Releasible
l.f.
(15)

April 27, 1995

U.S. Nuclear Regulatory Commission
Office of Nuclear Regulatory Research
Attn: Robert Brill - MS-T-10-E33
Washington, DC, 20555

SUBJECT: Bi-Monthly for USNRC Grant NRC-04-93-089

Dear Mr. Brill:

Please find enclosed the joint bi-monthly, for the period 3/1/95 to 4/30/95 for USNRC Grant NRC-04-93-089. Please also find a summary of our technical progress to-date.

**Bi-Monthly**

*Current Status*

The task we are now performing is identifying the signatures of software-based controller failures. This task consists simulating the operation of a steamline at the PVNGS during both normal operation and during controller failures, manipulating and storing the transient data in a easily analyzable form, and isolating from the database those signals which most clearly constitute a failure mode signature.

We performed this task for one failure case. We have isolated the signature of an analog-to-digital (A/D) converter card failure from operational data obtained from the simulator.

*Next Steps*

The next steps will consist of modeling other types of controller failures, such as an actuator failure, and identifying their signatures. After this analysis is complete, it will be possible to select the pattern recognition paradigm for automated decision making.

Please note that fault signature identification task accomplished here was scheduled to be performed in the month the June on the timeline dated March 8, 1995. Hence please regard the fault signature analysis described here as being preliminary in nature.



D 115

## Technical Performance

The following paragraphs describe the progress of the project to date. The progress report is versed in terms of the five tasks envisaged in the proposal. In these paragraphs, the five task descriptions are shown in *italics*.

*Project Objective*

The objective of this research is 'to develop and demonstrate an active information processing system which is capable of detecting controller failures on-line.' The basic premise underlying the objective is that nuclear power generating stations are evolving towards highly automated, supervisory control, and will expose the public to an order of magnitude less risk than the current generation of plants. The reduction in risk will primarily be achieved by simplifying the plants, and by designing the plants to allow inherent processes to replace engineered safeguards.

It is to be expected that the control systems designed for advanced nuclear power plants will have engineered safeguards, such as fault detection and error recovery, designed into them. Given that the physical complexity of the next generation of plants will be materially reduced, the complexity of the digitally-based systems controlling these plant may exceed the complexity of the plant itself. It may well be the case that the dominant contributor to risk will be the control system itself. They will almost certainly have designed into them latent errors, errors which only become apparent or recognizable in unanticipated ways.

Protection against the consequences of common-mode failures is offered through diversity. Ideally, the application of diverse technologies to the problems of common-mode failures inhibit the occurrence of latent errors. To provide for diversity in critical information processing tasks, such as the on-line monitoring of software performance, it is necessary to develop software-fault detectors which operate independently of the software itself.

i) *Development of a representative plant model, such as a turbine control valve.*

The development of a representative turbine control valve model is complete. Some of the problems we encountered during the modeling process were i) difficulty in compiling the simulation code on the AIX machine, ii) difficulty in executing simulation models because of differences in compilation, iii) difficulty in developing the turbine model because the documentation has gaps in it, and iv) difficulty in stabilizing the simulation model because of the lack of in-phase negative feedback. This prompted the development of an electro-dynamical generator model.

Figure 1 shows a nodalization diagram of the RELAP5 model currently in use. The hydrodynamic components of the model include a steam generator as a materials properties source, a single steamline, a turbine control valve, the steam manifold, a high pressure turbine, and the reheater volume sink. The remainder of the model

utilizes RELAP5's generic control variable block functions to simulate the electro-dynamics of the generator, and the turbine speed controller. The model is representative of one of the four steam lines of Unit One of the PVNGS. Table 1, below, contains data characterizing its nominal, steady-state operation.

| Steam Generator Pressure (psia) | Turbine Manifold Pressure (psia) | Turbine Control Valve Position |
|---|---|---|
| 993.0 | 941.13 | 0.5455 |
| Turbine Rotational Speed (RPM) | Turbine Torque (lb-ft) | Generator Power (MWt) |
| 1801.8 | 8.92e5 | 214.11 |

**Table 1: Operational Data**

The model was subjected to several simulated load-change transients. Figures 2 and 3 show the response of the model to one such change. After an initialization transient, a step change in load was imposed on the system by modifying the exciter current. Figure 2 shows the controller's positioning of the TCV. The controller responds rapidly to the external perturbation, and repositions the control valve with minimum settling time. Figure 3 shows rapid response of the generator model to the step change in load.

ii) *Development of control failure models.*

We have modeled and simulated the failure of an analog-to-digital conversion board in the turbine speed control system's speed sensor signal. The failure was modeled by assuming that the board's digital output signal saturated 'high' and caused the error signal into the control algorithm to saturate 'low'. We are in the process of developing several other controller failure models, such as the degradation of the electro-hydraulic servo-valve, which will be simulated using RELAP5's generic control variable capability.

One of the difficulties we have encountered is that software-based system failures seem to be classified according to the nature of the patches needed to fix the bug, and not according to the root cause of the failure. Thus, the exact classification of any fault detected depends on the computer language used in the correction.

One of the more interesting observations we found in the literature was that intermittent or transient faults may dominate fault occurrence. These are software faults whose occurrence is sporadic, and whose origin is very difficult to trace.

iii) *Formalize and encode the fault detector's information structure.*

The information structure of the fault detector is primarily contained in its feature space. The feature space is the ensemble of features, such as 'turbine manifold pressure', which contain the problem's quantitative descriptive information. In this problem, the selection of the feature space is constrained by the availability of plant data. Some state variables, such as quality, may be useful, but not available at the plant. Other data may not contain the information essential to the identification of failure signatures.

The formalization of the feature space involves selecting and/or extracting only features containing relevant information. In this project, a two-step procedure is being used: Step 1) Population of a Database - We have populated a small database of operational transients. Each transient consists of an initialization/relaxation transient and the operational transient itself. The transients selected for the initial population simulate step changes in the loading of the electrical grid on the system. Step 2) Fault Signature Identification - For each fault selected, simulate the failure, and determine the features which distinguish it from normal operational behavior and from other failure modes. The feature space is then the aggregate of the features necessary to identify each failure type.

Figure 4 shows the feature space signature of a simulated A/D conversion failure, described above. The Figure shows the feature space used in the analysis, and six clusters of data. Here, the feature space consists of the turbine speed, TCV position, and Generator power. Each of the five transients contained in the space began at the operating point, as shown. Four of the clusters represent changes in load imposed by the electrical grid. The fifth, clearly labeled, represents the A/D board failure. In this spatial representation, the effect of the failure on the system is distinguishable from normal operational transients.

iv) *Application to the Detection of Operational Faults.*

In this step, we will encode, execute, and verify an algorithm which distinguishes normal operational data from data containing faulted behavior. There are many paradigms available to automate this decision making process, ranging from multi-linear perceptrons to associative stochastic automaton (ASA).

To configure the ASA as a detector of controller faults, it is necessary to generate an experiential base which encompasses only non-faulted controller signals. The lack of association with the experiential basis is then interpreted as an indication of failure. In this way, any signal which strays outside of the basis will cause a fault to be annunciated. If the annunciation signal was improper, an operator can simply indicates this to the ASA, which it corrects its behavior accordingly. Faults do not have to be modeled in this approach; only the normal behavior of the controller need be sampled.

Other pattern recognition paradigms may be used for the purposes of comparison or if they prove to be more effective or suited to this particular task.

v) *Documentation of Results.*

Documentation will be generated. This includes the Final Report for the project, the Thesis of the Masters student, and publication in a peer reviewed journal. Some of this effort has already begun. Preliminary work on documentation of the core technical achievements, which will form the basis of the Final Report and journal article, has begun.

If there are any suggestions, questions, or concerns, please call.

Wayne C. Jouse
University of Arizona
Tucson, AZ, 85721
(602) 621-2401
*jouse@ccit.arizona.edu*

cc:
G. Martinez, EES
J.G. Williams, NEE
S. Crampton, Div. of Contracts, USNRC
E. Smerdon, COEM