

NRCREP - Progress Energy Comments on NUREG/CR-XXXX, "Approaches for Using Traditional Probabilistic Risk Assessment Methods for Digital Systems," (72 FR 58338 10/15/2007)

From: "Miller, David (Bryan)" <David.Miller@pgnmail.com>
To: <nrcprep@nrc.gov>
Date: 11/14/2007 2:09:34 PM
Subject: Progress Energy Comments on NUREG/CR-XXXX, "Approaches for Using Traditional Probabilistic Risk Assessment Methods for Digital Systems," (72 FR 58338 10/15/2007)

The Progress Energy comments on NUREG/CR-XXXX, "Approaches for Using Traditional Probabilistic Risk Assessment Methods for Digital Systems," (72 FR 58338, October 15, 2007) are attached. A hard copy of these comments will be placed in the US mail to the address indicated in the Federal Register notice.

D. Bryan Miller
Corp. Regulatory Affairs
Progress Energy
919-546-5243

10/15/07
72 FR 58338
3

<<07-062 McCabe - NRC Letter - Comments on NUREG-CR-XXXX Digital PRA.pdf>>

RECEIVED

2007 NOV 15 PM 5:29

RULES AND DIRECTIVES
BRANCH
USNRC

SUNSI Review Complete

Template = ADM-013

file://C:\temp\GW\00001.HTM

E-RIDS = ADM-03
Add = A. Kuritzky (ASK1)

11/15/2007

Mail Envelope Properties (473B47E1.3CC : 24 : 33740)

Subject: Progress Energy Comments on NUREG/CR-XXXX, "Approaches for Using Traditional Probabilistic Risk Assessment Methods for Digital Systems," (72 FR 58338 10/15/2007)

Creation Date Wed, Nov 14, 2007 2:09 PM

From: "Miller, David (Bryan)" <David.Miller@pgnmail.com>

Created By: David.Miller@pgnmail.com

Recipients

nrc.gov

TWGWPO01.HQGWDO01

NRCREP

Post Office

TWGWPO01.HQGWDO01

Route

nrc.gov

Files	Size	Date & Time
MESSAGE	456	Wednesday, November 14, 2007 2:09 PM
TEXT.htm	1378	
07-062 McCabe - NRC Letter - Comments on NUREG-CR-XXXX Digital PRA.pdf	274916	
Mime.822	380839	

Options

Expiration Date: None
Priority: Standard
ReplyRequested: No
Return Notification: None

Concealed Subject: No
Security: Standard

Junk Mail Handling Evaluation Results

Message is eligible for Junk Mail handling
This message was not classified as Junk Mail

Junk Mail settings when this message was delivered

Junk Mail handling disabled by User
Junk Mail handling disabled by Administrator
Junk List is not enabled
Junk Mail using personal address books is not enabled
Block List is not enabled



PO Box 1551
411 Fayetteville Street Mall
Raleigh NC 27602

Serial: PE&RAS-07-062
November 14, 2007

Chief, Rulemaking, Directives and Editing Branch
Division of Administrative Services
Office of Administration
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

SUBJECT: Comments on Draft NUREG/CR-XXXX, "Approaches for Using Traditional Probabilistic Risk Assessment Methods for Digital Systems," (72 FR 58338, October 15, 2007)

Ladies and Gentlemen:

Progress Energy is pleased to submit the attached comments on the subject draft NUREG/CR. Progress Energy is an active participant in the industry task force regarding the use of digital systems and regularly participates in Nuclear Regulatory Commission (NRC) public meetings on the subject. A summary of the attached comments is provided below.

- The term "software failure," as used in the report, warrants further clarification.
- The methods discussed in this report appear prohibitive due to the difficulty in determining accurate failure rates for the fault tolerant micro-processors in the digital system. Progress Energy looks forward to reviewing NRC work regarding the use of the "black box" method upon which it would be acceptable to model the digital system based upon the adverse consequences resulting from the failure.
- It is not clear what the bases would be for counting all maintenance errors or modification errors as "fatal errors."
- There are several instances of ambiguous or confusing use of acronyms throughout the report. Specific examples are attached.

Progress Energy looks forward to continuing its work with the NRC staff and the Nuclear Energy Institute on the safe application of digital systems in nuclear power plants. Please contact me at (919) 546-4579 if you have any questions.

Sincerely,

A handwritten signature in cursive script that reads "Brian McCabe".

Brian McCabe
Supervisor - Regulatory Affairs

DBM
Attachment

Progress Energy Comments on Draft NUREG/CR-XXXX

1. Use of the term "Software Failure"

The term "software failure" is used extensively throughout the report. This is misleading because software does not, strictly speaking, fail. As the report itself points out (see page C-1 discussion under "What is Software Failure?"), some software experts assert that "software does not fail because it invariably does what it is programmed to do." The observation that "the potential variability of the input to a software and the number of paths of execution with the software is so large that it is impossible to exhaustively test the software", while true, is not relevant with respect to supporting the claim that software does fail. The report also says, "Software design faults are an important cause of software failures." In reality, software design faults are the only subject of concern in this context. Whether introduced during initial development, during changes made as a result of testing, during the upgrade process, etc., every category of "software failure" the report attempts to define (see Table C-1) is ultimately a software design fault.

Since it's not realistic to expect that every use of "software failure" in the report be changed to "software design fault" (or some similar term), it is recommended that usage of the term "software failure" be explained at the beginning of the report, either within or immediately following the third paragraph in the "Background" section on page 1-1. The explanation should make the following points:

- The term "software failure" warrants clarification. Many experts would argue that software cannot fail. It can only do what it is programmed to do. This is an interesting discussion, but it is not the purpose of this report to argue or resolve such questions. However, it is important to explain up front how the report uses this term.
- In this report, the term "software failure" is used very broadly. The report frames the concept of software failure as "any deviation from the expected behavior" (e.g., "a violation of one of the functions"). This can refer to any situation in which functionality implemented at least in part by software in a digital system behaves in a way that is judged to be undesirable in the context of its specific application. This includes problems that arise from many sources. For example:
 - Programming errors that were missed by the verification and validation (V&V) and testing process
 - Unanticipated conditions - Requirements specifications that did not address every possible set of conditions that the system might be exposed to, including abnormal and faulted conditions
 - Incorrect requirements specifications
 - Applying a digital system in conditions it was not intended or tested for

Progress Energy trains its nuclear plant engineering personnel to understand that while hardware reliability can be improved through proper predictive, preventive, and corrective maintenance practices, software reliability must be designed in up front and maintained through rigorous adherence to appropriate procedures for software changes, regression testing, configuration management, etc. Plant personnel associate the concept of "failure" with the notion of something physically breaking. This is, in part, why the term "software failure," if not clarified early in the report, would likely mislead people.

Progress Energy Comments on Draft NUREG/CR-XXXX

2. Black Box Method

For current probabilistic risk assessments using event tree/fault tree (ET/FT), it is not clear why it would not be acceptable to model the digital system based upon the possible adverse consequences of the digital system failure using the black box method. For example, the digital feedwater control system has only a limited number of failures as a system, (overfeed of the steam generator an operator can correct, overfeed an operator cannot correct, loss of feed again that the operator may be able to correct and those the operator cannot correct, and under feed again with some operator recovery potential.) The only other failure modes for the black box method would be loss of power and loss of support systems. There should be data available to make much more reasonable estimates of the frequency of these events vice trying to determine the failure rate of fault tolerant micro-processors.

3. Fatal Errors

Errors introduced by changes or maintenance should be evaluated to determine how many of the 27% errors were "fatal errors" and how many were minor bugs or annoyances that were introduced. It is not clear what the basis would be for counting all maintenance errors or modification errors as "fatal errors."

4. Use of Acronyms

There are several instances of ambiguous or confusing use of acronyms:

- "DCS" is used for "digital control system"; however, "DCS" is typically understood by control system engineers to mean "distributed control system". Therefore, the use of "DCS" will lead some readers to believe that a "distributed control system" is being referred to when the broader category of "digital control system" is actually intended.
- "ISA" is defined as "industry standard architecture" in the acronyms list on page xvi, but it is never used to mean that in the report. "ISA" is defined as "integrated safety architecture" on page 4-15, but it also refers to the professional society/standards body formerly known as "Instrument Society of America" on pages 11-1 and C-34.
- "SFM" is defined as "software failure mode" in the acronyms list on page xvii, on page C-12, and in Table C-6 on page C-48, but it is also defined as "system failure mode" in Table C-2 on page C-17.
- "SRS" is defined as "Savannah River Site" in the acronyms list on page xvii, in Section 9.4.7 on page 9-22, and in Table 9-12 on page 9-23, but it also refers to the "Systems Reliability Service" in the references on page 11-5, and it is typically understood in the nuclear power industry to mean "software requirements specification".