B&W mPower™ DSRS Section 7.1 Comment Sheet

No.	Type	Sub-Section	Comment:

1.	E,S	7.1.1(V)
		7.1.2(V)
		7.1.3(V)
		7.1.4(V)
			Subsection V (Implementation) text is identical in Sections 7.1.1 through 7.1.4 (fundamental design principles independence, redundancy, determinism, and diversity and defense-in-depth). To avoid this unnecessary repetition, suggest that implementation be addressed generically by moving Subsection V text to Section 7.1. Sections 7.1.1 through 7.1.4 would continue to include the Subsection V title; however, the text under each of these sections would simply refer to Section 7.1 for discussion of implementation (similar to how Section VI (References) is currently treated in Sections 7.1.1 through 7.1.4).

2.	E	7.1, 1st paragraph, last line	To be consistent within Section 7.1 and with other Commission documents (e.g., DI&C-ISG-02), revise "defense-in-depth and diversity" to "diversity and defense-in-depth"
3.	T	7.1, 2nd paragraph, 2nd sentence	Reference is made to NUREG-0800, Part II for description of the staff's review philosophy and framework for new iPWR design certification and COLA. Part II to NUREG-0800 does not exist – please clarify.
4.	T	7.1.1(II)	In the DSRS acceptance criteria section, item (3) refers to using the guidance in IEEE 7-4.3.2-2003, clause 5.6 which states that Appendix E should be referred to for guidance on communication independence criteria. However, the current revision of Reg. Guide 1.152 (rev. 4) does not endorse Appendix E of IEEE 7-4.3.2-2003. There seems to be a conflict here. Suggest clarification, or attributed from DIC-ISG-02 be incorporated.
5.	T	7.1.1(III)	The terminology that NRC staff reviewers will use "engineering judgment" to evaluate the design against power and control signer interdependencies potentially introduces confusion with applicants on how to be address these areas for the staff to effectively review and make a reasonable safety finding.
6.	T	7.1.1(III)	Under the section of "physical independence" this section refers to safety systems, protection and control systems. Suggest differentiating simply between safety and non-safety, and add "risk-significant" systems to discussions on physical independence attributes.
7.	T	7.1.1(III)	Under the section of "electrical independence," suggest adding that the isolation devices should be classified as safety related and meet all applicable qualification criteria in accordance with EQ requirements.
8.	Q	7.1.1(III)	Under the section of "communication independence," there is a multitude of information and guidance provided in DI&C-ISG-04, Section 1, that did not appear to be brought forward into the new DSRS. Are there any plans by the staff to incorporate the guidance in the ISGs into the DSRS?
9.	T	7.1.1(III)	Under the section of "Functional Independence," suggest additional guidance on the functional allocation and independence of safety related functions such as RTS and ESF. DI&C-ISG-02, section 6 contains guidance on the functional independence as it relates to the echelons of defense in the overall diversity and defense-in-depth analysis. This guidance could address functional independence within a single protection system division, and across multiple, redundant divisions.

[Type text]

© 2012 Babcock & Wilcox mPower, Inc. All Rights Reserved. This document is the property of Babcock & Wilcox mPower, Inc

B&W mPower™ DSRS Section 7.1 Comment Sheet

No.	Type	Sub-Section	Comment:
10.	T,S	7.1.2.I	Suggest in addition to the items listed, the application should address the issue that redundancy by itself is not sufficient to guard against common cause failures.
11.	T	7.1.2.I	Under the section of "Technical Rationale", suggest adding discussion on the single failure criterion and the potential that in some design elements, the issue of spurious actuations resulting from a single failure need to be addressed by a probabilistic risk assessment.
12.	S	7.1.3(II)	DI&C-ISG-4 contains several suggestions and reasonable guidance for addressing determinism in the I&C architecture design. Suggest a thorough review of these for incorporation into the DSRS.
13.	Q	7.1.3(I)	If the DCA is Digital platform neutral with how does the reviewer "specifically evaluate the real time deterministic performance of the digital I&C platform." Does this section no become an ITACC item or DAC?
14.	Q	7.1.3(II) 2,3	Same comment as above. If we are hardware neutral how do we satisfy these requirements associated with real time performance for the hardware and software?
15.	T	7.1.3(II)	Suggest adding/clarification of the definition of "real time system" (i.e., NUREG-CR/6083).
16.	E,S	7.1.3(II)	Under the DSRS Acceptance Criteria section, item (5): Suggest alternate terminology with less ambiguity than a "risky design practices." Could rephrase to state: "Design practices that do not implement rigorous real-time and deterministic performance in digital I&C systems such as…."
17.	T,S	7.1.3(IV)	Suggest adding item (6) in which applicants should provide a typical time response and system timing analysis that covers input process, logic processing, output processing, voting, etc. and incorporates the overall response time analysis for the protection safety functions.
18.	E, S	7.1.3(IV)	Under item (5), suggest rewording to remove ambiguity in terminology (see comment #16).
19.	Q	7.1.4	Should the DSRS address both diversity and defense-in-depth with the actual safety systems, or the application software that is used to develop/program the safety-system (e.g., VHDL with FPGAs)?
20.	Q	7.1.4(III)	10CFR50.62 contains language for vendor-specific reactor designs (e.g., B&W) and implementation of the ATWS rules. We need to clarify this as it relates to the mPower reactor design.

21.	E, Q	7.1.1(III)
		7.1.2(III)
		7.1.3(III)
		7.1.4(III)
			The first sentence in Subsection III (Review Procedures) in Sections 7.1.1 through 7.1.4 reads: "Specific DSRS acceptance criteria acceptable to meet the relevant requirements of the NRC's regulations identified above are as follows for review described in this DSRS section." This sentence appears to be out of place – Was it intended to be the first sentence under the title "DSRS Acceptance Criteria" for Sections 7.1.1 through 7.1.4 instead?

22.	T, Q	Appendix B	In addition to the list of information the NRC staff will review, should the application add risk-significant and beyond-design-basis (severe accidents) elements that are part of the I&C function design basis?

© 2012 Babcock & Wilcox mPower, Inc. All Rights Reserved. This document is the property of Babcock & Wilcox mPower, Inc

B&W mPower™ DSRS Section 7.1 Comment Sheet

No.	Type	Sub-Section	Comment:
23.	T	Appendix B, #4	Add item in list to include the overall functional analysis of the I&C architecture.
24.	Q	Appendix C	Under section 4, it is not clear how item 4.A relates to redundancy?
25.	E	Appendix C	Item 3.B and 4.C both refer to inter-channel communications which is redundant. Suggest that this be revised.
26.	T, Q	Appendix C	How will a reviewer determine the level of "simplicity" or "complexity"? Are there qualitative or quantitative criteria that can be referred to? This seems very subjective. One possibility is to provide review guidance that applicants must identify all primary functions required for the system to achieve its safety function, and then justify any extraneous functionality. A clear presentation of both the safety and performance requirements will add to determine that all functions trace back to these criteria.
27.	E	App C, Pg 7.1-25, next to last paragraph, 5th line	Delete the additional space following the term "etc"
28.	Q	Appendix C.6 (2nd B)	The DSRS states that the reviewer "consider whether basic software is implemented in high level programming language", does this mean we need to commit to a programming language in the DCA?
29.	Q	Appendix C.6 (2nd D)	Same comment as above, do we need to commit to a software language in the DCA
30.	T, Q	Appendices C & D	While we understand that NRC mPower DSRS Sections 7.1.1 – 7.1.4 (Fundamental Design Principles) generally include discussion on software, much of the discussion on software implies a Von Neumann or Harvard architecture (micro) processor. Should references and guidance be included to address FPGA and related VHDL (or other HW descriptive language) software instantiated non-microprocessor-based logic, (e.g. NUREG/CR-7006)?
31.	E, Q	Appendix D	It is not clear why references 21-34 (IEC-61000) are included?
32.	S, T	Appendix D	Suggest adding IEC 61508, "Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems" be included.

Key (to Type of comment)

E – Editorial
S – Suggestion
Q – Question
T – Technical

© 2012 Babcock & Wilcox mPower, Inc. All Rights Reserved. This document is the property of Babcock & Wilcox mPower, Inc