May 11, 2001

MEMORANDUM TO Jack R. Strosnider, Jr., Director
Division of Engineering
Office of Nuclear Reactor Regulation

FROM: Michael E. Mayfield, Director /RA/
Division of Engineering Technology
Office of Nuclear Regulatory Research

SUBJECT: TRANSMITTAL OF NUREG/GR-0020 "EMBEDDED DIGITAL SYSTEM RELIABILITY AND SAFETY ANALYSES"

This is the first in a series of reports that provide the technical basis for a new reliability and safety analysis method that accommodates, both specially developed and COTS-based digital systems. This work is being conducted to meet NRR's User Need Number 2000-5, which states in part, "Investigate and develop methods and models for quantitative assessment of highly reliable safety-critical software-based critical systems..."

NUREG/GR-0020 "Embedded Digital System Reliability and Safety Analyses" provides the technical basis for a method to analyze the behavior of digital systems under the influence of internal/external and normal/faulted conditions of the inputs, outputs, hardware, and software. The uniqueness of the analysis method is that it accounts for software design faults while most methods are hardware oriented and only account for random hardware faults.

When completed, the series of reports can be used to establish an acceptable method to characterize and analyze digital systems for performance, reliability, failure modes, and safety. The reports are also expected to provide valuable insights into subsystem and system safety evaluation methods, and insights to support integration of digital systems into PRA.

The research is being performed under a Cooperative Agreement between NRC and the University of Virginia, Center for Safety-Critical Systems (CSCS) and involves developing assessment methods for evaluating digital systems for reliability and safety including the interrelated dependencies of hardware and software.

A technical literature search identified methods that characterize the behavior of a digital system under the influence of internal and external faults. The methods were segmented according to the ability to account for both hardware and software faults, and the ability to analyze the resultant outputs for safe or unsafe failures.

A method was selected that used automated qualitative analysis to generate hardware and software faults, and quantitative analysis to arrive at reliability and safety metrics, such as mean-time-between-unsafe-failures. The technical basis for the selected method is presented in the report. The method is presently being used for safety critical digital system safety evaluation in Europe and is being reviewed by safety assessors from TUV Germany.

The report also surveys and evaluates common-mode and common-cause failure definitions as applied to digital systems.

Further research will develop the selected method in the areas of safety assessment process, detailed methods, and tools to properly characterize and analyze digital systems for performance, reliability, failure modes, and subsystem and system safety.

In summary, the research is aimed at promoting more efficient staff review of digital systems by providing a sharp focus on risk significant areas. This should lead to less staff time involved in the review of the software development process. The completed research results can be incorporated in a branch technical position for use by staff and licensees.

We plan to provide a briefing on the overview and future direction of this research at a later date. If you have any questions about this research, please contact John Calvert (415-6323), a member of my staff in the Engineering Research Applications Branch, Digital I&C Team.

Attachment: As stated

Distribution:
A. Thadani
R. Barrett
C. Doutt
M. Fields
M. Cunningham
T. King
ERAB r/f

***SEE PREVIOUS CONCURRENCE**

**DOCUMENT NAME**: g:\erab\jNUREG20-NRRsubmittallLtr3.pd.wpd
OAR in ADAMS? (Y or N) Y ADAMS ACCESSION NO.: ML011030132 TEMPLATE NO. RES-__
Publicly Available? (Y or N) Y DATE OF RELEASE TO PUBLIC _____ SENSITIVE? ____
**To receive a copy of this document, indicate in the box: "C"** = Copy without enclosures **"E"** = Copy with enclosures **"N"** = No copy

| OFFICE | ERAB/RES | | ERAB/RES | | ERAB/RES | | D/DET/RES | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| NAME | J.Calvert* | | S.Arndt* | | S.Bahadur* | | MMayfield | | | |
| DATE | 04/19/01 | | 04/19/01 | | 04/19/01 | | 05/9/01 | | | |

OFFICIAL RECORD COPY