FPL

July 7, 2014
L-2014-184

6/5/2014
79FR32578

4

Ms. Cindy Bladey
Chief, Rules, Announcements and Directives Branch (RADB)
Office of Administration
Mail Stop: 3WFN 06-44M
U.S. Nuclear Regulatory Commission
Washington, DC 20555–0001

Subject: Request for Comments on Draft Regulatory Issue Summary, "Embedded Digital Devices in Safety-Related Systems" (Docket ID: NRC-2014-0129)

Florida Power and Light Company, the licensee for the St. Lucie Nuclear Plant, Units 1 and 2, and the Turkey Point Nuclear Plant, Units 3 and 4, and its affiliates, NextEra Energy Seabrook, LLC, the licensee for the Seabrook Station, NextEra Energy Duane Arnold, LLC, the licensee for the Duane Arnold Energy Center, and NextEra Energy Point Beach, LLC, the licensee for the Point Beach Nuclear Plant, Units 1 and 2 (hereafter referred to collectively as "NextEra"), hereby submit comments on the draft Regulatory Issue Summary 2014-XX, "Embedded Digital Devices in Safety-Related Systems," published in the Federal Register on June 5, 2014 (79 FR 32578).

NextEra endorses the comments of the Nuclear Energy Institute (NEI), dated July 7, 2014. NextEra offers the attached table of comments which provides additional perspective on the NEI comments.

We appreciate the NRC's consideration of NextEra's comments.

Sincerely Yours,

James M. Petro, Jr.
Nuclear Licensing and Regulatory Compliance Director

SUNSI Review Complete
Template = ADM – 013
E-RIDS= ADM -03
Add–
E. Eagle (eoe)

Florida Power & Light / NextEra Energy

Comments on Draft Regulatory Issue Summary 2014-##
"Embedded Digital Devices in Safety-Related Systems" (Docket ID NRC–2014–0129)

#	Section, Page, Line #	Comment	Proposed Resolution
1	General Comment	The RIS provides a very wide interpretation of the function and use of embedded digital devices. This leaves the position of the NRC up for continuous interpretation and revision. The INTENT Section stated is to provide a "technical" position on existing regulatory requirements.	The RIS should provide clear technical positions that may be used by the industry. General references to other industry documents or Regulatory Guides should be specific.
2	INTENT	The RIS indicates that it applies only to I&C in safety related systems and then later describes embedded digital devices *used in Electrical systems for power distribution which are* typically not I&C systems.	A clear scope is needed for this RIS.
3	INTENT	The RIS states that it is limited to Safety Related systems and then in the next sentence states that it applies to embedded systems in non-safety systems.	Any reference to non-safety systems should be eliminated throughout the RIS.
4	General Comment	This RIS appears to be focused on Software Common Cause Failure (SCCF) and does not address more generic common cause failures (CCF) that would be part of a Common Cause Analysis (CCA). While a software failure may be the cause of a CCF, there are other systematic failures which manifest themselves as software failures but are caused by expected external events such as lightning, EMI, RFI, etc.	The RIS should approach this subject from a CCA perspective vice drilling down on one part of a CCA which is represented by the SCCF. SCCF are those failures where the causal factor is the software (functional requirement failure, hardware failure, human coding errors, etc) vice conditions where the software may be damaged or corrupted by external events. A CCA would better serve the industry vice only evaluating a SCCF.
5	Background Information	NRC guidance from BTP 7-19 does not provide any reference to embedded digital devices.	A reference should be provided that supports the RIS position on embedded digital devices.
6	Page 1, Section INTENT, 2nd Paragraph	By title, the RIS is applicable to safety-related systems. The statements within this paragraph expand the scope to include non-safety-related systems.	Other than the first sentence, consider deleting the entire paragraph.
7	Page 2, Section BACKGROUND INFORMATION, 1st paragraph	(a) Consider expanding the 1st sentence to add perspective to this background statement (b) The 3rd sentence does not add perspective to this paragraph and should be deleted.	(a) "...and fluid systems) in response to increasing obsolescence and age-related failures or where analog spare parts are neither available nor can they be substituted." (b) Consider deleting the 3rd sentence in its entirety

8	Page 2, Section BACKGROUND INFORMATION, 2nd paragraph, (ends on the top of Page 3)	The definition appears too broad and includes, to a large extent, digital devices that are already enveloped within Regulatory and industry guides and standards. The definition should be narrowed to those devices within the RIS target population of concern.	Consider revising the paragraph in its entirety to the following: "For purposes of this RIS, an embedded digital device is a stand-alone or actuation device (that is not thought of as a computer), but contains embedded software written to control that stand-alone or actuation device, where the software performs one or more functions that is specialized for the particular device that it runs on, along with time and memory constraints. [NOTE: Embedded software in this case should not be used interchangeably with firmware because firmware can be applied to ROM-based code on a computer, on top of which the OS runs, whereas embedded software is the only software on the device]"
9	Page 3, Section BACKGROUND INFORMATION, 3rd paragraph	The statements made in this paragraph are challenging for two reasons: (1) BTP 7-19 makes no direct reference to embedded digital devices; and, (2) BTP 7-19 criteria is intended for regulatory guidance only and not as criteria for industry use when implementing digital upgrades. (Reference: NRC Letter, Dated August 12, 2013 to the Shearon Harris Nuclear Power Plant, Titled: *Shearon Harris Nuclear Power Plant Unit 1 – NRC Evaluation of Changes, Tests, and Experiments and Permanent Plant Modifications Baseline Inspection Follow-up Report 05000400/2013009.*	Consider deleting paragraph in its entirety.
10	Page 3, Section BACKGROUND INFORMATION, 4th paragraph	Recommend editorial changes for clarification purposes.	2nd Sentence: "The embedded software within an embedded digital device..." 3rd Sentence: "...exclude the application of embedded digital devices from consideration within an assessment..."

11	Page 3, Section BACKGROUND INFORMATION, 5th paragraph	Using NRC IN 1994-020 may not be a good example for demonstrating the concern expressed in the RIS for two reasons: (1) The condition was not the result of a software common cause failure. The condition was the result of a common mode failure resulting from a design review that did not ensure that replacement equipment was compatible with the specific application service environment. This was clearly a design deficiency regardless of the digital aspects of the device. (2) The OE is significantly dated. This was clearly acknowledged as such by the cross-reference to industry documents published since the event occurred.	Consider deleting in its entirety.
12	Page 3, Section BACKGROUND INFORMATION, 6th paragraph	Using NRC IN 2007-015 may not be a good example for demonstrating the concern expressed in the RIS for two reasons: (1) The RIS is attempting to demonstrate the importance of a "software common cause failure (CCF) of redundant safety-related equipment using components with non-diverse embedded digital devices." However, the event that occurred as described in IN 2007-015, does not demonstrate this. IN 2007-015 states in conclusion that the industry needs to focus on "design and control of network architecture". (2) Same as comment 6.	Consider deleting in its entirety.
13	Page 4, Section BACKGROUND INFORMATION, 7th paragraph	The latter part of the second sentence through to the end of the paragraph appears to tangent off into a discussion of electromagnetic compatibility (EMC). EMC is an important in-service environment design consideration, but it is not the only one. Also, there appears to be no clear discussion as to the tie between EMC and software failure.	Consider deleting in its entirety.

14	Page 4, under SUMMARY OF ISSUE, 1st paragraph	The first sentence states the following: "The key is that the increased use of embedded digital devices in safety-related equipment may increase a facilities vulnerability to a CCF..." However, no basis is stated as to what the "increase" is compared to. The first sentence goes on to state, "...challenge equipment to EMC..." Here again (see comment 13 above), EMC is neither the issue nor a demonstrated cause of software CCF with embedded digital devices. The first sentence concludes with, "...or otherwise degrade equipment reliability to adversely affect safety. There appears to be no point of reference given or an OE analysis that would reach that conclusion.	Consider deleting the first sentence in its entirety.
15	Page 4, under SUMMARY OF ISSUE, 1st paragraph, Item (2)	Item (2) assumes a new failure mode exists that could result in a CCF. Therefore, the statement needs clarification as such.	Revise Item (2) as follows: "*the need to address new failure modes, and if a new failure mode* exists, address the potential vulnerabilities to software CCFs; and,"
16	Page 5, under SUMMARY OF ISSUE, 2nd to last bullet	Reference to BTP should be removed based on discussion in Comment 5, above.	Consider removing reference to BTP 7-14
17	Page 6, under SUMMARY OF ISSUE, the 2nd paragraphs before item (2)	The first statement may not be accurate because IEEE 379-2000 was endorsed by Reg. Guide 1.53, Revision 1, and addresses actuation devices. The second statement should be clarified to more closely represent issue and application of embedded software in actuation devices.	Consider deleting first sentence in its entirety Consider revising the second sentence as follows: "Manufacturers are increasingly introducing digital technology into non-actuation and actuation devices that, in turn, are used in applications such as; digital displays, motor controllers, sequencers, pumps, valve actuators, breakers, uninterruptible power supplies, emergency diesel generator controls, etc."
18	Page 6, under SUMMARY OF ISSUE, the first paragraph before item (2)	Clarification is needed to address commercial grade items	Revise a portion of the paragraph as follows: "...non-digital technology is being replaced with commercial grade devices that contain embedded software that may not have been developed in accordance with..."

19	Page 6, under SUMMARY OF ISSUE, Item (2), 3rd bullet	Reference to BTP 7-19 should be removed based on response to Comment 5 above.	Consider removing reference to BTP 7-19.
20	Page 6, under SUMMARY OF ISSUE, last paragraph on the page	The second sentence does not appear to clearly communicate the adverse effect of the software CCF concern and should be clarified.	The second sentence should be revised to state the following: "It may be possible that an intended safety protection feature could be defeated by a new software failure mode of an embedded digital device and result in a software common cause failure when the same embedded digital device is used in the redundant safety system execute feature."
21	Page 7, SUMMARY OF ISSUE, top paragraph	Same response as Comment 1, above	Consider deleting paragraph in its entirety.
22	Page 7, SUMMARY OF ISSUE, second from the top paragraph	Same comment as Comment 4, above.	Consider deleting paragraph in its entirety.
23	Page 7, under SUMMARY OF ISSUE, Item (3), 2nd paragraph	The first sentence should be clarified to ensure specifications to vendors apply to more than just commercial products.	Consider revising the first sentence as follows: "...specifications for vendors supplying safety-related and commercial products targeted for commercial grade dedication, requirements to identify the use of..."