

Gallagher, Carol

From: Ross, James2 (GE Power & Water) [james2.ross@ge.com]
Sent: Wednesday, July 20, 2011 12:11 PM
To: Gallagher, Carol
Subject: Docket ID NRC-2011-0109 NUREG/CR-XXXX
Attachments: NUREG_Software_Failure_JYL_Comments.docx

Please see attached GE-Hitachi comments on the subject Docket ID titled " Development of Quantitative Software Reliability Models for Digital Protection Systems of Nuclear Power Plants, Draft Report for Comment".

<<NUREG_Software_Failure_JYL_Comments.docx>>

Sincerely,
James A Ross
VP, Nuclear Licensing
GE Hitachi Nuclear Energy

1299 Pennsylvania Ave. NW
Suite 900
Washington, DC 20004
T 202 637.4160
F 202 637.4016
C 202 412.9632
E james2.ross@ge.com
www.ge-energy.com/nuclear

5/18/2011
76 FR 28819
①

RECEIVED

JUL 20 PM 12:27

RULES AND DIRECTIVES
SECTION

*SONSI Review Complete
Template = ADM-013*

*E-RTDS = ADM-03
Add = A. Koritzky (ASK1)*

The following are comments on NUREG/CR-XXXX, Development of Quantitative Software Reliability Models for Digital Protection Systems of Nuclear Power Plants Draft Report for Comment:

#	Section, para.	Description
1.	1.2, 2 nd para.	The discussion on control and protection systems should have more discussion on the two software failure modes that are typically modeled: the failure of its designed functions, and the spurious failures, which are not designed. Both the failure of designed function and the spurious software failure could result in a plant trip. It could also result in loss of some mitigation systems / functions.
2.	General	This draft does not seem to have addressed the dynamic nature of software. The test designed for the software may capture the majority of failures. However, certain combinations of inputs may not be covered by the tests since the inputs to the software in an accident scenario would be evolving all the time. Attempt of context-based software failures has been documented in later sections. However, it is not clear on how to model the software behaviors in different accident scenarios and during different phases in a certain accident.
3.	2.1, last para.	The end of this section states: "Therefore, CCF across different systems, whether they are considered to be diverse or not, is beyond the scope of this study." However, software CCFs across different systems are the dominant risk contributors to new reactor designs. The exclusion of software CCFs may not be well justified.
4.	2.2.1, 2 nd para.	The discussion of SRGMs seems to focus on the characteristics of software development phase (i.e., failures are identified and fixed during the debugging and testing phases). However, the software failures modeled in a nuclear power plant PRA should reflect the fact that the software has ended its development phase. During the operation phase, software failures will be reported and fixed. However, such fixes may not be fully tested as in the original design phase, which could result in other breaks. In summary, the adoption of SRGMs should be further evaluated with the above identified concern.
5.	6.2.2.1	This section includes some examples for the calculation of software failure's contributions. The assumed cutsets only include one software failure, which may not reflect the actual designs, especially the new reactor designs.
6.	6.2.2.2	Similar to the comment for section 6.2.2.1, the calculation assumes that only one software failure is required to be modeled. This may not be appropriate for new reactor designs. For example, a non-safety system function may be failed by the non-safety control software, or by the spurious software failures from the safety-related control/protection system (e.g., isolation system).