EPRI | ELECTRIC POWER RESEARCH INSTITUTE

6/5/2014
79FR32578

June 23, 2014
PT-061814-044

1

Cindy Bladey,
U.S. Nuclear Regulatory Commission
Office of Administration
Mail Stop: 3WFN, 06–44M
Washington, DC 20555–0001

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

Dear Ms. Bladey:

This letter responds to the June 5, 2014 Federal Register Notice (79FR32578) seeking comment on the subject Draft Regulatory Issue Summary (RIS). Our comments are compiled in the attached table.

If you have any questions, please contact me by email or at (650) 855-2310.

Sincerely,

RC Torok

Raymond C. Torok
Principal Technical Leader
Electric Power Research Institute (EPRI)
Phone: 650-855-2310
Cell: 650-387-5905
E-mail: rtorok@epri.com

Attachment

c: R. Austin
K. Canavan
M. Gibson
T. Taylor
G. Clefton, NEI

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

EPRI 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	The draft RIS seems appropriate and helpful in calling attention to embedded digital devices in plant equipment and their potential for creating undesired behaviors, including common-cause failures (CCF). However, it seems to be overly reliant on diversity as a protective measure against CCF. It does not mention other protective measures that may be more appropriate and effective for embedded digital devices. As written, the guidance could lead to greater use of less-than-optimal approaches for protecting against CCF in embedded devices, with attendant adverse effects on safety. However, relatively minor changes could help remedy the situation.	
9	Page 1, Intent, second paragraph and page 7. "Summary of Issue" section 2	This RIS is limited to safety related equipment. However, there is extensive discussion of non-safety CCF within the "Intent" section and Summary of Issue" section that will lead to some confusion and possibly the incorrect assumption that safety related requirements must be applied to non-safety equipment. Of particular concern is the scope of the second point: "the need to address potential facility vulnerabilities to CCFs", as this should be applicable only to CCF of safety related equipment.	Discussion of non-safety CCF is out of scope for this RIS and should be removed to: 1. Provide better clarity and focus of the stated scope and intent of the RIS. 2. Reduce confusion and enhance implementation of the RIS The discussion of non-safety CCF is better discussed in other products
10	Page 2 and 3, definition of "embedded digital device "	The definition and extended list of technology (ASIC, etc.) has become overly broad and ambiguous. The full definition of "software- developed firmware" and "software-developed logic" needs additional definition. The inclusion of various host technologies would include nearly all electronics, analog or digital. Workable definitions that define the scope of the RIS more deterministically is recommended as the current definition will hinder RIS implementation.	Refine the definitions to deterministically exclude electronic circuitry that does not include a load, store, execute architecture or working memory. Structure the definition to differentiate the means of execution from the means of program storage.

2	Page 2, third paragraph, third sentence	The statement seems to assume that non-diverse components have a significant likelihood of CCF and diverse components do not. Neither is necessarily true. There is no guarantee that diverse components performing the same function won't both be vulnerable to potential triggers of software faults (for example, Y2K, out of range inputs, invalid timing signals, network communication disturbances, etc.). The emphasis should not be on ensuring diversity, but on ensuring reasonable assurance of adequate protection against CCF. CCF protection would probably consist of some combination of preventive design measures (possibly including internal diversity), that preclude certain types of CCFs by avoiding triggers that might activate them, and mitigation measures that enable the plant to cope with such failures.	An alternative statement that might be better is: *Addressees should be aware that embedded digital devices in redundant safety-related components (including components implementing safety-related execute features such as motor control centers and actuated equipment) could introduce potential for common-cause failure (CCF) due to designed-in software faults or defects.*
3	Page 2, fourth paragraph, second sentence	This statement appears to assume that diversity is the one and only way to protect against CCF. Again, the assessment should be about protection against CCF – not just diversity.	An alternative statement that might be better is: *Inadequate consideration of these devices in assessing susceptibility to potential software CCFs could lead to an adverse safety consequence.*
4	Page 3, second full paragraph, third sentence	Again, the RIS seems to assume that diversity is the one and only way to protect against CCF.	An alternative statement that might be better is: *However, NRC staff guidance does not automatically exclude the application of these (so-called "simple") devices containing the firmware from consideration within an assessment of vulnerabilities to potential CCF.*

5	Page 3, second full paragraph, fourth sentence	Design measures that preclude or reduce the likelihood of various types of failures and CCFs should be added to this list. Good process attributes (e.g., design documentation, quality development, testing, etc.) do not ensure a good design. Simplicity is good in that it makes it easier to anticipate undesired behaviors and failure modes and achieve more complete test coverage. Diversity can be helpful in either preventing or mitigating certain types of CCFs, but it increases complexity, and is not always appropriate. For example, diversity among redundant divisions that all have the same functional requirements does not protect against CCFs that originate in requirements specification faults (which various researchers have concluded is the most likely place to introduce a fault in a high integrity system). And there is no guarantee that such diverse systems will not be susceptible to the same stressors (for example, Y2K or out of range data or an invalid timing signal). Diversity should be encouraged where it makes sense, but not mandated, and the RIS should also encourage use of good design features (for example, data validation, watchdog timers, cyclic software architecture with no branching, invariance with respect to plant transients, etc.), which greatly reduce the likelihood of software-related failures and arguably can provide simpler solutions and greater assurance of adequate protection against failures and CCFs.	An alternative statement that might be better is: *Nevertheless, several potentially important factors may be considered within a CCF assessment to evaluate the suitability for use of an embedded digital device, including:* • *simplicity* • *design features and measures that preclude or reduce the likelihood of failures and CCFs* • *diversity* • *design documentation* • *quality development* • *testing* • *operational history*
6	Page 3, last paragraph	The example of IN 2007-015 seems out of place in this RIS. While this is a good example of a CCF vulnerability introduced by digital equipment, it really is about the use of shared resources, not embedded digital devices. It is also a good example of a case where design measures that protect against broadcast storms, or segmentation of the I&C architecture to limit the extent of a failure, are the appropriate protective measures for CCF – not diversity.	One alternative is to simply delete this example. Another is to leave it in and use it to explain that diversity is not the only way to protect against CCF and that preventive measures against CCF can be implemented outside the digital components that might be affected by the CCF

7	Page 6, Section (2)	If BTP 7-19 is applied to embedded devices as written, it might force the use of diversity as the only practicable way to meet the guidance (100% testability is rarely a viable option for digital devices, and demonstrating CCF coping capability per the BTP might not always be possible). This could effectively force the use of diversity in the components that contain the embedded devices, which would further complicate training and maintenance concerns. It is not clear whether the net effect on safety would be positive. Perhaps a supporting analysis, including cost-benefit considerations would be helpful.	If BTP-19 is not going to be revised, and its guidance is intended to be applied to embedded systems, then some additional guidance should be provided on the need to consider cost-benefit and the net effect on safety of using diverse components rather than simplicity and other preventive design measures to address CCF concerns
8	Page 7, second paragraph	BTP-19 is limited in that it recognizes only 100% testability and diversity as evidence of adequate preventive measures for CCF. (It also allows for a demonstration of coping capability as evidence of adequate CCF protection). However, it does not consider defensive design measures and other metrics for simplicity, which may be more appropriate and effective CCF protection solutions for embedded equipment.	This endorsement of BTP-19 should probably be tempered until BTP-19 is revised. An alternative statement that might be better is: *The guidance in BTP 7-19 describes some approaches for addressing potential CCFs of embedded digital devices located in equipment performing safety-related system execute features.*