazeale Nuclear Reactor
University Park, PA 16802-2304

Phone: (814) 865-6351
Fax: (814) 863-4840
E-mail: mat16@psu.edu

RADIATION SCIENCE & ENGINEERING CENTER

U.S. Nuclear Regulatory Commission
Washington, DC 20555-001

January 31, 2016

SUBJECT: Comments regarding draft ISG NUREG 1537 Docket ID NRC–2012–0167

The Penn State Breazeale Reactor appreciates the opportunity to comment on the draft Interim Staff Guidance (ISG) for NUREG 1537 which updates Chapter 7 regarding instrumentation and control license applications/amendments for Non-Power Utilization Facilities (NPUF).

PSU understands this is generic guidance to be used with future initial Safety Analysis Reports (SAR) and License Amendment Request's (LAR) for a broad range of possible projects. This complicates both the document and the review as the reader must attempt to discern what *may be* applicable to existing licensee's amendment request. The same problem may exist for the NRC staff reviewer. The comments presented in this letter are bias toward the existing licensee submitting an amendment or renewal request.

The draft ISG represents a massive increase in requirements and if issued and used as written will ensure that most facilities will never update their antique failing instrumentation with digital replacements. Indeed few if any instrumentation upgrades that require an LAR will occur. One of our major concerns is that NUREG 1537 is interpreted and used as if it were rule. While NRC management maintains that this is only a guidance document and it provides "one method to meet the regulation," in practicality, absent other firm direction, NUREG 1537 is and will continue to be *the regulation* enforced by the staff. This existing practice can be seen in the recent license renewal process and is reinforced by staff comments like "if the NUREG asks 483 questions, the licensee needs to provide 483 answers".

The ISG promulgates additional "design basis" requirements that go well beyond the scope of digital upgrade guidance and are not to our knowledge derived from promulgated regulation. Many are good engineering practices for complex digital systems controlling dangerous processes; others are simply power reactor design criteria that have been added to the ISG design listing. This appears to be an out of process method of promulgating a 10CFR50 "Appendix A like" set of general design criteria for NPUFs. Examples include: automatic

bypass functions; environmental qualification; physical, electrical and communications separation; train separation; cyber security process and program requirements. While the stated position is these items are not "requirements"; how many LAR RAIs will be issued until the licensee has justified why each and every item is not applicable to their facility or a proposed upgrade?

We assert that the actual health and safety consequences to the public from NPUFs (or lack of consequences) are not adequately represented in the basis of the ISG or in the current review processes used for NPUF LARs. This bias is evident in words like "large risk" and "undue threat to public safety" when talking about digital system failures. We assert the NRC has not done a credible assessment of NPUF accident consequences and overestimates the public health and safety risk of our facilities and underestimates the safety benefits of modern digital system integration when compared to the antique, obsolescent, and increasingly unreliable analog technology now being employed at most NPUFs. The low (but not incredible) probability of a software common cause failure (SCC) occurring to create a yet unimagined accident scenario that is not bounded by the Maximum Hypothetical Accident (MHA) belies our engineering understanding of the risks associated with low power, low temperature reactors. For most (if not all) NPUFs there is no credible mechanism for the instrumentation system to create a beyond MHA event just as there is no credible mechanism for the MHA itself.

Additionally, we assert that the stated conclusion that any essentially any digital upgrade creates an "un-reviewed safety question" and requires a LAR is not adequately justified and we request additional public meetings to further explain the basis of this position.

Finally, part 1 of the draft does not appear to be a finished product but rather one in the development process. The ISG seeks to be a stand-alone document that includes digital guidance and bring all "issues to address" (the draft ISG refers to these as requirements) into one convenient document while simultaneously having each sub-section (RPS, RCS, RMS) stand alone for amendment request purposes. We appreciate the stand-alone concept, but many items appear to requirements from source documents without full evaluation and rewording to NPUF terminology and philosophy. The result is a verbose highly repetitive document with lists of "requirements" that will be nearly unusable for an initial submittal (or renewal) and confusing to the licensee seeking a subsection or system level LAR. Additionally, much of the added "guidance" is training level discussion that is poorly worded and difficult to discern what the "issue to address" actually is. Some sentences are repeated verbatim in the same or adjacent paragraphs and important concepts are missing or obscured (see attached table for examples). This leads the reviewer to conclude that part 1 needs to be critically proofread for content, clarity and implementation structure. It is not ready for publication. Part 2 of the document is much better written, more concise, and appears usable

as written (although I do not necessarily agree with all the content). Many of the criteria in part 1 appear unaddressed in the part 2 review; therefore including these criteria in the SAR at the level described in part 1 is unreasonable and unwarranted. Issuance of part 1 in its current form will stall instrumentation upgrades at all but the most well-resourced facilities.

In closing I would restate the obvious; there are still difficult philosophical and technical issues in digital upgrades that the NRC and licensees need to work thorough to revise NUREG 1537. As we hand these facilities over to a new generation of research/operators and new regulators we need to incorporate as much historic knowledge and lessons learned as possible. Both the NRC and the current NPUF licensees need to devote the resources necessary to get this done correctly. A well designed, well-reasoned, usable product will be cost effective for all involved. A poorly done document increase confusion, delay needed system upgrades, and further threaten the continued viability of the Nation's civilian held research reactors.

Sincerely,

Mark A. Trump
Associate Director for Operations

Cc – Electronic:
K. Ünlü
T. Litzinger
D. Hardesty - NRC

Number	1537 text (partial/paraphrased)	Comment	Suggestion
1.	Part 1 General comment	The document contains many items to consider that appear to be a compilation of good engineering practices as well as time honored nuclear traditions. These are presented in the form of requirements the licensee must address. Please provide context or relate the items to the 10CFR50. If the basis is just to provide the NRC with "reasonable assurance" then I would presume that many of the comments resolutions will likely be delegated to "Information the staff deems necessary to provide reasonable assurance that the facility is safe." This philosophical regulatory issue is beyond the scope of this document review and I would find a comment response of "Necessary for reasonable assurance" a reasonable response.	
2.	P1 The format and content guide and the standard review plan (SRP) are intended to be used as a comprehensive and integrated document that provides the reviewer with guidance that describes methods or approaches that the NRC staff has found acceptable for meeting NRC requirements.	As written part 1 is not yet ready to be used as a format and content guide. The document needs a thorough proof-read, redundancies removed, content clarified and requirements referenced. If it is to be used it must be overhauled. In an earlier conceptual discussion, some Risk based filtering was to be applied for different plant designs (principally along power level and pulsing design). This seems reasonable in both part 1 and part 2. I am sure that it was applied to reduce the number of requirements, but not to segregate them. A useful document from early in the process was a table listing the part 1 requirements with the part 2 review criteria. Is this where the numbers in the part 1 left column come from? Another document listed source of the requirement. These auxiliary documents answer many questions and if updated these developmental references would be of use to both the licensee and the staff in the future.	Rework part 1, strip out "good ideas" (or label them as for as such) and half-baked discussion left overs, clean up/standardize language, review and eliminate obvious power reactor requirements, verify that material presented as requirements have some legal basis and reference source "requirements", cross reference part 1 and part 2, eliminate or explain number in the left side column

Number	1537 text (partial/paraphrased)	Comment	Suggestion
3.	This ISG is not a substitute for NRC regulations and compliance with the ISG is not required. The approaches and methods in this ISG are provided as an acceptable means to meet the NRC regulations. Methods different from those described in this final ISG should provide a basis for the staff to make a determination that an applicant is able to meet NRC regulations.	Given the lack of regulation to support the specified design criteria, this seems legally correct, practically moot. The NRC uses this as a requirement guide. Therefore the content of this guide needs to be highly scrutinized. It is evident part 1 has not received that level of scrutiny. Part 1 needs rework. The guide really contains a lot of good design considerations....things to consider in designing a system. Each of these things does not need to be analyzed described, reported, justified.... The existing staff may understand it, but in 10 years that will be lost and it be carefully considered requirements left over by very knowledgeable retired senior staff and accepted "law".	Clearly designate requirements from review considerations or good engineering practices.
4.	Change under 10 CFR 50.90 only if: i. A change to the technical specifications (TSs) incorporated in the license is not required, and ii. The change, test, or experiment does not meet any of the criteria in paragraph 10 CFR 50.59(c)(2). continuing	The position stated here is any digital modification to "important to safety system "automatically results in the need for a LAR. Reviewing the 10.19(c)(2), it is presumed the staff position is that digital automatically results in a *SSC failure possibility with a different result than previously evaluated in USAR ...*	As noted in the cover memo, we need more public meetings to discuss this, the reasoning, and how to proceed. PSU believes it possesses the capabilities to adequately assess the impact of changes to the facility, and the NRC is overly focused on this type of change.
5.	Page 5 A discussion of access control features, which includes both preventing unauthorized access but also allowing authorized access. Access control applies to both analog and digital systems. Access controls such as alarms and locks on panel doors, or administrative control of access to rooms, should be discussed in Section 7.2 Design of Instrumentation and Control Systems.	I do not believe access control and cyber security are within the scope of 10CFr50.34 for NPUFs.	Explain the regulatory basis for access controls and cyber security or reduce the requirements to a request for information or design consideration.

Number	1537 text (partial/paraphrased)	Comment	Suggestion
6.	Page 6 The basis for evaluating the reliability and performance of the I&C systems should be included. All systems and components of the I&C systems should be designed, constructed, and tested to quality standards commensurate with the safety importance of the functions to be performed. Where generally recognized codes and standards are used, they should be named and evaluated for applicability, adequacy, and sufficiency.	Duplicate sentence example	Proof read and eliminate
7.	Page 7 I&C systems should be designed to have functional reliability, including redundancy and diversity, commensurate with the safety functions to be performed and the consequences of failure of the system to perform the safety function. For example, an I&C system for a NPUF should be designed to perform its protective function after experiencing a single random active failure within the system.	This whole section on determining applicability and designing to the analysis is good words, but there is a lot of determinant prejudgment contained in this document that the LICENSEE must re-litigate for relief. Even in the paragraph quoted, the example states the **I&C system** needs to tolerate a single active failure. Much of the I&C system does not. RPS yes (if the analysis needs it to function). But a digital system must tolerate more? A passive software failure and active failure....?	Re think the paradigm based on risk. Clarify.

Number	1537 text (partial/paraphrased)	Comment	Suggestion
8.	Page 7 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 8 Part 1, Standard Format and Content for controlling parameters as reference bounds for design. These values may be (1) restraints derived from generally accepted "state of the art" practices for achieving functional goals, or (2) requirements derived from analysis (based on calculation and/or experiments) of the effects of a postulated accident for which a structure, system, or component must meet its functional goals	IMHO Quoting this legalistic definition from 10CFR50 without reference hardly improves the clarity of this section.	If you are going to quote the code, reference it. What are you trying to tell the licensee here? Eliminate the text
9.	Page 8 As a minimum, each of the design basis aspects identified in ANSI/ANS 15.15-1978 should be addressed.	ANSI/ANS 15.15 is withdrawn	
10.	Page 8 **Software design basis "requirements"**	The bullets in this section are subjective requirements. Reword the applicant (licensee) shall submit documentation under oath that provides clear verification of that each design basis function is fully implemented, and all variables protected with all analysis clearly provided so that the staff can perform a review without asking any questions.	Clarify
11.	• Traceability - It should be possible to trace the information in each design basis item to the safety analyses, facility's system design documents, regulatory requirements, applicant/licensee commitments, or other documents	I do not know what a requirement that says "it should be possible" means. Is that SHALL? These concepts were not required during the previous digital implementations and represents a large expansion of requirement without regulation. This concept should be true for this document. A clear traceability from statue to code to requirement	

Number	1537 text (partial/paraphrased)	Comment	Suggestion
12.	Unambiguity - The information provided for the design basis items, taken alone and in combination, should have one (and only one) interpretation	????	Provide example
13.	Page 9 Design bases for the I&C system, subsystems, and components should include the following, as applicable.... Safety or control functions and any unique or facility-specific functions performed by the I&C system or subsystems	A listing of all the facility unique functions that may be performed seems excessive and a burden to the NRC reviewer. There are many functions provided that are not safety related and have no need for a licensing review. In a new facility, undergoing initial licensing this will be in a state of flux (or paralysis caused by the the need to freeze the application). Would you like a description of the mundane functions as well?	
14.	Any special requirements such as redundancy, diversity, quality assurance, and environmental requirements derived from the results of analyses of the full range of operating conditions and postulated accidents	What is a special requirement?	
15.	PAGE 9 • Each clause in IEEE 7-4.3.2-2003 and RG 1.152, R3 were reviewed for applicability on a section-by-section basis. If review guidance (Part 1)/acceptance criteria (Part 2)matching the intent of that clause was not addressed it was "expanded" into the list of criteria. • Removed the references to GL 95-02 in Sections 7.3-7.7; updated the reference and moved discussion of guidance for a digital upgrade to the beginning of Section 7.2.	These appear to be left over notes from development.	Proof-reading error remove,
16.	PAGE 9 The system description in the SAR should include equipment and major components as well as block, logic, and schematic diagrams.	This sentence is repeated in the paragraph below	Proof read and revise

Number	1537 text (partial/paraphrased)	Comment	Suggestion
17.	Page 10 The applicant should also submit hardware and software descriptions and software flow diagrams for digital computer systems. The applicant should describe how the system operational and support requirements will be met and how the operator interface requirements will be met. The description should also address the methodology and acceptance criteria used to establish and calibrate the trip or actuation setpoints, or interlock functions.	This paragraph is a slightly different working but again a repeat of the paragraph before it.	Proof read and revise
18.	Page 11 Technical specification LSSSs, LCOs, and surveillance requirements for the I&C system should be established. These parameters and requirements should include system operability tests, trip or actuation setpoint checks, trip or actuation-setpoint calibrations, and any system response-time tests that are required.	I disagree with the requirement to duplicate technical specifications in chapter 7. Add refer to 10CFR50.36 for criteria for the content of technical specifications in this section. This section should only identify the applicability of a 10CFR50.36 to a SSC or parameter. It should not try to state the TS or the basis. That is a function of chapter 14 and will lead to confusion and conflict.	Fine tune this requirement. As stated I would either wholesale paste I&C TS into chapter 7 or just list the specs from chapter 14.
19.	Page 11 Un-reviewed safety question	I understand the term un-reviewed safety question is no longer "used". Part 50 uses only with thermal annealing of RPV	Evaluate use / Eliminate term

Number	1537 text (partial/paraphrased)	Comment	Suggestion
20.	PAGE 11 50.59 discussion it is likely that digital modifications to safety-significant systems such as the RPS or ESF actuation system will require staff review.	The position stated here is any digital modification to "important to safety system "automatically results in the need for a LAR. Reviewing the 10.19(c)(2), it is presumed the staff position is that digital automatically results in a *SSC failure possibility with a different result than previously evaluated in USAR.* I fundamentally disagree with this position. While any complex or large change to I&C system would very likely involve a LAR, many smaller scale and simple changes should not. RTRs as a rule have very simple systems, some without diversity because it is not needed for H&S of the public. There are many mods that we should be able to do under 50.59 without LAR. The changes we are likely to do will decease system failures and any associated consequences.	I request public meets be held to clarify this position and the basis for it.
21.	Page 11/12 adverse effects similar change replace auto action with manual, change to man-machine interface…… changing a valve from "locked closed" to "administratively closed	 Hanging unfinished - thought or does this mean etcetera? several of the points have nothing to do with digital, they are any change? Restating/repeating points in a list does not increase the validity of the discussion. ????? Digital manual valves?	Rework this section, have a public meeting, force adoption of NEI 01-01…
22.	Section 7.3 RCS Tech spec discussion	The requirements of the code are much different than the TS criteria used at RTRs. It is good that both parties review the actual requirement. Do not repeat chapter 14 here….	Add reference to 10CFR50.36.

Number	1537 text (partial/paraphrased)	Comment	Suggestion
23.	RCS training section pg. 13	Long winded generally good training here. Who is it for?	Consider a bulleted list
24.	RCS design basis Page 14	Where are the numbers from? What do they mean? This appears to be a listing of NRC generated general design criteria. There is a lot of verbiage here without a lot of action. The list is highly repetitive, with repeat sentences and concepts.	Source the criteria, simplify wording consider bullets
25.	4 thru 12	This is a repeat verbose way of saying the RCS operates to maintain parameters within the boundaries established by the analysis and the design. Why must this be said over and over? see paragraph above 1-3.	Simplify, bullet list of criteria to consider and address (as appropriate) in the single description of the RCS.
26.	12 Page 15 Provide a summary of the analysis used to verify the adequacy of control systems with respect to maintaining variables within operational limits during facility operation and to verify that the impact of control system failures is appropriately included in the MHA analyses	The use of the term MHA here seems inappropriate. Control system failures may drive limiting accidents, but the MHA is postulated beyond a credible event and is not driven by the RCS.	Change MHA to accident analysis
27.	Page 15 The RCS and the reactor reactivity control system should meet the requirements of minimum shutdown margin considering the stuck rod criteria.	It is unclear to me how the instrumentation portion of the RCS does this or could.... this is a chapter 4 design issue.	

Number	1537 text (partial/paraphrased)	Comment	Suggestion
28.	Page 16 discussion of experiments	Much of the listed stuff on experiments seems out of place in chapter 7.	This section needs rethought or thrown out. Description of interlocks between known experiment fixtures and the I&C systems are in scope the rest; not for this chapter. The SAR will be a mess.
	Mechanical forces adversely affecting shielding or confinement arising from causes as in mechanical forces on fuel cladding arising from the manipulation of experimental components, experiment flooding, buoyancy, from tools used for such manipulation, from thermal stress, vibration, or shock waves, or from missiles arising from functioning or malfunctioning experiments	Mechanical impact on the fuel?	
	Radiation fields or radioactive releases from experiments which can mask the performance of an operational monitoring system intended for the detection of fission product releases at early stages	Experiment failures can mask simultaneous fission product release?	
	Provide a description of the factors in experiments that can adversely affect the operability and integrity of the RCS and any associated technical specifications arising from experimental systems	While it seems reasonable n chapter 4/13 to decide the outside limits for power channel calibration and the need to control the calibration impact of experiments, other than known deficiencies in design, how is chapter 7 to address this? This belongs in chapter 10 experiments and administrative controls of experiments.	

Number	1537 text (partial/paraphrased)	Comment	Suggestion
29.	There are 256 uses of the word describe and 183 analyze. A 500% increase over the previous document	Hopefully an applicant will not actually try to do what is described in the content guide. You would not want to review it. The continuous use of provide a description of (fill in anything being asked for) in multiple contexts is confusing and will result in an unreadable SAR. I believe you want a single well organized description of each system that addresses certain criteria. Ask for that and then give a desired organization of the factors you would like discuss. If they are logically grouped, (and numbered) the applicant could write to the grouping and reference your criteria number as there are addressed. A cross reference across the entire SAR could be provided against all the criteria as they come up in various sections. Think about the whole you want to review. The NRC should provide an example a good section 7 submittal as an appendix to assist in preparation.	Revise guidance directions to get what you can actually review. Provide example in an appendix
30.	Criteria 23 Page 18 The conclusions of the analysis of postulated accidents and accidents as presented in Chapter 13 of the SAR are used to verify that facility safety is not dependent upon the response of the control systems. In addition, failure of the control systems themselves or as a consequence of supporting system failures, such as loss of power sources, should not result in facility conditions more severe than those described in the analysis of MHA and postulated accidents. Show that the accidents analyzed in Chapter 13 of the SAR do not depend on the operability of the RCS to assure safety	This seems out of place, to show in chapter 7 the accidents in chapter 13 are independent of the control system. It seems any discussion of independence is in the basis of the chapter 13 analysis.	Eliminate this requirement.

Number	1537 text (partial/paraphrased)	Comment	Suggestion
31.	Criteria 23 Page 18 If the RCS and RPS are separate systems, the safety functions should be placed with the RPS. This requirement does not apply to a combined RCS-RPS	The words of the author belie a different mind-set than that exposed by NRC management. This document "does not provide requirements" or a design basis. So why does this sentence as well as much of this document state (234 times) repeat something very different?	Critically evaluate the terminology used throughout the document. What it says and what management says are two different things. What will it mean in 10 years?
32.	Criteria 24 Page 18 The RCS protects against a failure or operation in a mode that could prevent the RPS from performing its intended safety function. The design of the RCS should consider the following: • effects of control system operation upon accidents, • effects of control system failures, and • effects of control system failures caused by accidents. Provide a description showing that the failures of any component in the RCS or any auxiliary supporting system for control systems are bounded by the analysis of postulated accidents in Chapter 13 of the SAR. While failure analyses typically address random hardware failures, this evaluation should also address failure modes that could be associated with software failures	Where are these sourced from? They are not from 1537, and they are not really digital issues. IF the RCS is required to protect the RPS (and they're not the same system) then RPS will fail its design criteria. While I am glad this paragraph does not ask for another "analysis", I am uncertain what a "description showing" something means. What does the author want me to certify under oath of affirmation? The MHA is a non-credible event, the author is perusing power reactor credible event initiators to ensure the consequences of digital failures are not worse than proposed. Our low or negligible risk facilities meets part 20 with a non-credible event. Even if our analysis misses something, the consequences can only be low impact. Even the SL-1 accident had no offsite consequences.	Re-evaluate the inclusion of multiple design criteria from consequential design guidance in the low to negligible risk facility. The answer too many of these discussion will be a repetitive statements of bounded by the MHA.

Number	1537 text (partial/paraphrased)	Comment	Suggestion
33.	Criteria 24 Page 18 The SAR should contain a review of the consequential effects of postulated accidents and accidents are bounded by the accident analysis in Chapter 13 of the SAR. Finally, the review should summarize the safety analysis regarding consideration of the effects of both control system action and inaction in assessing the transient response of the facility for accidents and 19	Reword simplify.	Reword entire section "The SAR should contain a overview of any consequential effects of RCS induced transients and discuss how these accidents are bounded by the chapter 13 SAR accidents."
34.	Criteria 25 Page 19 Operational bypass criteria 25	RCS is reactivity control system, not facility control system. This requirement is over-reaching and impractical given the list of interlocks provided in the next paragraph. This is power reactor mentality of a centralized control room that controls everything remotely. This would have to be done early in the design of the facility and will burden the control room operator with tasks and indications.	Change this section to "bypasses of reactor control or reactor control or protective functions should be under the direct control of the reactor operator (when feasible) and clearly indicated to the operator. Providing control room indication and control of the interlocks should be evaluated during initial design. Examples of functions and bypasses to consider include: OR Delete this section in its entirety.

Number	1537 text (partial/paraphrased)	Comment	Suggestion
35.	Criteria 26 Page 19 Direct interacting or interlocking with system controls may be justified if analyses of an experiment or experimental facility could show hazard to itself, the facility, equipment, personnel, or the environment. Any such automatic limiting devices should demonstrate that function of the RPS will not be compromised, or a safe shutdown condition will not be prevented (see Chapter 10, "Experimental Facilities and Utilization"). Provide a description of those conditions in which experiment controls, including reactivity changes, can interact with operating controls.	Verbose complicated	Replace section with "if the analysis and design of experimental facilities (Chapter 10) results show that automatic reactor limiting devices are needed (or are used), describe how the and when the interaction with the RPS/RCS occurs or is accomplished.
36.	Criteria 27-28	Verbose, don't repeat TS in chapter 7	Simplify to last sentence *Provide a summary of the calibration, inspection, and testing (including self-tests and surveillance tests) to validate the desired functionality of the RCS.*
37.	Various QA program and construction permits	The document refers to the need for a QA program for a construction permit holder. Please elaborate on QA requirements for an upgrade and when a construction permit for an instrumentation upgrade is required.	Existing RTRs have no requirement for QA programs.
38.	Criteria 32 Access control	My answer would be it is inside the CAA, see the PSP for access control requirements. Where do the rest of these requirements come from?	Simplify to actual requirements. Label good ideas as good ideas.
39.	Criteria 33 Page 22 Cyber security section The cyber security program should include policies, procedures and processes for providing appropriate assurance that the SDOE is adequately protected from cyber threats and attacks.	The ISG implements, outside the regulatory framework, the requirement for a cyber security program with policies, processes and procedures. If a requirement for this exists in the code, it belongs in chapter 12? What are the regulatory bases for requiring a program and procedures?	This document seems to contain many ideas that never went through a thorough review process. There is no regulatory basis for cyber security at RTRs….yet.

Number	1537 text (partial/paraphrased)	Comment	Suggestion
40.	7.4 RPS description The RPS should promptly and automatically place the reactor in a subcritical, safe-shutdown condition (scram) and maintain it there. This prevents or mitigates unintended operation in regions where risks of the following types could occur: fuel damage from overpower or loss of cooling events, *uncontrolled release of radioactive materials to the unrestricted environment, or overexposure of personnel to radiation.*	In 20 years of working in commercial power reactors and 5 years Naval reactors, I had not seen an automatic scram on high radiation level or uncontrolled release of rad material to the environment. Yet in 1537 they are presented as requirements and have been implemented at PSU. Please relate to the applicable 10CFR.	Provide source of requirement.
41.	RPS design .	Where do all these detailed design criteria come from? It would be much clearer to applicants if the document just listed these items as general design criteria for RTR control systems. Appendix A lists the general design criteria for power reactors, it seems clear someone wants them for RTRs.... where are RTR requirements except here?	
42.	Basis 1 Identify the MHA applicable to each mode of operation; this information should be consistent with the analysis provided in Chapter 13 of the SAR	? What is mode of operation in this context? Did this start out as Mode 1,2,3 in a power reactor document and not quite get cleaned up?	

Number	1537 text (partial/paraphrased)	Comment	Suggestion
43.	Consideration should be given to failures that cause actions as well as prevent actions, such that all possible effects are examined. Further, failures that could lead to single or multiple rod position changes or out-of-sequence rod patterns should be analyzed. *The staff considers operator error to be an anticipated operational occurrence, in addition to the consideration of single malfunction requirements, for which conformance to these **requirements** is to be evaluated.*	BWR rod worth minimizer lessons learned? Word for word from some document, which one? Please provide a reference to the **requirement** that the system be tolerant of a single failure and define that in a reference that includes operator error. Is the general design to be considered one passive failure, one active failure and one operator failure simultaneously? Is the operator error the active failure or the passive failure or is it in addition to both? Is a common mode software error an active or passive error or both simultaneously? Is the standard for the analysis no public H&S impact, no facility impact, or no challenge to the safety limit or all the above?	Too many requirements from unknown sources.
44.	Criteria 2 Neutron flux (power) monitor channels covering the range from subcritical source multiplication to well beyond the licensed maximum power level. Identify the variables that are monitored in order to provide protective action	What is well beyond? This requirement does not exist in the power reactor world, what is the source? If you change this sentence to the following, you can eliminate other sections of this document	Too many requirements from unknown sources. Identify the variables that the RPS must monitor and limit in order to provide protective action as necessary by the analysis in Chapters 4 and 13. Identity any quantitative performance requirements (accuracy, range, response time).

Number	1537 text (partial/paraphrased)	Comment	Suggestion
45.	The licensee should also identify the analytical limit associated with each variable. Performance requirements—including system response times, system accuracies, ranges, and rates of change of sensed variables to be accommodated until conclusion of the protective action—should also be identified in the system designation.	This discussion is essentially a duplicate of the scram time discussion in the next section below.	eliminate it.
46.	Criteria 3 **Separation between safety divisions** begins with the sensors monitoring the variables and continues through the signal processing and actuation electronics.	Sounds familiar….. is this needed in NPUFs. The language betrays a consequential design origin	Eliminate train separation requirements.
47.	Provide an analysis showing the establishment of the LSSS settings	Is this a chapter 7 analysis or chapter 4/13/14? Traditionally RTRs only need trip before the LSSS to be considered operable and in compliance.	
48.	Criteria 4 Identify the variables that are monitored in order to provide protective action	contains and duplicates concept paragraph to criteria 2	
49.	Criteria 8 Page 26 Where it is determined that the spatial dependence of a parameter requires several sensor channels to ensure the protection of the facility, the redundancy requirements are determined for the individual case. *In certain designs, for example, adequate monitoring of core power requires a minimum number of sensors arranged in a given configuration to provide adequate protection.* This aspect of redundancy is dealt with in coordination with the organization responsible for reviewing reactor designs to establish redundancy requirements	Appears to be criteria from very large reactor core design criteria. Is it really an issue that has been carefully evaluated for inclusion here…..?	

Number	1537 text (partial/paraphrased)	Comment	Suggestion
50.	Criteria 9 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. This level of protection should ensure that after the event, a single failure should not prevent mitigation of that event. **Credible effects of design-basis events that** do not depend on a given group of redundant instrument-sensing lines for mitigation or accident prevention may render inoperable any or all of that group of sensing lines without violating this criterion. All nuclear safety-related instrument-sensing lines should be protected from damage during normal operational activities and occurrences.	Appears to be criteria from power reactor design criteria. Is it really an issue that has been carefully evaluated for inclusion here…..? What is our design basis event? If I update my systems will this be a backfit on my plant?	Eliminate train separation guidance
51.	Criteria 10 Interlocks ensure that operator actions cannot defeat an automatic safety function during any operating condition where that safety function may be required. These interlocks include permissive for manually initiated operating bypasses and interlocks to ensure manually initiated operating bypasses are automatically removed when operating conditions would require the trip functions. Interlocks are also provided to *ensure that manually initiated maintenance bypasses can only defeat a single train or channel* of the RPS but not multiple channels or trains that would impair the system's…..	Appears to be criteria from power reactor design criteria. Is it really an issue that has been carefully evaluated for inclusion here…..? This would be a backfit on existing systems.	

Number	1537 text (partial/paraphrased)	Comment	Suggestion
52.	All operating bypasses, either manually or automatically initiated, should be automatically removed when the facility moves to an operating regime where the protective action would be required if an accident occurred. Status indication should be provided in the MCR for all operating bypasses.	These are power reactor requirements being promulgated without regulation to RTRs	
53.	12 Page 27 The RPS should provide automatic initiation so that (1) fuel design limits are not exceeded and (2) accidents are sensed and mitigated. Both require timely operation of RPS components, thus establishing the timing requirements for detecting parameters exceeding their setpoints and equipment actuation in the RPS. Provide an analysis of the real time performance of the RPS, from sensors to actuators.	This is a repeat concept to item criteria 4 This is really the only relevant point in this section and it should be moved up to criteria 4 where it is already addressed.	

Number	1537 text (partial/paraphrased)	Comment	Suggestion
54.	13 page 28 A special concern for digital computer-based systems is confirmation that system real-time performance is adequate to ensure completion of protective action within the time scale derived from the applicable analyses in the SAR. The digital instrumentation loop often includes the sensor, transmitter, analog-to-digital converter, multiplexer, data communication 29 Part 1, Standard Format and Content equipment, demultiplexer, computers, memory devices, controls, and displays. Timing analysis should consider the entire loop. System timing requirements calculated from the MHAs and other criteria have been allocated to the digital computer portion of the system as appropriate, and have been satisfied in the digital system design and implementation. Digital system architecture affects performance because communication between components of the system takes time, and allocation of functions to various system components affects timing. The architecture may also affect timing because an arrangement of otherwise simple components may have unexpected interactions.	This is a repeat of criteria 12. *Provide an analysis of the real time performance of the RPS, from sensors to actuators.*	
55.	14 page 29 The principle of defense-in-depth is to provide several levels or echelons of defense to challenges to facility safety, such that failures in equipment and human errors will not result in an **undue threat to public safety.**	I agree with the definition, but please provide a credible scenario for an existing RTR where a control or protective feature failure creates a beyond the MHA release to the public that results in an "undue" threat to the public.	

Number	1537 text (partial/paraphrased)	Comment	Suggestion
56.	15 page 30 Independent redundant **or** diverse reactor power level trips should be considered if a common-cause failure (CCF) failure of the RPS could result in exceeding the results in the accident analysis or have consequences **within** those of the MHA	The wording relative to the MHA does not make sense. "within" should be "beyond". Another section required 2 channels of power scram already, so this discussion appears moot.	
57.	Criteria 9 page 80 Manual capability may be necessary because all of the protection and control systems are digital-computer-based and therefore vulnerable to common-cause failure.	Another highly biased statement against digital.	
58.	Annunciators page 85 criteria 20 Negligible-risk research reactors need not comply with the single-failure criterion for the automatic detection of each MHA or design basis accident and the immediate execution of the achieving a safe shutdown condition (scram) of the reactor.	A small concession to negligible risk, we don't need single failure proof annunciators.	
59.	**I did not read the entire Part 1**	It was to long too repetitive, too many things to comment on.	
60.	**1537 part 2 comments**	I did not have a time to make a thorough review. My impression was it was much better, more concise. Many requirements in part 1 did not appear to be reviewed in part 2, but I was not detailed in my review (it was a skim). Clearly, some inappropriate evaluations (Cyber security for example) showed up.	