As of: November 14, 2012
Received: November 11, 2012
Status: Pending_Post
Tracking No. 1jw-81x7-orl8
Comments Due: November 13, 2012
Submission Type: Web

PUBLIC SUBMISSION

Docket: NRC-2012-0237
NUREG-0800 - Proposed Revision to SRP Section 19.3; Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants

Comment On: NRC-2012-0237-0001
Proposed Revision Treatment of Non-Safety Systems for Passive Advanced Light Water Reactors

Document: NRC-2012-0237-DRAFT-0002
Comment on FR Doc # 2012-25110

Submitter Information

Name: David Moses
Address:
130 Clemson Drive
Oak Ridge, TN, 37830-7664

General Comment

10/12/2012
77FR62270
(3)

See attached file(s)

Attachments

Comments on SRP 19.3

SUNSI Review Complete
Template = ADM-013

E-RIDS = ADM-03
Add = A. Cubbage (QEC)

Comments based on Draft SRP 19.3

The following comments on draft SRP 19.3 are summarized here and discussed in more detail in the attached white papers on "augmented design standards" and "short-term availability controls." The key issues are:

1. The "augmented design standards" in draft SRP 19.3 do not fully reflect the specific list of capabilities requirements in the EDO's memorandum to the Commission, June 23, 1997, "Implementation of Staff Position in SECY-96-128 - 'Policy and Key Technical Issues Pertaining to the Westinghouse AP600 Standardized Passive Reactor Design,' Related to Post-72 Hour Actions." (ML003708229) While capability to withstand the adverse effects of design basis accidents has been added, the requirements for availability controls and a quality assurance program and the exemption for dynamic qualification of active equipment are not addressed in the SRP Acceptance Criteria without any explanation of the bases for the changes in the so-called "Commission-approved guidance" as it is referred to in SRP 19.0 and Section C.I.19 of RG 1.206..

2. None of the current SRP or DSRS sections for SSCs provide cross-reference to the requirements for "augmented design standards" in SRP 19.3. Those NRC-generated DSRS that do reference SRP 19.3 fail to invoke the need to address "augmented design standards" when applicable to the RTNSS equipment that may be addressed in the DSRS thus leaving it up to the user to guess, infer or read between the lines on requirements. This lack of requirements flow-down and parallelism in the SRP/DSRS-based procedural controls for guiding staff reviews and for providing guidance for the designer/applicant design and documentation efforts will lead to confusion in both the review and design processes and would not pass muster in an Appendix B or NQA-1 type quality assurance audit of procedural controls. If QA auditors expect such clear requirements flow-down and parallelism in licensee's procedures at nuclear facilities, the same is to be expected of NRC regulatory guidance.

3. There has been no rulemaking to define investment protection short-term availability controls only a profusion of inconsistent NRC thought documents (see white papers). The regulatory criteria in 10 CFR 50.36(c)(2)(ii)(C) and (D) indicate that, lacking any operational experience for the new passively-safe designs to justify otherwise, these controls should be subject to technical specification LCOs since RTNSS reliability/availability controls are for equipment that will constitute the "primary success path" in accidents and transients in which ac electrical power remains available thus preventing such challenges from progressing to "design basis accidents or transients" and are selected based on the requirements for their reliability/availability being shown by PRA to be "significant to public health and safety." Once sufficient operational experience has been obtained to warrant reduced controls other than technical specification LCOs, these type controls can be removed from technical specification LCOs and then be invoked as administrative controls in either Specification 5.4 (Procedures) or 5.5 (Programs and Manuals) in the plant specific technical specifications. The allowances with regard to availability controls that NRC has encoded in the design certifications (DCs) rulemakings for AP600, AP1000 and ESBWR appear to be a ripe source of legal contentions by interveners during the COL if they recognize that (1) there is no operational experience base nor generic and specific rulemaking for such allowances where the DCs rulemakings are lacking in substantive details in this regard and (2) the allowances are inconsistent with the existing regulatory requirements for LCOs in 10 CFR 50.36(c)(2)(ii)(C) and (D). In addition, the selection process using PRA may be questionable since the PRAs are understood to be proprietary and not open to public disclosure. This latter situation may not sit well with potential COL interveners due to a lack of transparency,

Commission-approved design guidance (or "augmented design standards") for RTNSS

Background

The SRP Acceptance Criteria in SRP Section 19.0, both Revision 2 (June 2007) and the recent draft Revision 3 (September 2012), contain the following general statement: "The Commission SRMs relating to SECY-90-016, SECY-93-087, SECY-96-128, and SECY-97-044 provide Commission-approved guidance for implementing features in new designs to prevent severe accidents and to mitigate their effects, should they occur."

Section C.I.19.1 of RG 1.206 contains a similar statement: "The SRMs relating to SECY-90-016, SECY-93-087, SECY-96-128, and SECY-97-044 provide Commission-approved guidance for implementing features in new designs to prevent severe accidents and to mitigate their effects, should they occur."

These features of new designs are both the safety-related passive safety systems and the risk-significant nonsafety-related active systems that back-up the passive safety-related systems as demonstrated in PRA to minimize the frequency of challenges and to accommodate events such as ATWS, SBO, DBAs at times beyond 72 hours, seismic events, etc., as listed among the five criteria in Section C.IV.9.2 of RG 1.206. These active systems are subject to the Regulatory Treatment of Nonsafety Systems (RTNSS) as defined in SECY-93-87, SECY-94-084 and SECY-95-132.

But what is the specific "Commission-approved guidance for implementing features in new designs?" If found, how should it be implemented for equipment design and qualification? This guidance has finally semi-officially appeared as "augmented design standards" in the draft SRP Section 19.3 (Draft Rev.0 - October 2012)

Evolution of Specific Guidance

The specific guidance with regard to RTNSS design and qualification requirements comes from SECY-96-128 and its associated SRM on the design certification (DC) effort for AP600.

Section IV of the Enclosure to SECY-96-128 defined the staff proposals for requirements for equipment that would be needed to ensure safety in post-72 hour recovery operations following an accident. For AP600, Westinghouse had proposed relying on off-site equipment to cope with post-72 hour events. The staff disagreed stating in SECY-96-128 (with certain portions underlined below for emphasis):

> ...because Westinghouse is proposing the use of equipment with no protection or demonstration of its ability to withstand natural phenomena, the equipment may be susceptible to damage from environmental conditions such as water, wind, or earthquake aftershocks. The staff does not believe that offsite equipment and supplies should be credited in the design basis of the plant and, therefore, concludes that credit for the use of offsite transportable equipment and supplies cannot be given for supporting safety functions for the design basis of the AP600 for event scenarios with a loss of offsite power for more than 72 hours.

> Therefore, staff recommends that the Commission approve the position that the site be capable of sustaining all design basis events with onsite equipment and supplies for the long term. After 7 days, replenishment of consumables such as diesel fuel oil from offsite suppliers can be credited. The equipment required after 72 hours need not be in automatic standby response mode, but must be readily available for connection and be protected from natural phenomena including seismic events (per GDC 2).

In the SRM for SECY-96-128 (ML003708192), the Commission approved the following:

> The Commission approved the staff's position that the site be capable of sustaining design basis events with onsite equipment and supplies for the long term, with replenishment of consumables (such as diesel fuel oil) from offsite suppliers after seven days.

However, the quoted statements above are at best general guidance and the specific guidance to the staff on the details of what is interpreted as Commission-approved guidance is found in the EDO's memorandum to the Commission dated June 23, 1997, entitled "Implementation of Staff Position in SECY-96-128 - 'Policy and Key Technical Issues Pertaining to the Westinghouse AP600 Standardized Passive Reactor Design,' Related to Post-72 Hour Actions." (ML003708229) Without a direct quote in each case of this guidance, it can be summarized as follows that the post-72 hour RTNSS equipment must be:

- Required in the COL to assure availability controls for the post-72 hour SSCs.
- Designed to Seismic Category I standards "and constructed to the same requirements as nonseismic structures" where "for these systems and components, the design of anchorages must be consistent with the SSE design of equipment anchorages of Seismic Category I items and there should be no spatial interaction with any other non-seismic SSCs that could adversely interact to prevent the functioning of the post-72 hour SSCs following an SSE; but no dynamic qualification of active equipment is necessary."
- Ensured "that the post-72 hour SSCs can withstand the effects of high winds of severe hurricanes" so that "the SSCs shall be analyzed and designed for Category 5 hurricanes including the effects of sustained winds, maximum gusts, and associated wind-borne missiles. The use of a Category 5 hurricane for analyzing the effects of wind and wind-borne missiles for the design of the post-72 hour SSCs is based on" NUREG-1474 (that is, Hurricane Andrew) wind speeds and using winds gusts actors specified in ANSI/ASCE 7-93 [now updated to ANSIASCE 7-05 with possibly applicable update changes from 2010].
- Protected from floods.
- Be subject to QA requirements (in the case of AP600, one submitted by Westinghouse) but presumably meaning generally a QA program acceptable to NRC under SRP Chapter 17.

As of October 12, 2012 (77 FR 2012-25110), this Commission-approved guidance now appears in draft SRP 19.3 in Section II under "SRP Acceptance Criteria" under the subheading of "Area of Review – Augmented Design Standards." These "augmented design standards" now appear as a list of six staff guidance statements as follows:

1. The staff will verify that the applicant has met the following acceptance criterion: Safety functions required in the post 72-hour period following an accident can be accomplished with onsite equipment and supplies.

2. The staff will verify that the applicant has met the following acceptance criterion: RTNSS "B" SSCs and supporting equipment will be readily available for connection. Use of mobile equipment is acceptable after seven days. [***NOTE***: *Draft SRP 19.3 fails to define RTNSS "B" SSCs, but it is inferred from other previous draft design specific review standards (DSRS), such as ML12178A645 for mPower™ issued by NRC, that this refers to SSCs covered by RTNSS Criterion B which appears from the wording in various NRC-generated DSRS to be the same as Criterion (2) given in Section C.IV.9.2 of RG 1.206 as derived from Criterion B, Section I, of both the Enclosure to SECY-94-084 and Attachment 2 to SECY-95-132. This Criterion B as stated in SECY-94-084 is "SSC functions relied upon to resolve long-term safety (beyond 72 hours) and to address seismic events." NRC needs to clarify and be more specific and consistent in making and using such definitions; to do otherwise merely propagates and perpetuates confusion. In this case, it may be best to revise RG 1.206 and define same also in the SRP Introduction and perhaps again here in this SRP to make the usage specific and clear.*]
3. The staff will verify that the applicant has met the following acceptance criterion: RTNSS "B" SSCs and structures housing RTNSS "B" SSCs are designed such that they can withstand the effects of a safe shutdown earthquake (SSE); and, without repair, the SSCs are capable of performing their required functions following the earthquake.
4. The staff will verify that the applicant has met the following acceptance criterion: RTNSS "B" SSCs have been analyzed and designed to withstand the effects of high winds produced in Category 5 hurricanes and tornados, including the effects of sustained winds, maximum gusts, and associated wind-borne missiles.
5. The staff will verify that the applicant has met the following acceptance criterion: RTNSS "B" SSCs have been analyzed and designed to withstand adverse effects associated with design basis accidents (e.g., turbine missiles, pipe whip).
6. The staff will verify that the applicant has met the following acceptance criterion: RTNSS "B" SSCs and supporting equipment will be protected from floods, as required by GDC 2, "Design bases for protection against natural phenomena", and meet the criteria in SRP 2.4 and SRP 3.4.1.

Comments and Conclusions

Thus, the draft SRP 19.3 "augmented design standards" generally replicate the design guidance from the EDO's memorandum to the Commission dated June 23, 1997, except for:

(1) Adding the required capability to withstand the adverse effects of design basis accidents (Item 5 above),

(2) Failing to include availability controls as part of the "augmented design standards" in the SRP Acceptance Criteria although these are addressed separately in the Areas of Review and the Review Procedures,

(3) Failing to make it clear that dynamic qualification of active equipment is **not** required unless NRC management or staff has changed its mind then a footnote is needed to so indicate and explain the reasons why to avoid confusion, and

(4) Failing to include the requirement for the equipment to be subject to a QA program that presumably must meet the requirements of SRP Chapter 17. [***NOTE:*** *"Quality assurance" never appears in the text of drat SRP 19.3.*]

In addition, there is a lack of cross-referencing to this SRP and the need to address "augmented design standards" for RTNSS equipment in other SRP and DSRS sections, especially in the SRP or DSRS sections in Chapters 3, "Design of Structures, Components, Equipment," and 14, "Initial Test Program and ITAAC-Design Certification," but generally in all sections dealing with SSCs. This absence leads to a lack of parallelism in the procedural review requirements and design acceptance criteria embedded in the SRP or DSRS and a failure to provide a clear flow-down of design requirements to the procedures that implement both the staff reviews and the guidance to the designers, applicants and licensees for addressing the safety-related and/or risk-significant SSCs. This approach would never pass muster with an NQA-1 quality assurance audit of procedural controls. The inconsistencies foster confusion due to lack of clarity, specificity and consistency.

Finally, what constitutes acceptable availability controls needs to be better-defined since as described in a separate white paper there are questions arising from the origins of same in previous regulatory documents issued by NRC as to whether, without additional rulemaking to clarify requirements or operational experience to justify less stringent alternatives to technical specification LCOs, such controls satisfy and are consistent with the existing regulatory requirements in 10 CFR 50.36(c)(2)(ii)(C) and (D).

Comments based on Draft SRP 19.3

Potential Significance of Inconsistency of RTNSS Availability Controls Selection Process with TS LCO Selection Criteria 3 and 4 in 10 CFR 50.36(c)(2)(ii)(C) and (D)

Problem Statement

There is a notable inconsistency between specific regulatory requirements and the staff positions on RTNSS that might be used by knowledgeable interveners in court to hobble current and future COL licensing activities.

10 CFR 50.36(c)(2)(ii) states: "A technical specification limiting condition for operation of a nuclear reactor must be established for each item meeting one or more of the following criteria:...

(C) *Criterion 3.* A structure, system, or component that is part of the primary success path and which functions or actuates to mitigate a design basis accident or transient that either assumes the failure of or presents a challenge to the integrity of a fission product barrier.

(D) *Criterion 4.* A structure, system, or component which operating experience or probabilistic risk assessment has shown to be significant to public health and safety."

Criteria 3 and 4 appear in the Commission's "Final Policy Statement on Technical Specifications Improvements for Nuclear Power Reactors," 58 FR 39132-39139, July 23, 1993, and were adopted into the regulation effective August 18, 1995, by the rulemaking in 60 FR 36952-36959, July 19, 1995. Criterion 3 appeared earlier in the Interim Policy Statement published in 52 FR 3788*ff*, February 6, 1987.

To date in the design certifications of AP600 (10 CFR Part 52, Appendix C), AP1000 (10 CFR Part 52, Appendix D), and ESBWR (proposed rulemaking in 76 FR 16549–16570, March 24, 2011) short-term availability controls are acknowledged as the regulatory oversight means for assuring the reliability/availability of RTNSS. RTNSS are used for normal shutdown, may also form "part of the primary success path" in responding to events in which ac electrical power remains available, and are relied upon in responding to events in the post-72 hour timeframe after a design basis event when ac electrical power may be returned to service. RTNSS and their availability controls are also discussed in Chapter 22 of the FSERs for the passively-safe reactors design certifications: NUREG-1512 for AP600, NUREG-1793 for AP1000 and the draft for ESBWR. Only in Chapter 22 (Section 22.5.4.3, page 22-17) of NUREG-1512 is it clearly described what the availability controls are meant to be:

> ...proposed means for the implementation of RTNSS controls in the form of short-term administrative availability controls. The administrative controls are formatted similar to Technical Specifications, with operability requirements, applicability, actions and completion times if operability requirements are not met, surveillance requirements, and bases for the availability controls. However, there are no limiting conditions for operation (i.e., there is no requirement to bring the plant to a safe-shutdown condition when operability requirements are not fulfilled) if the completion times for required actions are not met.

In SECY-94-084, March 28, 1994 (ML003708068), and in the follow-on EDO's memorandum "Consolidation of SECY-94-084 and SECY-95-132," July 24, 1995 (ML003708048), the staff outlined the RTNSS process "concerning design and performance of active systems and equipment that perform non-safety, defense-in-depth

functions," which includes "the process to be used by the designer for specifying the reliability/availability (R/A) missions of risk-significant structures, systems, and components (SSCs) needed to meet regulatory requirements and to allow comparison with NRC safety goals" and "if active systems are relied on to meet the R/A missions, the designer will impose design requirements commensurate with risk significance on those elements involved." These staff documents further state that the "RTNSS process for each design" includes:

- A comprehensive baseline PRA considering all internal and external events,
- A focused PRA that "includes the passive systems and only those active systems necessary to meet the safety goal guidelines," and
- Use of the "SSAR to determine that it includes proper short-term availability control mechanisms, if required for safety and determined by risk significance."

In the recent issuance of draft SRP 19.3 in October 2012, the following verbiage is used in the Areas of Review to describe short-term availability controls:

> Availability controls are a form of regulatory oversight for the availability of non-safety-related SSCs in the scope of RTNSS. Availability controls are established in a manner similar to TS and include AC LCO, applicability specifications, action statements with completion times, surveillance requirements (ACSR) and frequencies. Availability controls are submitted to the NRC for review in the form of the Availability Controls Manual (ACM). The review of ACM is led by the organization responsible for the review of technical specifications in Chapter 16 of the Final Safety Analysis Report (FSAR). PRA and Severe Accident staff and staff responsible for review of specific SSC functions support the review of the ACM in the following ways:
>
> 1. Assuring that treatment of RTNSS SSCs in the ACM is commensurate with the assumptions in the PRA.
> 2. Confirming that, at a minimum, ACs have been included in the ACM for RTNSS "B" SSCs. [***NOTE***: *Draft SRP 19.3 fails to define RTNSS "B" SSCs, but it is inferred that is referring to SSCs falling under Criterion B, Section I, of both the Enclosure to SECY-94-084 and Attachment 2 to SECY-95-132. This Criterion B as stated in SECY-94-084 is "SSC functions relied upon to resolve long-term safety (beyond 72 hours) and to address seismic events."*]
> 3. Verifying the adequacy of the ACSR.

Thus it is clear that there is both a regulatory requirement to impose technical specification LCOs on equipment that "probabilistic risk assessment has shown to be significant to public health and safety" or that may form "part of the primary success path" when ac electrical power remains available and the NRC staff positions that state that active risk significant equipment should be subject to availability controls that are like technical specifications but are not technical specifications in the traditional regulatory sense. Unfortunately, since NRC has never issued definitive rulemaking on RTNSS as expected under the legal requirements of 5 *U.S.C.* 553(b), this situation sits out there inviting intervener petitions on the pending COLs for such plants as AP1000 that have design certifications to request that NRC cease licensing activities until NRC clarifies the rationale in a definitive and quantitative manner as to why some licensing requirements must comply with 10 CFR 50.36(c)(2)(ii)(C) and (D) while others get an apparently less stringent treatment. Arguments might be made that with ac electrical power available, the success path relying on RTNSS is responding to an anticipated

operational occurrence (AOO) not a "design bases accident or transient," but the counter argument is that the RTNSS is preventing the event from proceeding from an AOO to a "design bases accident or transient." Further, with these new designs, there is no operating experience yet to indicate that technical specification LCOs with shutdown requirements are not needed for equipment designated as RTNSS since there is no experiential substantiation of the assumptions in the PRA, and, since PRAs are understood to be considered proprietary and not subject to public disclosure, there is an inherent barrier to full transparency in how the PRA is being used to make such decisions. This is troubling since it appears to invite intervener challenges.

Additional Background

The issue of nonsafety-related investment protection equipment and its roles in plant safety and responding to transients was initiated by the NRC Office of Nuclear Regulatory Research (RES) pre-application reviews in the mid to late 1980s of the proposed passively-safe reactors MHTGR, PRISM and SAFR. The issue of "technical specifications or equivalent (or acceptable) administrative controls" for such systems is only really found in Sections 5.4.5.B, 5.5.5.A, 10.3.5.A, 13.1.5, and 16 in the draft PSER for the MHTGR (NUREG-1338, February 1989, ML052780497). The final draft PSER for the MHTGR (NUREG-1338, February 26, 1996, ML052780519) prepared by the NRC Office of Nuclear Reactor Regulation (NRR) does not address same but defers instead to the SECY documents on RTNSS prepared during the reviews of the AP600 and SBWR. Similar wording about "technical specifications or equivalent (or acceptable) administrative controls" is not found in the PSERs for SAFR (draft NUREG-1369) or PRISM (draft and final NUREG-1368).

The first detailed discussion of RTNSS that can readily be found and its relation to technical specifications is found in Section III.A (page 68*ff*) of the Enclosure to SECY-93-087, dated April 2, 1993 (ML003708021), and which followed upon NRC meetings with EPRI on the NRC review of the EPRI Utility Requirements Document (URD) volume dealing with the vendor-proposed passively-safe ALWRs such as AP600 and SBWR. The key relevant paragraphs from page 69 of the Enclosure to SECY-93-087 are quoted as follows:

> In addition, technical specification development is a subset of the overall regulatory treatment of the passive designs. The staff is evaluating the need to establish reliability-based technical specifications for passive designs. This evaluation will determine which systems and components (including certain nonsafety systems) require the imposition of technical specifications, and the parameters of the technical specifications. The Reliability Assurance Program is expected to strongly influence these technical specifications.
>
> Since the passive ALWR design philosophy departs from current licensing practices, new regulatory and review guidance is necessary so that the staff can appropriately review the AP600 and SBWR submittals. Significant decisions need to be made concerning the scope of staff review of the nonsafety systems and reliance on the passive systems. The staff will not require that the active systems meet all the safety-grade criteria, but there should be a high level of confidence that risk-significant active systems are designed in accordance with their performance/reliability missions to ensure their availability when needed.

In SECY-94-084, March 28, 1994 (ML003708068), and in the follow-on EDO's memorandum "Consolidation of SECY-94-084 and SECY-95-132," July 24, 1995 (ML003708048), which were noted above, there are two places where technical specifications are also mentioned:

- Page 3 of the Enclosure to SECY-94-084: "If active systems are determined to be risk significant, NRC will review these R/A missions to determine if they are adequate and if the operational reliability assurance program (O-RAP) **or** simple technical specifications and limiting conditions for operation are adequate to give reasonable assurance that the missions can be met during operation."
- Page 7 of the Enclosure to SECY-94-084: "Reviewing the SSAR to determine that it includes proper short-term availability control mechanisms, if required for safety and determined by risk significance such as simple technical specifications."

The first time that the reference to RTNSS and technical specifications in a NUREG-series report can be found is the staff's review report (not an SER *per se* since no licensing is involved) on the ALWR URD for the passively-safe ALWRs in NUREG-1242, Volume 3, Part 2, August 1994 (ML070600373), Section 3.2.2 (page 3.2-7):

> In principle, all non-safety SSCs in the focused PRA model needed to meet NRC requirements, safety goal guidelines, and containment performance goals are potentially subject to proper regulatory oversight. On the basis of their risk significance and R/A missions, the plant designer will also propose for staff consideration appropriate regulatory oversight measures for these non-safety SSCs. These measures may include a proper operational reliability assurance program and maintenance rule implementation, **and** proper short-term availability control mechanisms such as technical specification limiting conditions for operation and administrative control of shutdown configuration. In addition, deterministic requirements for risk-significant SSCs will be included in the design certification rule. These regulatory oversights will ensure that the risk significant non-safety SSCs are designed, constructed, maintained, and operated in accordance with their R/A missions.

Section 22.1, page 22-3, Item (3) of NUREG-1512 repeated the statement about "O-RAP **or** simple technical specifications" as quoted above (first bullet) from SECY-94-087 before Section 22.5.4.3, page 22-17, of NUREG-1512 goes on to describe that "administrative controls are formatted similar to Technical Specifications, with operability requirements, applicability, actions and completion times if operability requirements are not met, surveillance requirements, and bases for the availability controls" with "no limiting conditions for operation."

Consistent with the staff position quoted above from NUREG-1242, Volume 3, Part 2, the design certification rulemakings for AP600 (10 CFR Part 52, Appendix C), AP1000 (10 CFR part 52, Appendix D), and ESBWR (proposed rulemaking in 76 FR 16549–16570, March 24, 2011) identify the short-term availability controls given in the applicants' DCDs and further includes a statement that commits the COL applicant as follows: "An applicant or licensee referencing this appendix, in accordance with Section IV of this appendix, shall incorporate by reference and comply with the requirements of this appendix, including Tier 1, Tier 2 (including the investment protection short-term availability controls in Section 16.3 [for AP600 and AP1000 but Appendix 19ACM for

ESBWR] of the DCD), and the generic TS except as otherwise provided in this appendix."

However, it is not clear at this juncture that NRC will require the COL applicants to invoke/reference and summarize the short-term availability controls as technical specifications design features in Specification 4.0 or as administrative controls in Specification 5.4 (Procedures) or Specification 5.5 (Programs and Manuals) in the plant-specific technical specifications. As quoted above, Section 22.5.4.3 (page 22-17) of NUREG-1512 actually refers to these as "short-term ***administrative*** availability controls" and "administrative controls" but without stating that these will be in the generic technical specifications as such. Such an approach might obviate intervener contentions by including an invocation of the non-technical specifications controls in the license but it is unclear as to whether that would be sufficient to address not invoking LCO selection Criteria 3 or 4 in the current regulations at 10 CFR 50.36(c)(2)(ii)(C) and (D) to require the short-term availability controls to be made into technical specifications with LCOs until such time as there is sufficient operating experience to warrant their removal or reduction to a TS-cited administrative control.

One might argue of course that the short-term availability controls for the active nonsafety-related systems (that is, RTNSS) fall under O-RAP not technical specifications. The problem here is the O-RAP is also not at first glance clearly regulation-based. If one goes to SRP 17.4 or the more recent DC/COL-ISG-018, the first basis one finds is the SRM on SECY-95-132 with secondary references to the Maintenance Rule (10 CFR 50.65) and Appendix B to 10 CFR Part 50 (QA Rule).[1] O-RAP has its basis or initial definition in SECY-89-013, "Design Requirements related to the Evolutionary Advanced Light Water Reactor (ALWRS)," January 19, 1989 (ML003707947), which states:

> RELIABILITY ASSURANCE:
>
> Certification of a design will be based in part upon a probabilistic risk assessment (PRA) of that design. In that the validity of a PRA is highly dependent on the reliability of systems, structures, and components, the staff requires assurance that programs will be implemented that will ensure that the reliability of those systems, structures, and components (assumed in analyses) will be maintained throughout plant life. Therefore, a program to ensure design reliability must be provided as part of the FDA application. This program, which will be certified as part of the design, should address items such as (1) the Technical Specifications and Inservice Inspection/Inservice Testing (ISI/IST), (2) the maintenance program, (3) plant procedures, **and** (4) security.

With some effort, the heredity of the O-RAP may be traced to the TMI Action Plan (NUREG-0737) wherein reliability analyses were required for auxiliary feedwater systems (Action Plan Items II.E.1.1 and II.K.2.8; later 10 CFR 50.34(f)(1)(ii)(A)) and the in-core instrumentation systems for core cooling (Action Plan Item II.F.2; later 10 CFR 50.34(f)(1)(xviii)). When the TMI Action Plan was implemented in the regulations, 10 CFR 50.34(f)(1)(i) required a "plant/site specific probabilistic risk assessment, the aim of

[1] SRP 17.4 Acceptance Criteria citing SECY-95-132 states that "the requirement to provide a reliability assurance program is codified by incorporation within the design-specific rulemaking for an applicant for design certification." However, this is not in the AP600 or AP1000 DC rule and is only in the statements of considerations not in the proposed rule for the ESBWR.

which is to seek such improvements in the reliability of core and containment heat removal systems as are significant and practical and do not impact excessively on the plant (II.B.8);" although Action Item II.B.8 is not found in either NUREG-0737 or its Supplement No. 1, it is indicated to be a future activity of the TMI response per Section 3.1 of the TMI lessons-learned report in NUREG-0578. Further, 10 CFR 50.34(f)(2)(ii) requires establishing "a program, to begin during construction and follow into operation, for integrating and expanding current efforts to improve plant procedures." where "The scope of the program shall include...reliability analyses...(I.C.9)." In turn, TMI Action Item I.C.9 stems from Recommendation 2.1.9 in the TMI lessons-learned report in NUREG-0578 which Recommendation was concerned mostly with emergency operating procedures; however, NUREG-0578 was repeatedly concerned with achieving "high operational reliability for performance of safety systems." In the regulations at 10 CFR Parts 50 and 52,[2] the verbiage "reliability assurance" never appears, and the verbiage "reliability analysis" or "reliability analyses" only appears in the discussion of the AFWS at 10 CFR 50.34(f)(1)(ii)(A) and for the procedural improvement program at 10 CFR 50.34(f)(2)(ii). Thus, it appears that the regulatory bases for O-RAP lies in the 10 CFR Part 50 TMI Action Plan regulations, but these never are cited in SRP 17.4 or DC/COL-ISG-018. However, the intent quoted above in the inclusive statements from SECY-89-013 as well as the previous quote from Section 3.2.2 (page 3.2-7) of NUREG-1242, Volume 3, Part 2, using the word "and" to link O-RAP to technical specifications appears to be that technical specifications are part of the O-RAP not separate from O-RAP as perhaps implied by the "or" statement on page 3 of the Enclosure to SECY-94-084 and in Section 22.1 (page 22-3) of NUREG-1512 as quoted above.

The recent issuance of draft SRP 19.3 in October 2012 does not clarify the issues:

(1) What is the regulatory basis for the "short-term ***administrative*** availability controls" cited in Chapter 22 of NUREG-1512?

(2) Why, given the lack of relevant operating experience with the new passively-safe designs, are these short term availability controls not technical specifications subject to LCOs under the existing regulatory criteria issued in 10 CFR 50.36(c)(2)(ii)(C) and (D) given that RTNSS are active systems that:
   (a) Will constitute the "primary success path" in all accidents and transients in which ac electrical power remains available thus preventing such challenges from progressing to "design basis accidents or transients?"
   (b) Are selected based on their reliability/availability being shown by PRA to be "significant to public health and safety?"

Without more definitive rulemaking on RTNSS, the current record of regulatory and staff positions is mixed, confusing and somewhat counterintuitive about the basis for short-term availability controls being outside of technical specifications compared to the very

[2] The word "reliability" appears 14 times in 10 CFR Part 50 including those discussed in this paragraph and refers elsewhere to emergency ac electrical power (10 CFR 50.2 and 50.63), structural integrity (10 CFR 50.55a), RISC-3 equipment (RTNSS-type in 10 CFR 50.69), and GDC 21, 24 and 61 either in regard to separation and independence or testability. The word "reliable" appears 12 times about specific items of equipment or analysis methods such as in Appendix K. In 10 CFR Part 52, "reliable" does not appear, and "reliability" is only found in 10 CFR 52.63(a)(1)(vi) with regard to factors considered in Commission decision-making on changes to a design certification.

specific requirements in 10 CFR 50.36(c)(2)(ii)(C) and (D). O-RAP has a regulatory basis that is never cited in the implementing guidance in SRP 17.4 and DC/COL-ISG-018, but O-RAP is not an "either-or" situation since it apparently is intended to include technical specifications per SECY-89-013 as well as other procedural controls among which technical specifications are not listed in 10 CFR 50.34(f)(2)(ii). It is interesting to note that Westinghouse placed the short-term availability controls in Section 16.3 of the AP600 DCD not in Chapter 17 and used the same format in the AP1000 DCD (consistent with the statements from the Areas of Review from draft SRP 19.3 quoted above); however, General Electric-Hitachi elected to place these as an appendix in Chapter 19. Obviously, these different vendors had different interpretations of the regulatory record. Both design certification applicants point to their STS as the basis for formulating their generic TS with no discussion as to whether these administrative controls embedded in the short-term availability controls will be included in Specification 5.4 or 5.5 which would be the only practicable means to provide adherence to the assurance required by NRC in the design certification rulemaking short of including them as technical specification LCOs given the lack of operating experience to justify otherwise.

Conclusions

There is currently no legal or technically-justified basis by rulemaking or relevant operational experience to justify the acceptance of investment protection short-term administrative availability controls in lieu of technical specification LCOs as required under LCO Selection Criteria 3 and 4 in 10 CFR 50.36(c)(2)(ii)(C) and (D). Further O-RAP lacks a definitive regulatory basis except only by inference from TMI Action Plan regulations in 10 CFR Part 50, and O-RAP does not obviate the need for technical specification LCOs. In fact, the initial origins of O-RAP in SECY-89-013 indicate that the originally expressed intent was that technical specifications are an integral part of O-RAP where O-RAP is not a distinctive standalone. In addition, the selection of RTNSS based on PRAs that are not fully transparent by hiding behind claims of proprietary nondisclosure requirements is unacceptable and a likely source of abuse of privilege. This situation needs rectifying by rulemaking that is open and subject to public comment. Draft SRP 19.3 does not satisfy this need by itself and only perpetuates bureaucratic confusion in the absence of legitimacy and clarity in rulemaking in which NRC documents its rationale and the public is given the opportunity to review that rationale under the legal requirements of 5 *U.S.C.* 553(b).