NRCREP - Draft Report for Comment: NUREG/CR-XXXX, "Approaches for Using Traditional Probabilistic Risk Assessment Methods for Digital Systems"

From: "Wyant, Francis J" <fjwyant@sandia.gov>
To: <nrcrep@nrc.gov>
Date: 11/13/2007 2:36:24 PM
Subject: Draft Report for Comment: NUREG/CR-XXXX, "Approaches for Using Traditional Probabilistic Risk Assessment Methods for Digital Systems"

To whom it may concern:

The attached document provides comments on the subject report from the Nuclear Energy Safety Technologies staff at Sandia National Laboratories.

Regards,

10/15/07
72FR58338
(1)

Francis J. Wyant
Sandia National Laboratories
Org. 6761, MS-0748
(505) 844-5682, FAX: (505) 844-2829
Email: fjwyant@sandia.gov

<<SNL Comments on BNL draft.pdf>>

SUNSI Review Complete
Template = ADM-013

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

Mail Envelope Properties (4739FCB0.115 : 11 : 277)

Subject: Draft Report for Comment: NUREG/CR-XXXX, "Approaches for Using Traditional Probabilistic Risk Assessment Methods for Digital Systems"
Creation Date Tue, Nov 13, 2007 2:35 PM
From: "Wyant, Francis J" <fjwyant@sandia.gov>

Created By: fjwyant@sandia.gov

Recipients
nrc.gov
TWGWPO01.HQGWDO01
NRCREP

Post Office	Route
TWGWPO01.HQGWDO01	nrc.gov

Files	Size	Date & Time
MESSAGE	348	Tuesday, November 13, 2007 2:35 PM
TEXT.htm	1208	
SNL Comments on BNL draft.pdf	29854	
Mime.822	45679	

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

Sandia National Laboratories
Operated for the U.S. Department of Energy by
Sandia Corporation

Francis J. Wyant
SMTS

P.O. Box 5800
Albuquerque, NM 87185-0748

Phone: (505) 844-5682
Fax: (505) 844-2829
Internet: fjwyant@sandia.gov

November 13, 2007

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

Subject: NUREG/CR-XXXX, "Approaches for Using Traditional Probabilistic Risk Assessment Methods for Digital Systems"

To Whom It May Concern:

Sandia National Laboratories is pleased with the opportunity to provide the following comments on the subject report.

Overall the report was found to be well written and organized.

Methods Selection

The basis for selecting traditional ET/FT models and Markov models are presented in this chapter. The authors' justification for choosing the "best" two methods was not well explained. The authors list the different methodologies that could be used for assessing the reliability of digital systems. Although the descriptions are useful, they are not detailed enough to make a decision about which method is the best to adopt. The authors categorize methodologies into ET/FT-like methods ("traditional" ET/FT, "dynamic" FT, GO-FLOW, Binary Decision Diagrams), discrete-state continuous-time methods (Markov method, Petri Nets, SINTEF PDS Method), and other methods (Bayesian Belief Networks, Reliability Prediction Methods, Discrete Event Simulation such as Monte Carlo simulations, etc), but the discussions on the differences between methods within a given category were very superficial.

The reasons stated for proceeding with the traditional ET/FT method and Markov method were not well justified. The authors state that "heavy emphasis was placed on those methods likely to be used by the nuclear industry." The variations of ET/FT (dynamic FT, GO-GLOW, BDDs) were not further considered because traditional ET/FT models are already used in the nuclear industry. Was this the overriding basis for the decision?

The authors state that Markov models will be further investigated because Petri Nets and SINTEF PDS methods are essentially simplified versions of Markov models. They later state that Markov methods may be prohibitively complicated to construct and impractical to solve.

This in itself provides justification to further investigate the alternative "simplified methods." The authors should provide a better case as to why the Markov method was selected.

The authors do state the potential benefit of developing Hybrid methods combining the best of traditional and dynamic features, but do not follow through on this conclusion.

Evaluation Criteria

The authors define over 50 criteria for evaluating probabilistic models of digital systems, taking into account nine major issues. Issues like software reliability, complicated interdependences, etc. call attention to valid issues that are currently unresolved when evaluating reliability of digital systems. However, there are some listed criteria that are less important than others. Perhaps a weighting scheme should be applied to each criterion to indicate its importance in the overall method evaluation process. Additionally valid criteria should determine if the methodology captures meaningful aspects of the method. For example, some of the criteria like "documentation" appear to be irrelevant.

The utility of using these evaluation criteria in ranking four studies was not apparent (i.e., the rankings were presented, but not used elsewhere in the report). Four models of different systems were compared against the author-defined criteria, but in the end the results and conclusions appeared to be like comparing apples to oranges. Arbitrarily scoring them against the author-defined criteria was not particularly useful, especially given that several of the criteria were deemed not applicable to one or more of the studies presented, yet no correction was provided for this in the comparison of the results.

Finally, it is troubling that the authors did not apply the evaluation criteria during the process of selecting the probabilistic modeling methods they chose for further study earlier in the report.

Markov Model of DFWCS

The report states that Markov modeling is a useful technique for analyzing digital systems, specifically pointing out its limitations and advantages. But in Chapter 6, much effort is given to explaining how a Markov model should be made without actually making it. Then the chapter concludes that the Markov method is "too complicated and tedious" to construct and even if it were constructed it would be so enormous that it would be impractical to solve. However, they still plan to develop and solve the Markov model in the next phase of this project. This reasoning should be explained.

Issues with Markov Chain models that should be more fully addressed in the report:

- Ways to address uncertainties in transition probabilities.
- The report mentions that the computational power required for realistic modeling is prohibitive but does not discuss how to address it other than by the "simplified" model, which still leaves prohibitive computational issues and will also introduce additional uncertainties.
- If a Markov model is used to predict the future state of a system and a small error in transition probability is introduced into the calculation at the beginning, then the errors in the transition matrix will grow exponentially with time when predicting future states. This issue should be discussed.

- Ways to consistently combine different sources of data. This is mentioned in report, but no solution is presented.
- The results need to be converted into a format that is compatible with ET/FT for use in the PRA. The authors do mention this issue a number of times, however it is important enough to stress with a much more comprehensive and significant discussion in the introductory sections of the methodology descriptions of Markov methods.

Very truly yours,

Francis J. Wyant
Jeanne Dion
Risk & Reliability Analysis Department

Bobby Middleton
Fuel Cycle Experiments & Analysis Department