CONF 8911123-1

# Research and Development on the Application of Advanced Control Technologies to Advanced Nuclear Reactor Systems: A U.S. National Perspective*

CONF-8911123--1

DE90 002939

J. D. White
Oak Ridge National Laboratory
Oak Ridge, Tennessee 37831

L. R. Monson
Argonne National Laboratory
Idaho Falls, Idaho 83403

D. G. Carrol and Y. Dayal
GE Nuclear Energy
San Jose, California 95153

Submitted to the IAEA Technical Committee/Workshop
on the Impact of Advanced Technologies
on Reactor Systems

November 6-9, 1989

**DISCLAIMER**

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

*Work supported by the U.S. Department of Energy under Contracts
DE-AC05-84OR21400 and W-31-109-Eng-38

# Research and Development on the Application of Advanced Control Technologies to Advanced Nuclear Reactor Systems: A U.S. National Perspective*

## ABSTRACT

Control system designs for nuclear power plants are becoming more advanced through the use of digital technology and automation. This evolution is taking place because of: (1) the limitations in analog based control system performance and maintenance and availability and (2) the promise of significant improvement in plant operation and availability due to advances in digital and other control technologies. Digital retrofits of control systems in U.S. nuclear plants are occurring now. Designs of control and protection systems for advanced LWRs are based on digital technology. The use of small inexpensive, fast, large-capacity computers in these designs is the first step of an evolutionary process described in this paper.

Under the sponsorship of the U.S. Department of Energy (DOE), Oak Ridge National Laboratory, Argonne National Laboratory, GE Nuclear Energy and several universities are performing research and development in the application of advances in control theory, software engineering, advanced computer architectures, artificial intelligence, and man-machine interface analysis to control system design. The target plant concept for the work described in this paper is the Power Reactor Inherently Safe Module reactor (PRISM), an advanced modular liquid metal reactor concept. This and other reactor designs which provide strong passive responses to operational upsets or accidents afford good opportunities to apply these advances in control technology.

This paper describes the status of this work and its relevance to the nuclear industry in the U.S.

## 1. INTRODUCTION

Recent advances in computer-based digital data acquisition systems, process controllers, fiber-optic signal transmission, artificial intelligence tools and methods, and small inexpensive, fast, large-capacity computers--with both numeric and symbolic capabilities--have provided many of the necessary ingredients for developing large, practical automated control systems. Furthermore, recent reactor designs which provide strong passive responses to operational upsets or accidents afford good opportunities to apply these advances in control technology.

The U.S. Department of Energy (DOE) work on advanced controls for advanced reactors is concentrated at the Oak Ridge National Laboratory (ORNL) in the Advanced Controls Program, at Argonne National Laboratory (ANL) in the EBR-II Program, and at GE Nuclear Energy (GE) in design of the Power Reactor Inherently Safe Module (PRISM) reactor. The DOE is also supporting considerable work at various universities.

This paper describes briefly the status of the work being done by ORNL, ANL and GE to apply advances in controls technologies in a staged approach to meet the design goals of high reliability, low operating cost and simple operation for the PRISM. The relationship of this work to the U.S. commercial industry is also discussed.

## 2. NATIONAL PERSPECTIVE

For advanced reactors in the U.S., the goals of advanced, automated plant control systems include improvement of plant availability, low operating costs. simple operation and reduced challenges to plant safety systems.

### 2.1 Improved availability

Advanced, digital control technology can provide significant improvement in plant availability. Performance of analog subsystem controllers currently used in U.S. LWRs is limited in dealing with system upsets and major parameter changes. Dramatic improvement in virtually all aspects of subsystem control is enabled by the advent of economical, reliable digital microprocessors. Digital technology increases the potential for improved control algorithms that are better able to deal with nonlinear and discrete changes in parameters and redefinition of target states; it also increases the potential for self-checking for failures or decalibration. Multiplexed fiber-optic data transmission and distributed architectures provide an opportunity for noise reduction (and significant construction cost saving) by minimizing cables and interconnections.

## 2.2 Low operating costs

Analysis by GE on advanced automated plants indicates that the plant operating staff could be reduced by approximately 100 people. This reduction would lower plant operating costs by about $4 million per plant year[1]. For the PRISM concept, sufficient automation will be built in to support a design goal of one operator running an entire power block [ 3 reactors and one turbine generator] under both normal and faulted conditions. All normal plant operations (such as startup, shutdown, load following, etc.) will be automated.

## 2.3 Simple operation

The PRISM reactor is a modular system that has significant requirements for automation to keep plant operation well coordinated. In the PRISM, advanced controls incorporating improved diagnostics, alarm management, and graphical displays will give the operator much more useful information and guidance than in today's U.S. plants. Because of the strong passive behavior of the plants, the operator and the control system will be able to take significantly more time to respond to operational upsets.

## 2.4 Reduced challenges to the active or passive safety features

The use of fault-tolerant automation can reduce challenges to plant protection systems through its impact on operator performance and through its ability to keep complex operating systems within a prescribed operating envelope. Distributed, multivariate control techniques can be made less susceptible to single failures of sensors or components. Improved diagnostics and state-of-the-art graphical display techniques will help the operator know when the plant may be operating in a manner that might cause an operational upset unless some corrective action is taken.

## 3. THE APPROACH

These goals may be realized only if an intelligent plan of automation is pursued. This automation plan should consider integration of all elements of the control system (hardware, software, human). ORNL is designated as the lead laboratory for advanced controls and is responsible for DOE's national program planning in this area. The national program calls for a staged approach. The first stage is conceptualization, in which the most promising technological approaches are chosen for further study. The second stage is development and testing of each candidate. The third stage is computer simulations to demonstrate to users, designers and other researchers the advantages offered by the new control capabilities. All of these stages are underway at development sites at ORNL, ANL, GE and some universities. The fourth stage is plant demonstration and integrated testing of the developed strategy or technique. Some of this work is already under way at EBR-II. The fifth stage of this work will be interaction with ALMR designers and others to transfer the technology to the industry.

### 3.1 Plant Automation with Evolving Technology

In the U.S., the transition from today's nuclear control systems to the future designs for complete automation under human supervision is likely to occur in phases. The transition may be described in terms of 4 levels as shown in Figure 1. In Level 1, there will be some replacement of today's analog controllers with more reliable digital controllers performing basic proportional-integral-differential (PID) control. This phase of evolution is already under way in the U.S. [2,3,4,5]. Generally, digital implementations of control systems on U.S. reactors have been one-for-one replacements of the original analog systems and do not take full advantage of recent technological developments.

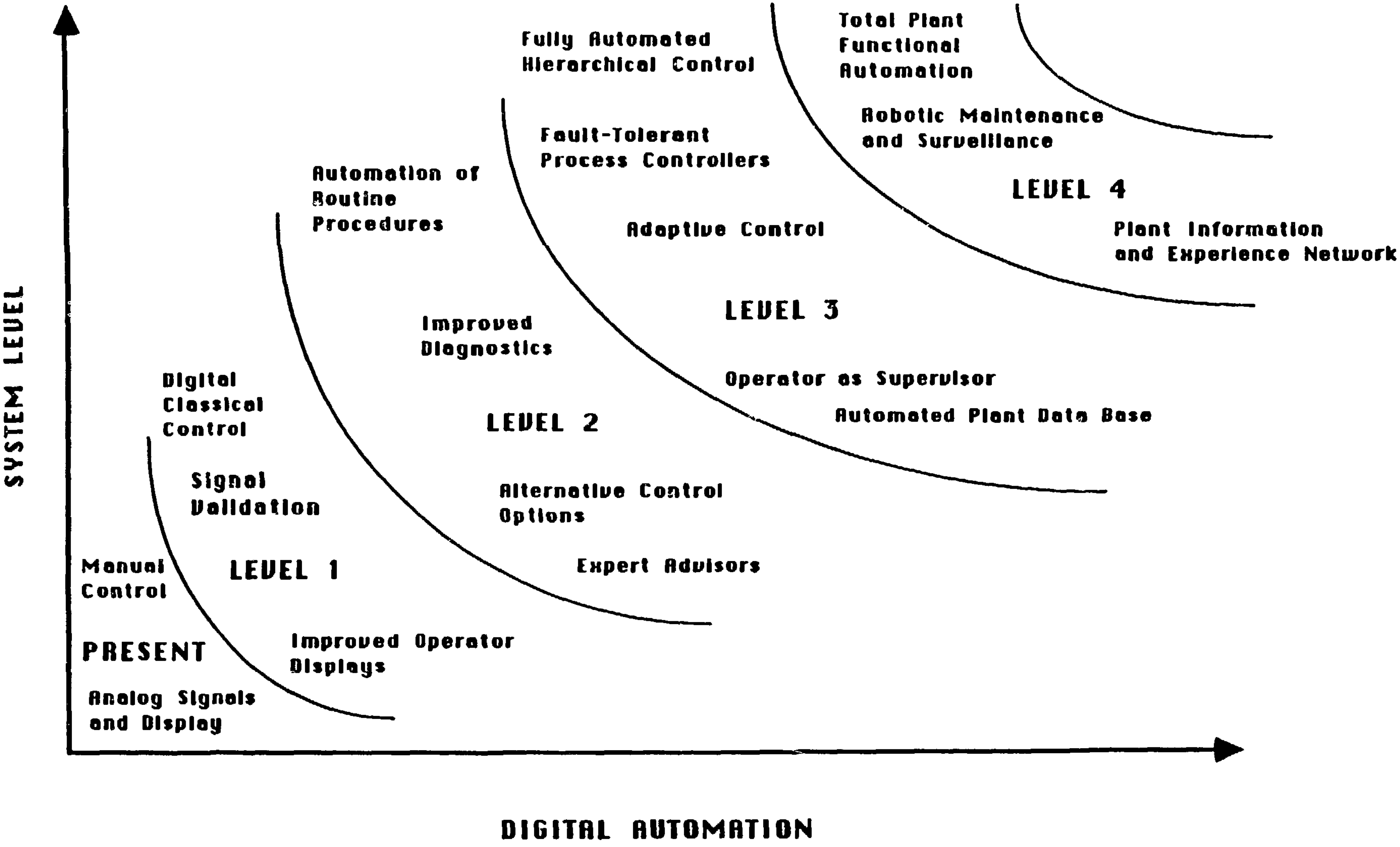
Total Plant Functional Automation
Fully Automated Hierarchical Control
Robotic Maintenance and Surveillance
Fault-Tolerant Process Controllers
LEVEL 4
Automation of Routine Procedures
Adaptive Control
Plant Information and Experience Network
SYSTEM LEVEL
LEVEL 3
Improved Diagnostics
Operator as Supervisor
Digital Classical Control
Automated Plant Data Base
LEVEL 2
Signal Validation
Alternative Control Options
Manual Control
LEVEL 1
Expert Advisors
PRESENT
Improved Operator Displays
Analog Signals and Display
DIGITAL AUTOMATION

Figure 1. Evolution of automation in nuclear power plants

In Level 2, routine procedures like startup, shutdown, refueling, load changes and certain emergency response procedures will be automated. Significant assistance will be given to the operator in the form of expert systems and control room displays of plant status. Control strategies will be predetermined choices selected from hierarchical, optimal, linear, robust, multivariate options. The EBR-II plant is moving into this stage now. The CANDU plant designs are at this level.

Level 3 is a significant advance toward automation. The operator's role will be to interact with and monitor the performance of the intelligent, adaptive supervisory control system. Smart sensors will validate their own signals and communicate with robust, fault-tolerant process controllers. The process controllers will be able to reconfigure the control logic to meet the operational objectives selected by the supervisory control system. Control strategies will be adaptive, uncompromised by nonlinear effects in the processes, and very robust to off-normal conditions. Plant designs will be completely automated with plant data bases available to the control system and the operator. Operational experience of all plant systems and components will be tracked in an automated data base. The control system will recommend maintenance schedules and outages to the operator. Human performance modeling will have permitted good allocation of function decisions in a way to keep the operator motivated and informed about plant status. This is the level targeted by GE for the PRISM plant design. Japanese plant designs also are targeting this level.

Level 4 is total automation of the plant, utilizing an intelligent control system aware of all operational status and in interactive communication with the operator to keep him apprised of operational status, any degraded conditions, likely consequences of degradations, and possible (recommended) strategies for minimizing deleterious consequences. By this time, plant designs will have many functions automated and robotized, including maintenance and security surveillance. The control system will be integrated with not only the total plant design, but also the national network of commercial power plants. The control system computer will learn from the network relevant information concerning other plants and component operational experience and will alert the operator if that experience is relevant to his plant. This level will not be reached by U.S. designs for many years.

## 4. DESCRIPTION OF ORNL WORK

To support the transition towards advanced automated control of nuclear plants, the Advanced Controls Program at ORNL is conducting four major kinds of activities:

> Demonstrations of advanced control system designs that would meet the goals described earlier;
>
> Establishment of a design environment that allows designers to formulate and test various control strategies;
>
> Testing and validation of advanced control system designs by simulation; and
>
> Guidance in control software and hardware specifications and implementation.

### 4.1 Demonstrations of advanced automated control system designs

ORNL is producing prototype demonstrations which show how appropriate state-of-the-art developments in control system theory, automation, artificial intelligence, information management, man-machine interface research and modeling, and computer simulation can be integrated into control system designs. These prototypic designs will demonstrate the advantages of advanced concepts and will be used as examples by ALMR designers in the DOE Programs.

#### 4.1.1 Balance of plant control

The balance of plant in any steam producing power plant is a complex system made up of feedwater pumps, valves, feedwater heaters, steam generators, turbines, turbine bypass systems and a condenser. In the U.S., analog control systems for the feedwater train are currently being replaced in some LWRs due to reliability and maintainability problems. The replacement systems are digital systems, but these are primarily digital versions of the analog (PID) control strategy previously used.

There are several better strategies possible with the use of digital control. These alternate strategies offer control of several parameters concurrently in an optimum manner to accomplish established goals and to meet imposed constraints. Benefits of multivariate strategies combined with smart sensors are increased fault tolerance, increased robustness, and increased flexibility to accommodate changes in hardware or software. ORNL is demonstrating simpler, fault tolerant, robust, flexible designs for the balance of plant systems of an Advanced LMR (PRISM). Although these demonstrations are for a multi-modular LMR, it will be useful to control system designers of all types of steam producing power plants. A first demonstration prototype for a feedwater train was completed in late 1988[6]. In 1989, the prototype was extended to include the other components making up the balance of plant.

### 4.1.2 Supervisory control

The design for PRISM (and some other types of advanced reactors) incorporates multiple modules which together produce power to meet grid demand. A chief virtue of multimodular plants is increased flexibility aimed at increased plant availability. For instance, if one reactor is shut down for refuelling, all others should be able to continue operation. A complication of the multimodular design is that all reactor cores are to be coordinated to meet the power demand and take advantage of the potential increase in availability.

To help with the increased complexity of highly automated multimodular plants with a reduced operating staff, ORNL is conducting research in supervisory control. In 1988, ORNL demonstrated an example of a hierarchical supervisory control strategy for one reactor[7]. A follow on demonstration, completed in FY 1989, included a three reactor power block like that proposed for PRISM. The controller structure is shown in Figure 2. At the top level of control is a plant level supervisory controller which determines how grid demands will be met, if possible, by the modules. Each module controller tries to meet the power demand of the

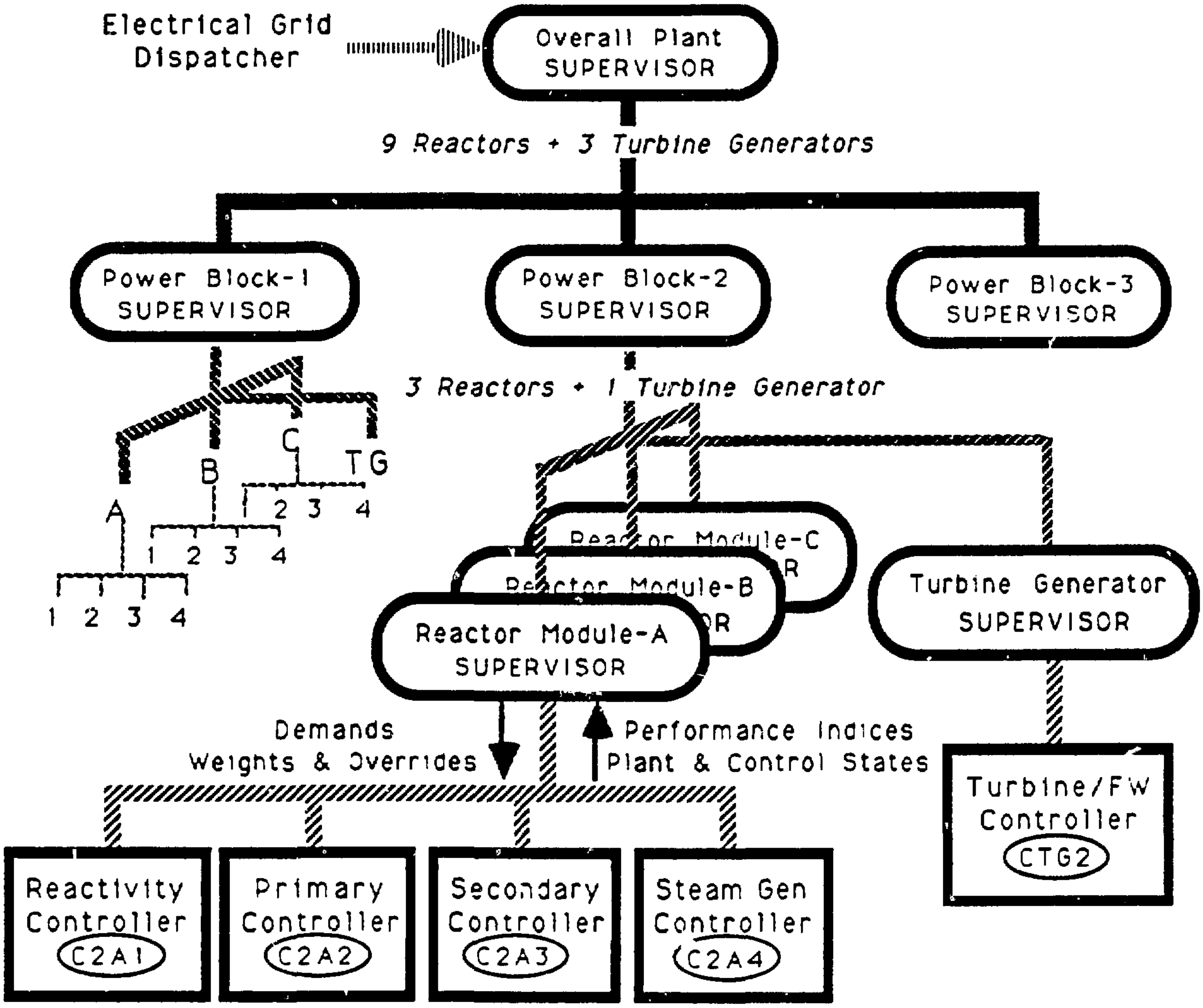

Figure 2. ALMR Supervisory controller architecture

plant supervisory controller by coordinating multiple reactor cores. This hierarchy continues down to the level of component control. The supervisory controllers at each level also monitor the performance of the controllers under it to assure its goals are being met and to detect faults in the plant or controllers.

This work includes a nonlinear, multivariate, optimal controller strategy developed as part of this program. This strategy allows the controller to follow a demand in the presence of unknown variations of parameters and subsystem responses. As a nuclear reactor goes through its normal range of operation, some of the plant parameters change. The nonlinear control strategy developed has the ability to track changing parameters and continue to optimally control the reactor or reactors.

As this development matures, the concept will be demonstrated in a collaborative effort with ANL and INEL at EBR-II on various subsystems.

### 4.1.3 Automated Start-up

ORNL is working on demonstrations of automation of parts of a plant start-up. The scope of the ORNL work is to develop software programs, control strategies, and control system philosophies for automated start-up of advanced reactors. In a collaborative effort, ANL/EBR-II will provide the necessary reactor facility for demonstrating the advanced control and diagnostics concepts where practical.

The first task is to implement a computer graphics aide in the control room that assists the reactor operator. Progress to date includes implementing the reactor start-up checksheets on a computer. This task provides an initial interface between the reactor operator, the display screens and the computer workstation, and provides a procedure prompting service to the operator.

Next, ORNL will provide to ANL algorithms and software to perform advanced optimal start-up control. ANL will provide the necessary engineering and manpower to get the equipment installed in the plant. GE participation in the planning of this demonstration assures maximum transferability of results to the PRISM design.

## 4.2 Design environment

The Advanced Controls Program will provide a centrally located, user friendly control system design environment. This environment will be available for control system designers within the ORNL program, the DOE community and, later, for any qualified user. The environment will consist of four parts: a) networked, intelligent, computer workstations into which have been integrated software tools, graphics capabilities, on-line design guidance, on-line documentation and interfaces to the large plant simulation capability at ORNL; b) plant/component models and databases useful for control system design and plant simulation; c) man-machine interaction models and guidelines for designing control system interfaces with operators; and d) information resources concerning control system strategies for automated control.

### 4.2.1 Intelligent controls analysis and design workstations

ORNL is developing a Controls Analysis Workstation for efficient engineering of control systems, especially for advanced modular liquid-metal reactors. The workstation is a desk-top computer and software package that provides a control system designer full capability from design through simulation to code generation.

The graphically-based software package provides a means of assembling models of the power plant and its subsystems[8]. The resultant model appears as a schematic of the plant. Software for automatic model generation will formulate the mathematical models of the plant using the plant schematic diagram. Some customizing may be required by the designer to arrive at a final model. The designer can interact with the plant model and candidate control system in either an on-line or an off-line mode, depending on the need.

### 4.2.2 Strategies for advanced control

Techniques of modern multivariate, optimal, and adaptive control are being examined for their potential benefits in actual reactor control and operations. Adaptive control schemes which allow the control system to adjust itself to variations in the internal parameters or conditions of the process being controlled are under evaluation.

A loop transfer recovery technique (LTR) technique which extends the response of a linear quadratic gaussian (LQG) controller and allows the designer to balance performance and robustness with respect to plant parameter variation is being used in some prototype designs.

4.2.3 Human-machine integration R&D

Cognitive Engineering support for the Advanced Controls Program will be provided in three areas. They are: 1) the preliminary design phase, 2) the final design phase, and 3) the testing and evaluation phase.

Expert, high-level advice to designers will aid their formulation of feasible objectives, performance specifications, and functions in the preliminary design phase. Specific cognitive engineering support will be in the form of expert high-level cognitive engineering design guidelines provided through an expert system that specifically considers the role of the operator in the system design. A set of preliminary guidelines was developed in FY 1989.

The design phase of the life-cycle involves developing design alternatives to achieve the overall objectives of the system, with consideration given to levels of automation (allocation of function). The cognitive engineering support for this phase will include the development, testing, and validation of a human operator model. A qualitative model of a human operator is being developed in a framework combining the capabilities of network simulation and knowledge-based simulation[9]. Prototype development was completed during FY 1987. In conjunction with other models, it will be applied within a workstation environment to aid in the evaluation of various design alternatives within a "total system" perspective, i.e., a system that includes all active elements including the human operator.

During the testing and evaluation phase, cognitive engineering support will be provided for assessing the performance of real operators within a real-time, full-scope simulator. Efforts will include support for the development of procedures, selection and training requirements and training systems.

### 4.3 Testing and validation of advanced control system designs by simulation

The ultimate goal of this task is to ensure that the users will be provided with the capability of simulating up to and including an entire control system design (both hardware and software) interacting with an "entire" nuclear plant. This will require real-time simulation capabilities for a wide variety of reactor subsystems, integrated systems, and controllers and is a key element in the PRISM development plan. Progress to date includes the acquisition and networking of a parallel processor computer, several Sun workstations, various other workstations and small computers into a substantial simulation capability.

### 4.4 Control software and hardware R&D

The Advanced Controls program will evaluate or provide standards, guidelines, and specifications for control software and hardware. ORNL will acquire and develop tools and methods for generation of large software programs needed for automation of nuclear reactors. Methods for locating logical faults and errors in software programs will be acquired and developed. The program participants will develop standardized software programs that will accommodate computer hardware system failures and plant component failures. Software verification and validation procedures will be acquired or developed and utilized. This work will begin in FY 1990.

## 5. DESCRIPTION OF ANL WORK

Automation involves the integration of computers and associated software with the human operator. The issue of reliability is being addressed at ANL in two ways: first, by making the reactor system designs tolerant of failure of individual controllers and tolerant of human error; and second, by improving and verifying the fault tolerance of computer hardware and software. EBR-II continues to conduct plant tests intended to demonstrate passively safe response to controller failures. The tests include simulation of total station blackout, loss of heat sink with failure to scram and tests that evaluate and demonstrate system response to individual controller failure. For example, a rapid run-up in speed of either the primary or secondary pumps leads to very mild transients. The same can be said for failures in the steam-system controllers, such as a rapid opening of the turbine throttle valve or the steam bypass valve. Since all of these operational upsets result in safe conditions, the concerns for controller reliability are much less and new technology can be much more aggressively applied.

### 5.1 Sensor validation

One method of sensor validation that has been tested at EBR-II is that of pattern recognition. A software package called the System State Analyzer[10] (SSA) has proven that pattern recognition techniques can not only determine the state of a plant, system, or component, but it can also show a failing signal and generate an accurate estimated signal for that sensor. The SSA has been tested both during normal operation and in special tests. In all cases, the SSA has responded appropriately.

The SSA works using "learned states" consisting of time slices of selected instrument channels that have relationships to each other. A current time slice of information is compared to the learned states library, and a match is found to the nearest learned state. In addition, an estimate is made of the value of each input signal based on the values of all the other signals. A plot is provided which shows the estimated value of the signal, a measure of the uncertainty, and a plot of the actual value of each signal. Accuracy of the SSA has been demonstrated to be very good.

Another means of sensor validation is the Sequential Probability Ratio Test (SPRT). The SPRT[11] is a mathematical procedure derived from sequential analysis (or time series). The SPRT is a statistical process which examines two signals, folds in historical data from the signals, and logically decides whether the signals are representing the same physical quantity. The SPRT methodology has been investigated to some degree at EBR-II and will likely be included with the fault-tolerant computer in some validation role.

Analytic Redundancy[12] is yet another method of sensor validation that has an application in nuclear (and other) systems. The technique, simply described, is one where signals that are related to a quantity are used as inputs to a model which is used to calculate the desired quantity. This technique may be used to provide redundancy where it is not practical to provide actual hardware redundancy. At EBR-II, the usefulness of analytic redundancy was shown when it was utilized to provide a double check on the remaining flowmeters in EBR-II after several of the original, non-replaceable flowmeters failed.

Additional methods have been proposed and used for sensor validation, including several variations of Kalman filter techniques and other, similar approaches.

## 5.2 Graphics, real-time communication and diagnostics

Work has been done at EBR-II, using ideas presented in the literature by Beltracchi[13], Rasmussen[14], and others, to construct real-time graphical displays that are true thermodynamic models of the plant. The graphics present information such that chunking[15] of information takes place. In this manner, it is actually possible to convey to the operator what state the plant is in and the relationships between systems and functions at any time. The ability of the human as a pattern recognition expert is exploited by using the computer to gather plant data and convert it to a graphical thermodynamic model of the plant process.

Diagnostics is another area where good progress has been made. At EBR-II, there are two specific approaches that are being used. The first is a pattern recognition system, and the second is a custom built expert system specifically designed for realtime work using fuzzy logic. The pattern recognition technique uses a workstation to receive plant signals and compare a "present" set of data to a set of pre-learned data (representing plant states). This comparison of the real-time data with the pre-learned patterns allows the status of the system to be deduced.

The real-time expert system approach consists of using a computer program "DISYS"[16], which allows the modeling of a system from the sensors, through components, groups of components, and through logic nodes. As real-time signals are gathered, the program also deduces which operational mode the system should be in, based on control signals. Instrument readings, after conditioning, etc., are sent through the nodal network, and a deduction made as to whether the system is operating properly.

### 5.3 Networking and distributed control local intelligence

At EBR-II a continuous upgrade program[17] has resulted in the installation of numerous digital controllers in the plant. The controllers have the capability to be networked together and to communicate to supervisory controllers or computers. Issues being considered at present include the need for redundant networks, the capability for failure detection, and the ability to switch smoothly from manual to automated control.

### 5.4 Plant testing of passive safety features

To ensure that advanced control techniques do not challenge the passive safety features of plants and systems, there is considerable effort at EBR-II directed at understanding the mechanisms of passive safety features as well as other plant dynamics. Several series of tests have been run at EBR-II that have served to characterize plant system transfer functions. As a result of these tests, a good understanding is emerging of the requirements for advanced control as applied to advanced reactor plant systems. A finding, based on plant testing, is that control systems must be carefully designed to prevent abrogation of the passive safety features inherent in system design.

### 5.5 Fault tolerance

At EBR-II an effort has been on-going to develop a method to provide formal proof of "the correctness" of fault-tolerant micro-processor based computers[18]. A fault-tolerant computer which has four processors is being analyzed and tested. The methods used to prove fault-tolerance include the use of theorem provers as developed at the Argonne Math and

Computer Science Division. These methods have been reported elsewhere and appear to allow proof that both the hardware and software will meet (or will not meet) the specifications of performance. By using these techniques, a fault-tolerant processor is being qualified for use as a safety circuit trip at the EBR-II plant.

## 6. DESCRIPTION OF RESULTS OF GE WORK

The modular PRISM (ALMR) 1395 MWe power plant concept as developed by GE Nuclear Energy will include an advanced state-of-the-art control system designed to facilitate plant operation, optimize availability, and protect plant investment. The control system will feature a high degree of automatic control and an extensive amount of on-line diagnostic and operator aids. GE Nuclear Energy sets the overall design requirements for the control and protection system, working with ORNL and ANL [and others where appropriate] to take advantage of the state of the art in digital technologies.

### 6.1 Introduction

The PRISM plant concept, selected by the DOE as the basis for the Advanced Liquid Metal Reactor plant design, consists of three power blocks, each made up of three identical reactor and steam generator modules connected through a common steam header to one turbine. Feedwater to the three steam generators in the power block configuration, along with the major control devices is shown in Figure 3. The control system is designed to control the multiple plant reactor modules and realize the full availability improvement potential of a multi-module plant while protecting plant equipment. Sufficient automation is built in to support a design goal of operating an entire power block with one operator under both normal and faulted conditions. All normal plant operations (such as startup, shutdown, load-following) are automated. The simplicity of the PRISM plant configuration (no control valves in the primary and secondary system, constant speed feedwater pumps), and the

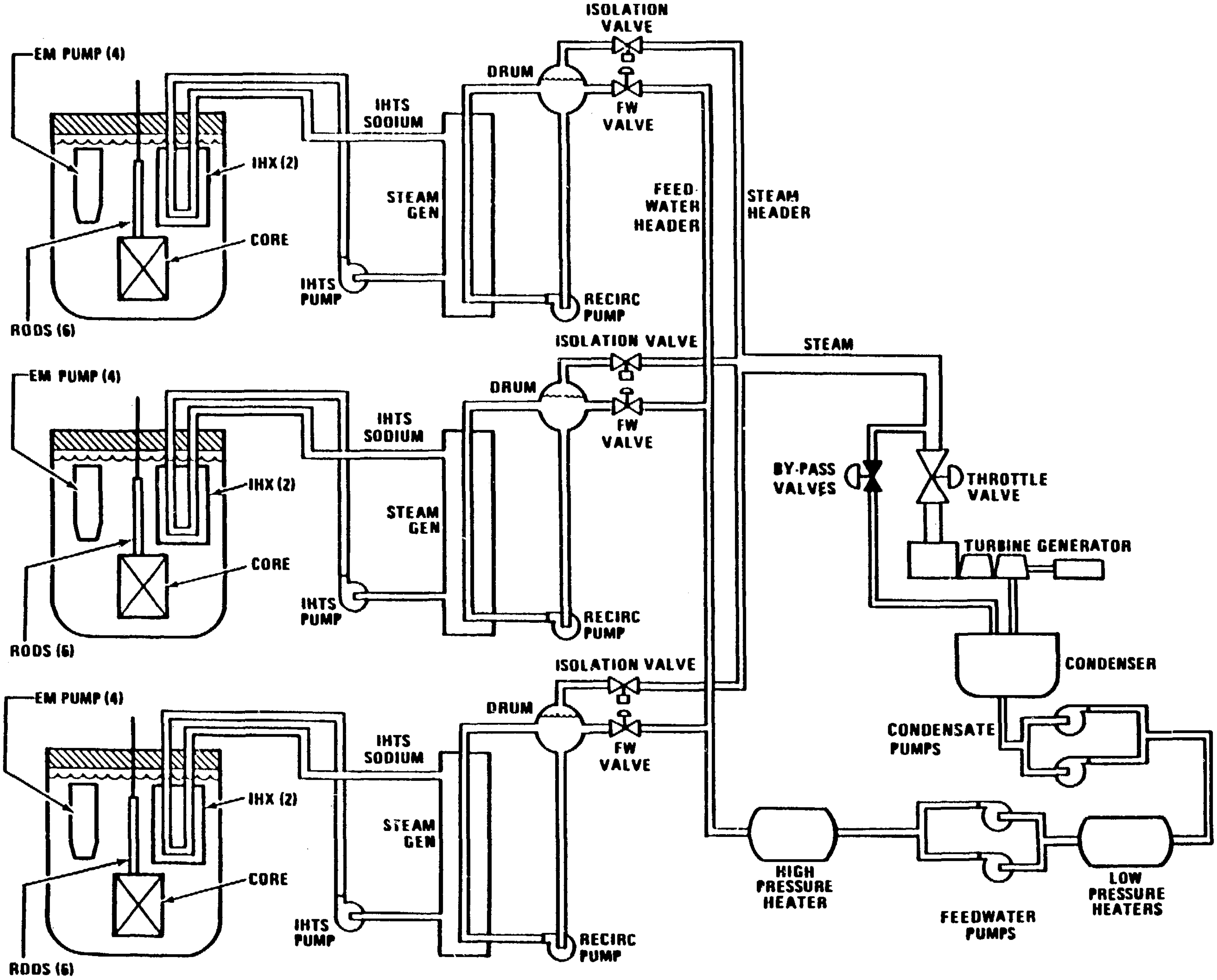

Figure 3. ALMR power block overview

inherently simple operability of the modules (large negative reactivity feedback, tightly coupled small core with only six control rods) has allowed increased automation to be introduced at reasonable cost.

Functionally, PRISM control consists of two basic elements: 1) the plant control system (PCS) and 2) the reactor protection system (RPS). The RPS is a highly reliable Class 1E system (designed on a per reactor basis) whose purpose is to automatically scram the reactor whenever safety setpoints are exceeded; whereas the PCS is an integrated plant-wide control system which provides for optimal control and operation under normal and faulted conditions. The RPS, backed up by the inherent safety features of PRISM, provides ample margin for defense against events that challenge plant safety. The RPS is cleanly separated from the PCS (RPS uses separate sensors, separate electronics, and separate actuators) so that no fault in the PCS can prevent the RPS from performing its safety function. This allows the PCS to be designed to protect plant investment, optimize availability, and facilitate plant operation without being burdened with safety functions.

## 6.2 Control system overview

The plant is controlled by an integrated network of computationally powerful controllers distributed throughout the plant and arranged hierarchically, as shown in Figure 4. The controllers perform automatic control actions, provide processed information to the operator, and respond to manual control commands from the operator's console. A plant data highway connects the operator consoles (one for each power block) to the supervisory controllers, and also provides data for consoles located in the support facilities (Technical Support Center, Operations Support Center). The controllers are redundant and fault tolerant, with automatic self-calibration and self-test features. Interconnection between the controllers is through a set of redundant noise-free fiber-optic data communication links. The supervisory controllers are used primarily for sending down setpoints to the local controllers, and for translating diagnostics from the local controllers into automatic action by other localcontrollers or suggested action by the operator. The NSS and BOP controls are integrated through the supervisory controller to facilitate overall plant control. At the local level the controllers use the real plant

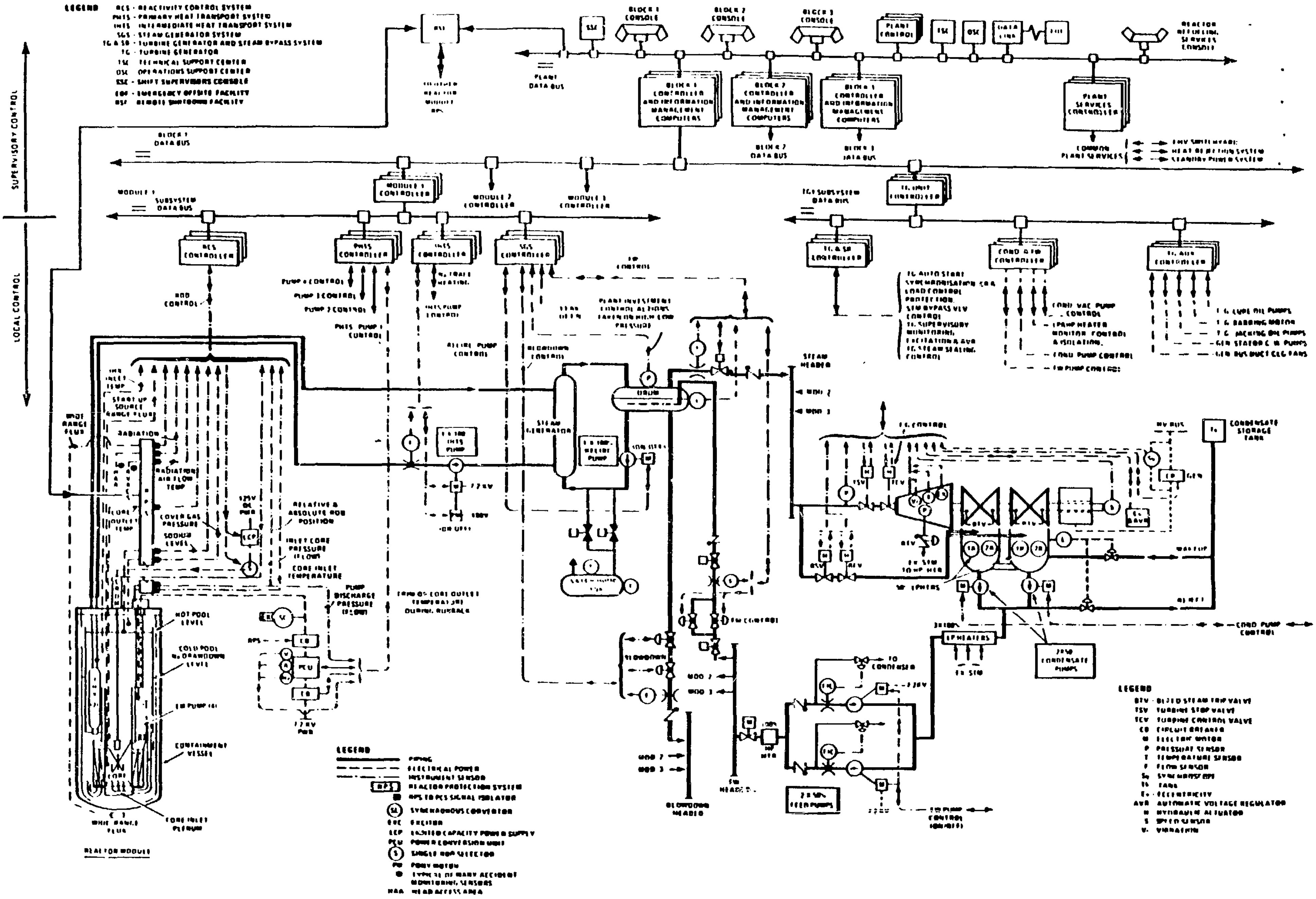

Figure 4. ALMR hierarchical control and plant interfaces

process data as input, run real-time state models of the process that they control and determine optimal control for the actuators, based on the supervisory controller setpoints. The local controllers also provide on-line component performance and degradation data for improved operation and maintenance evaluations.

Functional processing activities performed within the model-based controllers include data acquisition, reduction and validation; plant state estimation; analysis of plant performance; diagnosis of malfunctions; determination of correct control strategy; generating commands to subordinate controllers or actuators; providing decision support to plant operators, and maintenance advice to the maintenance operators. These functional activities, implemented through plant control software, are shown schematically in Figure 5.

The dynamic process models running in the controllers detect off-normal behavior on a continuous on-line basis. Incipient failures are identified and annunciated for corrective action or maintenance before they become major problems. If the failure can be handled by the local controller, it will automatically take action by itself, otherwise it will alert the higher level controllers and they will take the appropriate action. For simple transients the control system takes action automatically. For complicated multiple failure transients, where the transient diagnosis and mitigation strategy cannot be determined automatically, the control system alerts the control room operator and provides him with operator-aids that help identify the fault(s), and operator-prompts that assist him in taking the proper action.

### 6.3 Supervisory control

Supervisory control is provided at both the plant and block levels. At the plant level, the supervisory controller receives the grid dispatcher's demand and coordinates load demands with the three power blocks, via the power block controllers. The power block level supervisory controllers in turn coordinate the respective module controllers and turbine generator unit controller, and hence the lower level local controllers. The block

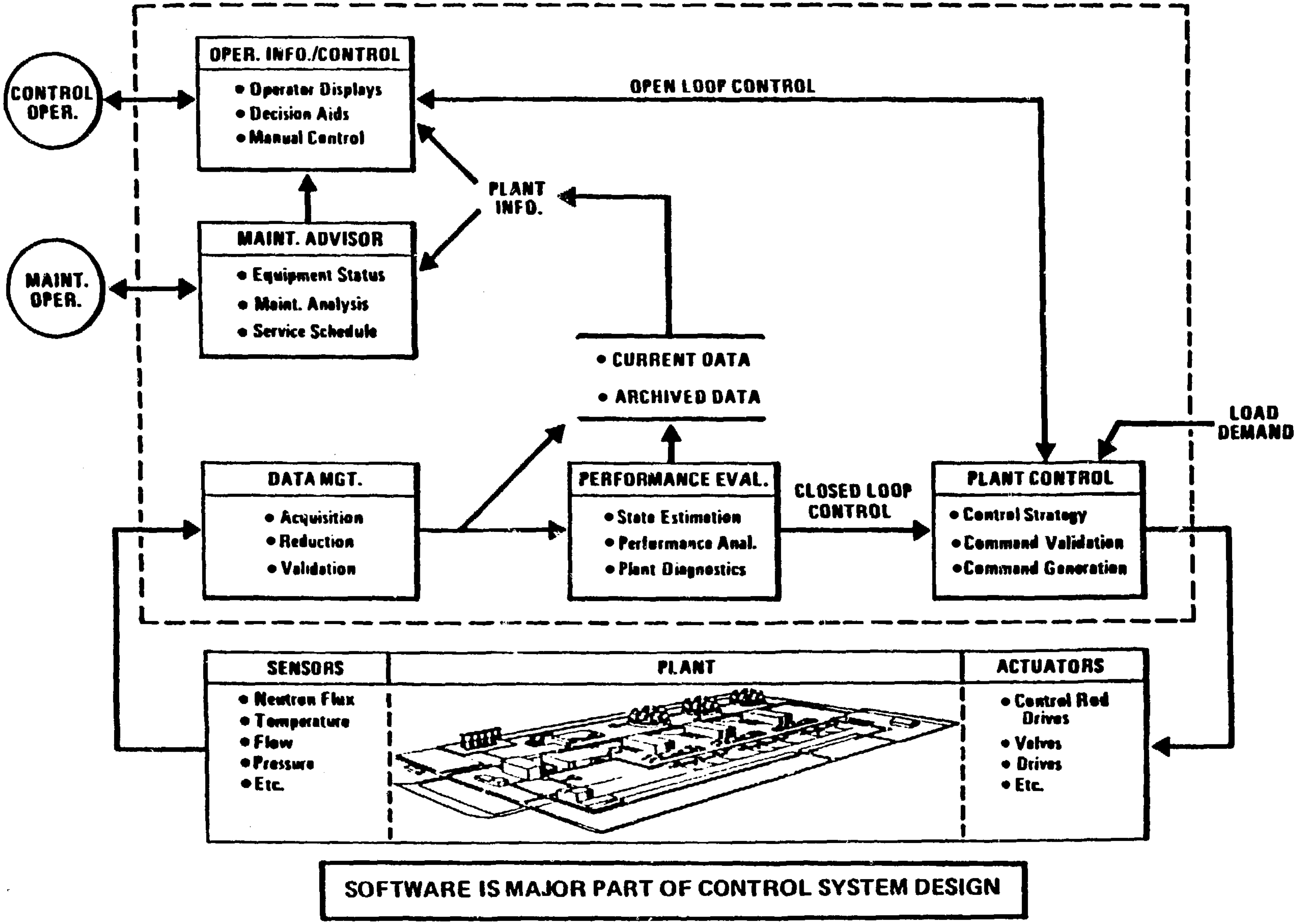

Figure 5. PCS software elements

controllers are also responsible for presenting plant data to the operators and providing an interface from which the operators can manually control the plant.

### 6.3.1 Automatic Control

Under automatic control, the supervisory controllers direct the local controllers either to perform sequential discrete control operations (primarily during startup) or to follow setpoint commands during continuous control (primarily through the 25-100% power range operation). These sequential actions or setpoints are determined through an evaluation of the plant state based on inputs from lower level controllers and knowledge of plant goals from higher level controllers, the operator, or grid dispatcher demands. Allocation of power to modules within a block is generally equal assuming all modules are at the same power and have the same margin available. However the allocation can be uneven if one module is power limited (and has less margin available) or if accelerated (or decelerated) burnup on a module is desired.

As an example of automatic operation during abnormal events in a block, consider the case of trip of Reactor 1. The Reactor 1 control system would automatically recognize the condition and alert the block controller. The block controller automatically interrogates Reactors 2 and 3 and commands them to raise power if they have margin, thus increasing availability. At the same time diagnostics on why the reactor tripped is sent to the operator so that he can take corrective action and bring it back on line as soon as possible.

### 6.3.2 Operator Information

In addition to the automatic control function, the supervisory controller is also responsible for presenting data to the operator and providing an interface for the operator to take manual action.

The information presented to the operator is well processed and the displays are designed according to human factors engineering standards. Trends are displayed along with the current value for easy understanding of the plant status. Capability of analyzing historical and sequence of events data is provided for evaluation of plant transients. An integrated alarm system is provided which analyzes alarms and presents them hierarchically in order of importance so that in the event of an accident the operator alarms and can request whatever level of alarm detail he wants. The operator displays are menu driven and any one of them can be called up easily at any time from the console.

A high level of plant automation is used; however, the capability for manual backup is provided. Both discrete plant components (such as valves and pumps) and entire plant processes (such as power runback) can be controlled manually by the operator. Such manual control is done through special control displays and control function keys available on the operators console.

## 6.4 Local control

The local controllers are responsible for controlling systems and subsystems within a power block. The controllers run models of the processes and systems they are controlling. These models contain an "estimator" or "observer" of the local physical systems operation which calculates key parameters, including those which cannot be measured directly (such as reactivity). All the key variables are fed back into the control process and this enhances the local controller performance. The feedback gains are selected to meet desired performance specifications. Faults occurring in the plant are detected and acted upon at low levels in the control hierarchy.

The local control stations communicate with the power block and plant level controllers via a redundant data bus, thus the probability of loss of communications is low. If loss of communication occurs, it is detected by both the local controller and the higher level controllers through loss of the "handshake" data exchange between the controllers.

## 6.5 Plant control complex

The plant control complex includes the man-machine interface needed for plant operation. Included in the control complex is the control center, remote shutdown facility, technical support center, and operations support center. Each of these areas provides unique support to the operators who direct the control of the plant and the technical and administrative staff who maintain it.

### 6.5.1 Control Center

The control center (CC) is the center of operations where the operators perform all the monitoring and control functions required. Preliminary analysis has indicated that through the use of extensive automation, the primary man-machine interface within the control center can be served by three consoles. Each console handles operations for an entire power block and is designed for one-man operation. The NSS and BOP controls for a power block are fully integrated into the block operator's console. Plant information is presented on video display units in the console and on a large viewing screen. The video screens are under software control and the displays are menu driven so that any display can be brought up on any screen. One screen is reserved for alarms so that whenever an alarm occurs it is logged and displayed and never lost. Displays are in real time, but old data can be called up, analyzed, and displayed if the operator so chooses. Manual control by the operator is also done from the console via the display screens and the console keys.

### 6.5.2 Remote Shutdown Facility

The remote shutdown facility (RSF) contains a Class 1E console from which all power blocks (nine reactor modules) can be shut down. Class 1E shutdown and accident monitoring capability is provided at the console. This facility is used in the event the control center is not operational (due to total PCS failure) or uninhabitable. The RSF is a seismic Category I building and contains a Class 1E HVAC system for operator protection.

### 6.5.3 Other Support Facilities

A technical support center (TSC) and operator support center (OSC) are provided with consoles connected to the plant data bus. These consoles are used only for information and have no plant control capabilities. The TSC provides technical support to the control room operators, especially in the analysis of plant transients. The OSC provides for an integration of group technical tasks (such as maintenance surveillance, testing, and calibration) which go on continuously during plant operation. An emergency off-site facility (EOF) is provided which receives processed data from the plant via a data link.

## 7. RELATIONSHIP TO COMMERCIAL NUCLEAR INDUSTRY

The commercial reactor industry in the U.S. is beginning to take advantage of some aspects of digital and advanced control technologies. The infusion of more advanced concepts into the LWR industry will be a slow process, as described earlier. The DOE-sponsored programs described in this paper will demonstrate for all of the nuclear industry how to take better advantage of technological advances. These demonstrations will be performed on computer simulations, tested at EBR-II and then utilized in the PRISM design.

Several industrial groups are already aware of these programs and are participating in technology transfer activities. For example, the Babcock and Wilcox Owner's Group is collaborating with DOE and ORNL in a joint effort to upgrade the Integrated Control System, utilizing some of the algorithmic approaches suggested by ORNL and others. ORNL is also being funded to assist in the DOE/EPRI ALWR Program, particularly in the areas of standards and man-machine interface requirements.

## 8. SUMMARY

The design of an ALMR has illustrated the need for an advanced control system architecture. Several organizations in the U.S. have joined in an effort to develop the needed systems for the new generation reactor plant. New techniques are being developed and tested under simulation. To the degree possible, they will be tested on the EBR-II plant. This facilitates a confident procession toward automation in the new generation of modular systems such as PRISM. The new capabilities will lead to improved plant operation which should enhance safety, availability and operability of the new passively safe LMRs. Spin-offs from this work already are beginning to impact the LWR community in the U.S.

## REFERENCES

[1] Personal communication: ALLEY, A. D., General Electric, San Jose, CA to R. A. Kisner, Oak Ridge National Laboratory, January 12, 1988.

[2] DIVAKARUNI, M., et al, "BWR Feedwater Control System Replacement in Monticello Plant", EPRI NP-4769-SR, September, 1986.

[3] MUELLER, N. P., and SILER, F. M., "PWR Feedwater System Failure Data as a Basis for Design Improvements", EPRI NP-4769-SR, September, 1986.

[4] GAYDOS, K. A., et al, "An Optimal Control Strategy in the Design of a PWR Feedwater Controller", EPRI NP-4769-SR, September, 1986.

[5] GRAHAM, K. F., and DIVAKARUNI, S. M., "EPRI Digital Feedwater Control Project: System Verification Plans in an Operating Plant", EPRI NP-4769-SR, September, 1986.

[6] WILSON, T. L., "Balance of Plant Control for the PRISM", Proceedings, 7th Power Plant Dynamics Control and Testing Symposium, May 15-17, 1989, University of Tennessee and IEEE Control Systems.

[7] OTADUY, P. J., BRITTAIN, C. R., ROVERE, L. A., "Supervisory, Hierarchical Control for a Multimodular ALMR", Proceedings, 7th Power Plant Dynamics Control and Testing Symposium, May 15-17, 1989, University of Tennessee and IEEE Control Systems.

[8] ROBINSON, J. T., "An Intelligent Simulation Environment for Control System Design", Proceedings, 7th Power Plant Dynamics Control and Testing Symposium, May 15-17, 1989, University of Tennessee and IEEE Control Systems.

[9] SCHRYVER, J. C., "Operator Model-based Design and Evaluation of Advanced Systems: Computational Models", Proceedings, 1988 IEEE Fourth Conference on Human Factors and Power Plants, June, 1988, Monterey, CA, p. 121-127.

[10] KING, R. W., SINGER, R. M., "Development and Application of Diagnostic Systems to Achieve Fault Tolerance" Proceedings, 7th Power Plant Dynamics Control and Testing Symposium, May 15-17, 1989, University of Tennessee and IEEE Control Systems.

[11] WALD, A., Sequential Analysis, Wiley New York (1947).

[12] RAY, A., DESAI, M. N., and DEYST, J., "Fault Detection and Isolation in a Nuclear Reactor", Journal of Energy, Vol. 7, No. 1, Jan-Feb. 1983, pp. 79-85.

[13] BELTRACCHI, L., "A Direct Manipulation Interface for Heat Engines Based Upon the Rankine Cycle", IEEE Transactions on Systems, Man, and Cybernetics, Vol. SMC-17, No. 3, May-June, 1987.

[14] RASSMUSSEN, J., "Skills, Rules, Knowledge: Signals, Signs, and Symbols and other Distinctions in Human Performance Models". IEEE Transactions on Systems, Man, and Cybernetics, SMC-13, 257-267 (1983).

[15] EGAN, D. E., SCHWART, B. J., "Chunking in Recall of Symbolic Drawings", Memory and Cognition, 1979, 7 (2), pp. 149-158.

[16] EDWARDS, R. M., CARPER, J. C., LINDSAY, R. W., ROBINSON, G. E., "Real-Time Testing of A Diagnostic and Control Guidance Expert System", Proceedings, 7th Power Plant Dynamics, Control and Testing Symposium, May 1989

[17] CHRISTENSEN, L. J., SACKETT, J. I., DAYAL, Y., WAGNER, W. K., "Plant Automation: EBR-II Experience and Future Plans with GE ALMR," ibid, Vol. 1, pp. 37.01-37.06.

[18] CHISHOLM, G. H., KLJAICH, J., SMITH, B. T., WOJEIK, A. S., "Towards Formal Analysis of Ultra-Reliable Computers A Total Systems Approach," Proceedings,7th DASC Digital Avionics Conference, Oct 13-16, 1986, Fort Worth-EEE, AIAA.