Trans. Am. Nuc. Soc., Vol. 49, June 1985

TABLE II
Design Assurance

Hardware:

1. Computer hardware will be designed to be fault-tolerant, i.e, capable of correct operation in the presence of any single failure.
2. Fault-tolerant properties assured through the use of automated reasoning techniques and validated through simulation.
3. Component reliability ascertained via Markov analysis.

Software:

1. Models assured through a combination of operational experience and parametric analysis using computer simulation.
2. Statistical test assured through operational experience.
3. Application algorithm and operating system assured via formal analysis techniques similar to automated proof-of-correctness which is performed in consort with a formal test data selection criteria.
4. Software reliability ascertained via software reliability modeling techniques.

Total System Validation

1. Total system validation will be supported by exhaustive testing. This testing will be accomplished by a validation team which is diverse from the design and verification teams.

Systems that are designed for reactor protection must adhere to stringent design requirements to ensure reliable protection. ecause of the complexity of computer-based systems, an adequate reliability demonstration becomes a vital aspect of this advanced application.

Initially, the demonstration must encompass the computer, ancillary hardware, applications software, and the operating system software. Because the technology supporting software reliability determinations is immature, the complexity of software must be minimized. This implies that an attempt to qualify an analytical redundancy-based flow protection system should progress in two phases. Phase I, fault-tolerant flow trip, will concentrate on a single flow channel, and phase II, fault-tolerant analytical redundancy, should extend the developments of phase I to encompass the analytical redundancy software.

An analytical flow channel is planned to be added to the EBR-II protection system. The primary benefit to the EBR-II facility is that, on completion of both phases, a replacement flow protection scheme will be available. Considering the experienced failures in the existing flow monitoring system and the desire to operate EBR-II for an additional ten years, the benefit translates into support for continued, reliable operation.

The technical developments necessary to complete both phases provide benefits to the commercial reactor community as well as space nuclear applications. Qualification of computers for use in reactor control and safety systems would allow reactor operators and designers to capitalize on the benefits of analytical redundancy, sensor validation, failure prediction, diagnosis, autonomous control, etc. Though the developments planned for EBR-II will not address these specific areas, the developments will remain generic to ensure compatibility with these other programs.

Phase I can be summarized as follows:

1. Provide a flow trip that duplicates the protective capability of a direct sensor.

2. Reduce or eliminate spurious trips due to internal faults or model error, i.e., model demands trip under conditions where direct sensor would not.

3. Develop and apply methodology to verify completeness and reliability of computer hardware and software design for reactor safety system use:

a. ancillary/support hardware; protect against single failure and common-mode failures

b. computer hardware; protect against a single failure and common-mode failure

c. software; certify capability and reliability of model

d. prove claims with respect to the certified model and lack of common-mode failures, using automated reasoning techniques

e. integrated software/hardware validation via testing and reliability modeling.

4. MITR-II: Integrated Fault-Tolerant Systems Implementation and Experiments, *David D. Lanning, John A. Bernard (MIT), John Hopps (Draper Lab), Asok Ray (MIT)*

This summary describes an ongoing implementation and experimental evaluation of an integrated fault-tolerant methodology on the automatic control system of the 5-MW(t) Massachusetts Institute of Technology (MIT) research reactor, MITR-II. This endeavor is a joint research effort between the C. S. Draper Laboratory (CSDL) and the MIT Nuclear Reactor Laboratory.

A system is fault tolerant if the capability exists to detect both abrupt and incipient failures, if there is a means of identifying and isolating failures, and if it is possible to reconfigure the system on-line so that no deterioration of performance occurs. The MITR-II's automatic control system (ACS), which is designed both to maintain the reactor power constant despite reactivity feedback from xenon and temperature and to adjust power in response to demand changes over the range 20 to 100%, was selected for a demonstration of this technology. The ACS positions either a fine control regulating rod or a coarse control shim blade in response to the decision of one of several possible control laws. Each control law depends, in turn, on the output of a variety of sensors (power level, period, rod or blade position, temperature, and flow) for its estimate of the reactor's state. The creation of a fault-tolerant instrumentation and control system therefore entailed incorporating fault tolerance in three separable areas. These were the sensors, the software including the control laws, and the hardware including the actuators that comprise the ACS.

The application of fault tolerance to the ACS's sensors involved developing an on-line signal validation methodology that uses redundant measurements, both direct and analytical, to provide a systematic procedure for fault detection, fault isolation, and measurement estimation. Fault detection and isolation decisions are made on the basis of mutual consistencies among all redundant measurements. Measurement estimation, and the concurrent task of sensor calibration, is accomplished via sequential tests that rely on both current and past measurements.[1] A major difficulty in the identification of valid signals is that fully operable sensors may exhibit deviations from one another if they are spatially separated or if they are characterized by different time constants. Should that occur, some sensors may be erroneously deleted. On the other hand, failure to isolate a degrading sensor may adversely affect the estimate of the measured variable. The MIT-CSDL approach surmounts these difficulties both by compensating all consistent measurements on-line so that their residuals are minimized and by updating the weighting factors for individual sensors on the basis of their respective *a posteriori* probabilities of failure. Hence, if a sensor fails abruptly, it will be immediately isolated and only the remaining sensors used to provide an estimate of the signal. However, should a gradual sensor degradation occur, the faulty sensor may or may not be immediately isolated, but its influence on the remaining sensors will be rapidly diminished because its weighting factor is decreased in proportion to its *a posteriori* probability of failure. Use of this methodology in conjunction with the direct digital control of the MITR-II has shown that it will maintain the power at the desired level despite either sudden sensor failures due to electrical faults or gradual failures due to the cycling of water shutters that alter the neutron flux seen by the sensors.

Concerning the control laws that are programmed into the ACS, the implementation of fault tolerance has required both the development of several different types of control strategies and a means of combining them to achieve reliable, efficient, and safe operation. Most prominent among the demonstrated control concepts is the MIT-CSDL nonlinear digital controller (NLDC), which uses reactivity constraints for the on-line assessment of the safety of any proposed control action.[2,3] Other strategies that have been demonstrated include steady-state controllers of conventional design, a decision analysis controller for steady-state operation, a predictive controller based on state analysis, several rule-based systems that use "fuzzy" logic, and an expert system.[4,5] The latter three are used in transient control. Work is in progress to combine these various control laws in a robust multitiered controller. The NLDC and the expert system are both capable of determining in real-time when a control signal should be changed in order to assure safety. However, neither can predict the power as a function of time. Hence, they will be used in a supervisory capacity and will form one tier. The predictive controller, and perhaps one of the rule-based systems, can provide estimates of the power as a function of time given a change of setpoint or a disturbance. However, neither is capable of guaranteeing feasibility of control (i.e., safety). Hence, their decisions must be reviewed by the supervisory tier. The predictive strategies will form a second tier and will have actual control of the system. A third tier, consisting of a decision analysis controller, will be used to select the means of control (i.e., temperature feedback, regulating rod, or shim blade). This tier will also detect faults and reconfigure the fault-tolerant control system. These three tiers, when used in concert, will guarantee reliability and safety. Regarding efficiency, consideration is being given to the creation of a fourth tier that will reconfigure the system to optimize performance. It will identify the reactor state and, given the nature of the required change, select which controller is to be used in each of the other three tiers.

Relative to the ACS's actuators, there are two possible approaches whereby fault tolerance could be achieved. First, given that the MITR-II has six shim blades and one regulating rod, more than one mechanism could be made available to the control system. Hence, if one actuator fails, the third tier controller could select a different actuator. This approach has been provided and the ACS can currently use either a single shim blade or the regulating rod. The second approach is to install redundant components and additional sensors in existing actuators. This second approach is currently being prepared for demonstration. A fault detection and isolation methodology similar to that implemented for the instrument signals can be used to identify any failed component and to reconfigure the actuator for continued operation.

The MIT-CSDL program to develop and demonstrate fault-tolerant technology on the MIT research reactor has been proceeding successfully. The most significant aspects of the program are that the technology has actually been implemented, that it has been shown experimentally to function as anticipated, and that its use has improved certain aspects of reactor operation.

1. A. RAY, J. A. BERNARD, D. D. LANNING, "On-Line Signal Validation and Feedback Control in a Nuclear Reactor," *Proc. Fifth Power Plant Dynamics, Control, and Testing Symp.*, Knoxville, Tennessee, March 1983.

2. J. A. BERNARD, D. D. LANNING, A. RAY, "Use of Reactivity Constraints for the Automatic Control of Reactor Power," *IEEE Trans. Nucl. Sci.*, **NS-32**, *1* (Feb. 1985).

3. J. A. BERNARD, D. D. LANNING, A. RAY, "Experimental Evaluation of Reactivity Constraints for the Closed-Loop Control of Reactor Power," *Proc. NRC-EPRI Symp. New Technologies in Nuclear Power Plant Instrumentation and Control*, Washington, DC, November 1984, Instrument Society of America.

4. J. A. BERNARD, A. RAY, "Experimental Evaluation of Digital Control Schemes for Nuclear Reactors," *Proc. 22nd IEEE Control and Decision Conference*, San Antonio, Texas, December 1983, p. 744.

5. J. A. BERNARD, A. RAY, K. S. KWOK, D. D. LANNING, "Design and Experimental Evaluation of a Fuzzy System for the Control of Reactor Power," *American Control Conference*, Boston, Massachusetts, June 1985.

5. Fault-Tolerant System Evaluation Experience: Markov Model-Based Methodologies, *Richard S. Schabowsky, Jr. (Draper Lab)*

Reliability/availability (R/A) modeling plays an increasingly important role in the design and evaluation of fault-tolerant systems. A large number of trade-offs must be made