January 23, 1997

MEMORANDUM TO: Jared L. Wermiel, Chief
Instrumentation and Controls Branch
Division of Reactor Controls and Human Factors
Office of Nuclear Reactor Regulation

Franklin D. Coffman, Jr., Chief
Control, Instrumentation and Human Factors Branch
Division of Systems Technology
Office of Nuclear Regulatory Research

FROM: Dr. Don W. Miller, Chairman
Instrumentation and Control Systems
and Computers Subcommittee
Advisory Committee on Reactor Safeguards

SUBJECT: ISSUES AND REQUESTED ACTIONS FOR NRC STAFF USE IN PREPARING FOR ACRS REVIEW OF PROPOSED FINAL SRP/BTP/RGs

The purpose of this memorandum is to forward a list of questions and requested actions for your use in preparing for ACRS review of proposed final Standard Review Plan (SRP) sections, Branch Technical Positions, and Regulatory Guides (RGs). We have discussed many of these issues during past meetings. As you know, some ACRS Members feel very strongly about some of these issues. Therefore, I am providing this list of issues and requested actions to facilitate your preparation in resolving these matters during future Subcommittee and ACRS deliberations.

Issue 1:

Several Members of the ACRS point to Ontario Hydro's experience at Darlington as an innovative approach to software (S/W) design and assessment. Cognizant members of the staff have informally expressed concern that the formal methods introduced (forced on?) by Parnas for software design are confusing and "a step backwards." The staff has expressed the view that the approach advocated by Parnas is neither transparent nor useful. Furthermore, the staff believes that we are substantially ahead of the Canadians in this area.

Recommended Action:

- Discuss the staff's opinion of the S/W design methods used by Ontario Hydro.

Issue 2:

A recurring question and concern raised by Members of the ACRS has been that S/W system

26

design methods have high reliance on process with little reliance on product testing or evaluation as a means for developing high quality, highly reliability S/W. There is agreement that a high quality process will improve product quality and reliability and that a precisely defined and auditable process results in a product which is easier to maintain and update, and simplifies configuration management. However, some ACRS Members expressed concern that the acceptance criteria are not clearly specified. From their view, the acceptance criteria provides limited guidance on what is acceptable and what is not acceptable in terms of requirements for accuracy, consistency, and competency.

Recommended Action:

- Address these concerns by citing specific examples (i.e., using a simple system). On the issue of acceptance criteria explicitly demonstrate how acceptance criteria are specified by the IEEE standards.

- Discuss the assertion that the acceptance criterion provides limited guidance on what is acceptable, what is not acceptable, and that there is no criteria for accuracy, consistency, and competency.

Discussion:

The following abbreviated definition of Verification and Validation (V&V) may be considered as starting point in discussing these questions and concerns.

> V&V is "the process of determining whether the requirements for a system or component are complete and correct, the products of each development phase fulfill the requirements or conditions imposed by the previous phase, and the final system or component complies with specified requirements. Note the activities involved in V&V for digital systems are essentially equivalent to some of the activities that have traditionally been performed for design and acceptance testing of any nuclear-safety related equipment." (Reference: "Guideline on Evaluation and Acceptance of Commercial Grade digital Equipment for Nuclear Safety Applications", July 1996.)

V&V is important to assessing that the process is done correctly. Testing is used to verify the process is completed and the product meets specified requirements.

V&V provides for and requires a well defined PROCESS to assure the process of S/W development is complete and correct AND that the PRODUCT at each phase of development process performs as expected AND that the FINAL PRODUCT performs as specified. What it does not do is guarantee performance indefinitely nor provide a statistical methodology for predicting failure.

Simply put, V&V is a well-defined process for design and performance evaluation of S/W products analogous to the design and performance evaluation process used for hardware (H/W). There are; however, two distinct and important differences: 1) the process of translating system requirements into S/W requirements is difficult and is the cause of design errors being the dominant source of failures. Design errors are fundamentally human performance errors and are not stochastic. Other S/W failures such as coding errors, although less prevalent, also are not stochastic. In the case of H/W, most failures are not dominated by design errors. Consequently, H/W failures are dominated by "mother nature" and are random and stochastic. Stochastic failures can be characterized by mean time to failure and failure rates. If design errors were dominant in H/W systems, H/W systems would have properties similar to those found in S/W systems (i.e., the inability to predict failures

and common-mode failure in redundant systems).

Golay (see below) captures this concept from a different perspective:

> "The concept of S/W failure is fundamentally different from H/W failure. A S/W failure consists of encountering an initially present but still undetected error. Conversely, a H/W failure consists of exciting a failure mode by exercising a flaw which has been introduced since the last time that this failure mode was demonstrated to be inactive. Thus, a perfect S/W program can be expected to remain error free {indefinitely} but an analogous H/W system can not".

Issue 3:

On numerous occasions the staff and the ACRS have stated that nuclear safety systems are inherently simple. The SRP Chapter 7 update is based on consensus based industrial standards, standards that represent generally accepted S/W engineering practice and consensus standards developed for all S/W based systems, simple or complex.

A question has been raised on several occasions, including at the recent meeting with the Commission, whether guidance or standards can be developed specifically for simple systems such as those used with nuclear plant safety systems.

Recommended Action:

- Discuss the feasibility of this approach with specific attention to the pros and cons?

Issue 4:

The methodology for addressing common-cause failures {CCFs} should be adaptable to redundant S/W based systems. In fact, identification of possible CCF paths may be inherently easier than many H/W paths since it is well known that S/W failures are dominated by design errors and that design errors are a significant contributor to CCFs.

Recommended Action:

- Discuss the methodology for addressing CCFs in digital systems

Issue 5:

The SRP is intended to be guidance for reviewers of digital systems and should not include specific examples. Several ACRS Members have suggested that the SRP cite analytical tools that may be used in specific cases. For example, tools for translation of system requirements into S/W requirements.

Recommended Action:

- Cite possible examples of tools that may be used?

Issue 6:

The staff has stated that a graded approach to reviews based on importance to safety will be used. However, the criteria for reviews based on a graded approach are not explicitly defined. The staff also stated that guidance on graded quality assurance (GQA) is being developed for PRA as a part of the SRP update to Chapter 19. A draft Regulatory Guide for GQA has been developed.

Recommended Action:

- Consider how or whether the fundamental concepts and methods in the GQA RG can be applied to the review of digital systems?

Issue 7:

During past ACRS discussions, it has been suggested that the guidance provided for review of digital systems is analogous to the quality assurance QA process for safety-related equipment specified in Appendix B. This analogy has been implied when one considers the graded approach to review and consider the use of the concepts the RG for graded quality assurance.

Recommended Action:

- Comment on the merits of this analogy?

Issue 8:

The methodology and tools used in developing design specifications should be transparent and independent of natural language.

Recommended Action:

- Provide examples including a tutorial on their use.

Issue 9:

There is an expectation that the designer/developer complete tasks specified by the process. The SRP specifies what is to be done and in some cases why, but not how to do it, which is designer specific.

Recommended Action:

- Evaluate S/W development and design methods that supplement or provide an alternative to the traditional "Waterfall" methodology on which the IEEE S/W standards are based. Two such approaches were reported in papers published at the recent PSA'96 ANS Topical meeting in Park City, Utah. I have included references to each with quotes from their respective papers.

  1. M.W. Golay, J. Lunlholfer and M. Ouyang, "A Strategy for Developing and Demonstrating Highly Reliable Nuclear Software".

  * Applies primarily to simple systems
  * The keys to developing reliable S/W are a combination of requiring the

structure to be simple and a thorough testing program.

* The concept of S/W failure is fundamentally different from H/W failure. A S/W failure consists of encountering an initially present but still undetected error. Conversely, a H/W failure consists of exciting a failure mode, by exercising a flaw which has been introduced since the last time that this failure mode was demonstrated to be inactive. Thus, a perfect S/W program can be expected to remain error free {indefinitely}, but analogous H/W cannot.
* When these methods have been compared to the more traditional methods {i.e. Waterfall} they have been shown to produce usable code more efficiently and to be considerable more effective in eliminating various forms of S/W errors.

2. A. Clark and C. Smidts, "Systematic Generation of Software Failure Mode and Effects Analysis for Fault Tolerance".

* This approach is recovery-oriented and focuses on tolerating and recovering from faults to continue to provide service.
* The S/W FMECA approach was prototyped ... for FAA's new air traffic control system which has an unavailability requirement of 1E-7.
* Like H/W FMECA, S/W FMECA identifies inadequacies in the design, identifies the need for corrective actions and provides data to develop test plans. However, unlike H/W FMECA, S/W FMECA process described in this paper takes a recovery-oriented paradigm, where failures are designed to be tolerated rather than eliminated, because S/W failures are more difficult to identify and eliminate than are H/W failures.

Comment: It will be interesting to see what position the NAS study takes on these issues.

Issue10: Reference: GL 95-02 and digital I&C upgrades.

Several ACRS Members expressed the view that there is some ambiguity in the licensing application process for digital I&C upgrades. The update of the SRP Chapter 7 should help, but there remains a question whether more should be done. Currently, the staff recommends that licensees who are considering upgrades contact the staff ahead of time and present an overview of the proposed change. The staff will then provide an opinion on whether it can be done via 10 CFR 50.59 or whether a license amendment is required to assure an unreviewed safety question (USQ) does not arise. The staff and industry should have gained sufficient experience since issuance of GL 95-02 to "narrow the gray areas" and more clearly identify criteria for 50.59 changes. The NRC
Technical Training Center (TTC) plans to hold a second Regulatory Perspectives Workshop" in January or February regarding these matters. This topic should be discussed both formally and informally.

Recommended Action:

- Based on experience with digital upgrades, clarify criteria for 50.59 changes.

Issue 11: Reference: K. Korsah, T.J. Tanaka T.L.Wilson and R.T Wood, "Environmental Testing of an Experimental Digital Safety Channel", NUREG/CR-6406, September 1996.

Significant Findings and Conclusions:

1. Interfaces were found to be the most vulnerable element of the Experimental Digital

Safety Channel (EDSC). "Thus, qualification testing should confirm the response f any digital interfaces to environmental stressors."

2. The most prevalent stressor induced upsets, as well as the most severe, were found to occur during the EMI/RFI tests. These tests produced the only permanent failure of the EDSC (i.e., power supply). Also, the effect of the stressor was typically immediate, whereas the occurrence of high temperature/humidity and smoke exposure effects was delayed for some interval (i.e., tens of minutes).

Discussion:

High-voltage spikes on power leads were found to cause a greater number of upsets and within a relatively short time (i.e. seconds) compared to low-voltage, sinusoidal rms noise on the same power leads (Reference: 4.8, "Summary of EMI/RFI Test Results"). Throughout all the EMI/RFI tests, this (the power supply of the original PRS/MUX multiplexer backplane under test inside the GTEM cell failed permanently after the 20MHz, 72V/m test.) is the only hard or permanent failure that occurred. The minimum field strength at which temporary errors occurred with the DTC was 40V/m. (Reference: 4.7.3, "Analysis of RS03 Test Results").

It was noted that susceptibility of particular systems can be mitigated by grounding, shielding isolation and surge practices.

Recommended Action:

Considering the results from the EMI/RFI tests address the following two questions:

1. How similar were the high-voltage spikes on power leads to transients that might be expected from transients resulting from lightning?

2. Taking into consideration the BNL Risk study of environmental stressors, which concluded that lightning represented the highest environmental risk for digital I&C systems, does the EPRI EMI/RI Guideline endorsed by an NRC SER provide sufficient guidance relative to grounding, shielding, isolation and surge practices?

Issue 12: NRC Research Plan

Identify the most important regulatory and technical issues raised in the National Academy of Science Phase 2 study and relate them to current NRC research programs for I&C and identify new research programs needs. Include issues considered in this memo where appropriate.

Recommended Action:

Identify points of agreement and disagreement with the NAS/NRC Phase 2 study report. Present the preliminary assessment of the changes required as a result of the study.

cc: ACRS Members
J. Larkins
R. Savio
S. Duraiswamy
ACRS Staff and Fellows