CONF-890673--2

DE89 014776

OVERVIEW OF THE US PROGRAM OF CONTROLS FOR ADVANCED REACTORS*

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

J. I. Sackett, L. R. Monson, R. W. Lindsay
Argonne National Laboratory
Idaho Falls, Idaho 83403

D. G. Carroll
GE Nuclear Energy
San Jose, California 95153

Submitted to the IAEA/IWGFR for presentation
at the
Specialists Meeting on Advanced Control
for Fast Reactors
Argonne, USA
June 20-22, 1989

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

OVERVIEW OF THE US PROGRAM OF CONTROLS FOR ADVANCED REACTORS

1. INTRODUCTION

An automated control system can incorporate control goals and strategies, assessment of present and future plant status, diagnostic evaluation and maintenance planning, and signal and command validation. It has not been feasible to employ these capabilities in conventional hard-wired, analog, control systems. 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.

Under the sponsorship of 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 the EBR-II site by Argonne National Laboratory (ANL) , and 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 presents an overall U.S. national perspective for advanced controls research and development. The goals of high reliability, low operating cost and simple operation are described. The staged approach from conceptualization through implementation is discussed. Then the paper describes briefly the work being done by ORNL, ANL and GE. The relationship of this work to the U.S. commercial industry is also discussed.

2. NATIONAL PERSPECTIVE

Contemporary experience of U.S. industries--steel, automotive, aviation, electronics, defense, and food processing--has shown that to compete successfully, a high degree of automation is needed. The U.S. nuclear industry also will have to employ automation in plant operation, control systems, maintenance, and construction to compete with alternative power sources. For the advanced liquid metal reactors (LMRs) in the U.S., the goals of advanced, automated plant control systems include improvement of plant availability, low operating costs, simple operation (especially of multimodular plants like the PRISM design), and reduced challenges to plant safety systems.

2.1 Improved Reliability

Analog subsystem controllers, used in the essential control processes in current U.S. nuclear power plants (NPP), have evolved over many years and have generally performed satisfactorily around a design point. Performance of these analog controllers is limited, however, 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. Good reliability can be further enhanced by use of fault-tolerant design techniques, previously used only in NPP protection systems. Communications among subsystems and other levels of hierarchy is greatly improved and simplified by digital techniques. Multiplexed fiber-optic data transmission and distributed architectures provide an opportunity for noise reduction (and significant construction cost saving) by minimizing cables and interconnections. The availability of on-board memory 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. These and other advantages of advanced, digital control technology can provide significant improvement in plant availability.

2.2 Low operating costs

Recent work 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]. Sufficient automation will be built in to support a design goal of one operator running an entire power block under both normal and faulted conditions. All normal plant operations (such as startup, shutdown, load following, etc.) will be automated.

2.3 Simple operation

Although U.S. nuclear power plants currently exhibit some automation at the individual or subsystem level, integration and coordination of subsystems is minimal. The tasks of managing the interactions among systems is left to the operators. Even in plants where a form of cross limiting between subsystems is used to provide anticipation of major changes in parameters, prompt operator interaction is still required to re-establish satisfactory operating conditions. The PRISM reactor, being designed by General Electric under the sponsorship of the U. S. DOE, is a modular system that has significant requirements for automation. Modular systems must be automated to keep plant operation well coordinated. Even discounting economic considerations, the large operating crew required if there is no automation has the potential for poor coordination of effort. 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 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). The effort to develop control system concepts and prototypes that are appropriate for advanced fast reactor power plants is concentrated at ORNL, ANL and General Electric. ORNL is designated as the lead laboratory for advanced controls and is responsible for the 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. Level 1 will include automated data management at a plant. This is actually occurring to a limited extent now in U.S. LWRs. In this level there will be some replacement of today's analog controllers with more reliable digital controllers performing basic proportional-integral-differential (PID) control. EPRI has sponsored demonstration of selected subsystem automation in operating plants [a Monticello unit owned by Northern States Power, Dresden Units 2 and 3 owned by

Commonwealth Edison, and the Sequoyah plant owned by the Tennessee Valley Authority] [2,3,4,5]. Digital reactor protection systems are also currently operational at Arkansas Nuclear One-Unit 2, Southern California Edison's San Onofre Units 2 and 3, Arizona Public Service's Palo Verde and Louisiana Power and Light's Waterford Unit 3. Generally, digital implementations of control and safety 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.

Manufacturers are developing product lines of digital instruments and controllers intended both for installation in new plants and replacements for their analog counterparts in today's operating plants. Most of the current effort is being applied to hardware reliability, fault tolerance, and communications. Functional performance (algorithm improvement), which now resides mostly in software, is receiving somewhat less emphasis.

Level 2 will be automation of routine procedures like startup, shutdown, refueling, load changes and certain emergency response procedures. 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.

Level 3 is a significant advance toward automation with capability for full automation of all hierarchical levels of control. 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.

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

Oak Ridge National Laboratory is integrating emerging technologies in control theory, software engineering methodologies, very high level languages, advanced computer architectures, artificial intelligence, human-machine modeling, and plant-wide design database management into advanced control concepts. Collaboration with other national DOE LMR program participants is assuring an integrated program for advanced reactor concepts.

4.1 Overview of program tasks

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.

4.2 Demonstrations of advanced automated control system designs

The purpose of this group of activities is to provide timely demonstrations of prototypic designs for control systems for selected aspects of the ALMR concept (PRISM). The first demonstrations will be made on the computer simulators at ORNL and other national laboratories and, in some cases, the demonstrations will be made on prototypic controller hardware. Where possible, these demonstrations will be made on existing reactor systems such as the EBR-II in Idaho Falls, Idaho, the Fast Flux Test Facility in Washington and in-house research reactors at ORNL. These demonstrations will show how the most 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 viable demonstrable control system designs. These prototypic designs will be used as examples by ALMR designers in the DOE Programs.

4.2.1 Balance of plant control

The feedwater train 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 U.S. LWRs, incidents causing a significant fraction of lost plant availability can be attributed to the feedwater system. These LWR designs have analog control systems for the feedwater train. These analog systems are cumbersome, inflexible, unintelligent; they 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.

Although PID control is a proven strategy, 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. These multivariate strategies offer increased fault tolerance, increased robustness, and increased flexibility to accommodate changes in hardware or software. Putting these strategies into a digital control system also allows the use of smart sensors to improve fault tolerance and robustness. Research at ORNL in improved man-machine interfaces and artificial intelligence will lead to more efficient utilization of the operators. ORNL is incorporating research and development advances in these areas to demonstrate simpler, fault tolerant, robust, flexible designs for the feedwater systems of an Advanced LMR (PRISM). Although this demonstration is 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 was completed in late 1988[6]. In 1989, this work is continuing to include the other components making up the balance of plant.

4.2.2 Supervisory Control

The design for PRISM (and some other types of advanced reactors) incorporates multiple modules which together produce power to meet grid demand. All reactor cores are to be coordinated to meet the power demand. A chief virtue of multimodular plants is increased flexibility aimed at increased plant availability. If one reactor is shut down for refuelling, all others should be able to continue operation. This increased flexibility requires development and demonstration of an appropriate control strategy.

As process complexity grows, the advantages of advanced automated control increase. In a process where inability to maintain control has such high cost associated with it, as is the case with control of nuclear power plants, increase in complexity of control is particularly undesirable. One technique for combating complexity is the use of a hierarchical control structure, with each level of control supervising the controllers on the next lower tier of the hierarchy. This technique is proposed by GE for PRISM.

In 1988, ORNL demonstrated an example of such a hierarchical control strategy for an advanced multimodular LMR[7]. This work is described in another paper at this meeting. At the top level of control is a 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 plant supervisory controller by coordinating multiple reactor cores. This hierarchy will continue down to the level of component control. Any controller unable to fulfill the goal set by its supervisor communicates back up the hierarchy. The supervisor then tries to meet its goal by another method.

At appropriate levels, a nonlinear, multivariate, optimal controller strategy is used. The strategy has been developed as part of this program. The strategy transforms a two-point boundary-value problem, which must be solved off-line, into an initial value problem, which may be solved on-line. This strategy allows the controller to follow a demand in the presence of unknown variations of parameters and subsystem responses. A key feature of this algorithm is called parameter tracking. As a nuclear reactor goes through its normal range of operation, some of the plant parameters change. Also, over the life of a plant, the 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. Since supervisory control is required for PRISM, GE is reviewing the ORNL work and helping with planning for further development and demonstration efforts.

4.2.3 Automated 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. This work is described in more detail in another paper at this meeting.

The first task is to implement a computer graphics aide in the control room that assists the reactor operator. The joint ORNL/ANL work starts by 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.

ORNL will develop the start-up control strategy and algorithm. The algorithm should be based on the equipment available and implement the existing start-up control strategy. This will be a rather simple control philosophy, but a phase that is necessary in order to proceed with high confidence.

Next, ORNL will provide 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. The architecture of the control system will be based on the philosophy that a single failure of a sensor, failure of a controller, failure of a supervisory computer, or failure of a data bus will not require a reactor shutdown. GE participation in the planning of this demonstration assures maximum transferability of results to the PRISM design.

4.2.4 Future planned demonstrations

These and other demonstrations in following years will help transfer to the reactor industry the benefits of the latest proven advances in control systems strategy, control system and whole plant simulation, computer aided software engineering for control systems design, human-machine interaction modeling and analysis, and the other technologies being used within the program. These further demonstrations will include: 1) advanced control with maintenance planning; 2) fault-tolerant architectures; 3) control systems optimally designed to be easily understood by the human operator; and others as required.

4.3 Design Environment

The Advanced Controls Program will provide a centrally located, user friendly 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.

4.3.1 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 software consists of computer programs to organize the specification of requirements, to perform complex mathematical and logical simulations of the control design, and to illustrate the system through graphical and text manipulation software. The Controls Analysis Workstation will assist the control engineer in all aspects of the design process.

The advantages of the workstation will be

- Productivity enhancement through improved tools and design environment
- Error reduction
- Automatic record keeping
- Standardization of controls analysis methods
- Communications between design teams

The workstation will include a graphically-based software package that provides a means of assembling models of the power plant and its subsystems[8]. The resultant model will appear 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 workstation environment will advise the user on the use of appropriate control techniques and strategies, on the operation of particular plant components, and on the use of the control design workstation itself.

The designer can interact with the plant model and control system in either an on-line or an off-line mode, depending on the need. On-line interaction is when the plant is operating (perhaps in real time) and the designer can experiment to gain a feel for the behavior of the plant system. Off-line interaction provides for batch runs. For example, parametric runs can be performed to develop a family of performance curves for a particular subsystem.

4.3.2 Strategies for advanced control

The push for safe, reliable, and efficient operation, as well as for increased component lifetime, efficient maintenance, and improved human-machine interaction, places new duties and requirements on the plant control systems. These requirements take several forms: (1) tight control of continuous-variable type subsystems, (2) coordination of many interacting continuous-variable type plant subsystems, (3) control of discrete-event type subsystems, (4) decision-making for fault avoidance and mitigation, and (5) high-level decision-making for planning and coordinating all facets of plant operation and maintenance. Techniques of modern multivariate, optimal, and adaptive control are being examined for their potential benefits in actual reactor control and operations.

Adaptive control schemes allow the control system to adjust itself to variations in the internal parameters or conditions of the process being controlled. Adaptive control strategies often involve a model directly in the generation of the feedback signal. These controllers are structurally different from linear quadratic gaussian (LQG) controllers that use a model of the process to generate an estimate of the complete state vector.

The loop transfer recovery technique (LTR) technique extends the frequency response of the LQG controller and allows the designer to balance performance and robustness with respect to plant parameter variation. The LTR technique will be expanded to apply to nonlinear observers. Investigation of other techniques for enhancing robustness will be explored in subsequent years.

Automation of large-scale systems will necessarily require control and coordination of discontinuous-variable type systems. Traditionally, ladder-logic models and diagramming techniques have been employed to represent and perform this type of control. Other methods for organizing and diagramming the discrete event systems are emerging. These are State-Based Control Logic and Object-Based Control Logic. We are currently developing and using state techniques. The combination of state and object methods will yield a powerful design tool.

4.4 Human-machine integration R&D

The Advanced Controls Program at ORNL will provide an integrated environment that is supportive of the entire life cycle of a control system design. This life cycle spans activities from the preliminary design through final testing before installation, and will reflect acknowledgement of the human operator as an active system element.

For the short term, new analysis tools in the form of human performance expert systems and cognitive models of the reactor operator are being developed. These state-of-the-art tools will be utilized within analyses that currently ignore or make relatively gross assumptions about human performance. These applications will form the basis for an experience base that can be utilized in the long-term. The experience gained from application of the developed tools will be utilized to achieve a proven approach to higher levels of automation.

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, demonstrating a number of feasibility constructs including: a) the ability to link a network simulation model with a reactor plant process code, b)

the ability to have dynamic interaction between the two models, and c) the ability to link the network simulation model with a knowledge-based model created in an expert system modeling environment in order to promote diagnostic expertise for the simulated operator. Planned modeling activities include development, testing, and validation of a full-scale, single operator/single LMR module version of the model.

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.

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. 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.

4.5 Testing and validation of advanced control system designs by simulation

In the initial stages of the control system design and testing cycle, the

simulation of both the processes and the control systems can be combined in an integrated simulation, and not (necessarily) run in real time. Later in the design life cycle, however, the interfacing of separate process simulations and controller hardware will be required. Eventually, the integrated system would need to be run in real time to design and test the hardware and operator interfaces. In all cases, the designer should be assured of dealing with "verified" plant simulators. Hence 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.

Methods are being developed to ensure that the Advanced Controls Program software development conforms with industry standards (ANSI, IEEE, NRC Regulatory Guides, etc.) in order to both ensure high quality output and to make sure that the resulting controller designs are certifiable.

Simulator validation and verification work will be a continuing effort, and will depend on the availability of pertinent data and corroborating runs from independent codes. We expect to be able to use EBR-II data in support of the LMR simulations, as well as comparisons with DSNP, ARIES, and SASSYS code predictions.

Controller testing will be initiated along with the demonstration projects begun in 1988 and continued with further refinements and elaborations. Additional testing demonstrations will be accomplished with the proposed EBR-II automated startup activities. The possibilities for tying in prototype controller designs to full-scope training simulators have also been investigated for two specific LWR simulators which are available for R&D activities.

The generic design environment and testing capability will be based on the amalgamation of the workstation, advanced control design, and demonstration project activities, and will be tried and tested on many simulated and real-life projects in the interim.

4.6 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.

The software capabilities mentioned above demand that the underlying hardware handle several concurrent resource-intensive processes efficiently and reliably. Real-time operating system (RTOS) requirements for speed, reliability and adaptability will tax the capabilities of the systems available.

Standards and methodologies exist for guiding the development of computer software, including IEEE, ANSI, NRC and DoD-2167a. After a preliminary evaluation, some of these guidelines will be adopted or modified to produce a software development standard especially tailored for control systems.

Modern computer-aided software engineering (CASE) tools already exist which can provide quality assurance, enforcing standards as well as providing audit trails for managing changes in the systems and automatic generation of documents. Some of these tools have (at least) some ability to generate actual high-order language computer code (such as C or Ada) from structure analysis and design specifications. So-called fourth- and fifth-generation tools (4GL and 5GL) and application generators already remove much of the burden of "coding" from software developers.

5. DESCRIPTION OF ANL WORK

Automation using present and developing technology is much more than closed loop control. It involves the integration of computers and

associated software with the human operator. There is, therefore, an understandable concern about reliability. The issue of reliability is being addressed 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 involving simulation of total station blackout and loss of heat sink with failure to scram are well known. Less well known are the continued 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. The point of this work is that if the results of such events can be shown to be safe, then the concerns for controller reliability are much less and the new technology can be much more aggressively applied. The benefits gained are tied to operational considerations, such as more optimum control (tuning) of the plant and operation with fewer operators.

Where the reliability of computer hardware and software is an issue, such as their use in safety systems, more effective methods of verification of fault-tolerance are required. Because of the large size and complexity of most of these systems, the verification process must be automated. Such a system has been developed at ANL and is being applied to verification of the reliability and fault tolerance of a computer-based safety system intended for installation at EBR-II. The technique involves application of a new approach to modeling hardware and software so that it can be evaluated using an automated reasoner. The system checks to ensure that the original design specifications are indeed satisfied by the design or, if not, it indicates why.

An experiment currently underway at EBR-II involves a fiber optic link from the plant data-acquisition system to a CRAY computer at the INEL Super Computing Laboratory. Tests have been successfully conducted to demonstrate that a high fidelity simulation of plant dynamic response can

be maintained during the course of plant transients. Future work will involve a faster-than-real-time simulation to project the consequences of individual control actions.

5.1 Sensor validation

Validation of signals from sensors is critical for any advanced technology leading to automatic control. Several methods have been proposed and tested to provide 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. From that, a new estimated state is generated, and an ordered signal list is generated and displayed (called a signature plot) which shows the signals and their deviation from the expected ideal distribution of signals. In addition to the signature plot, an estimate is made of the value of each input signal based on the values of all the other signals and their relationships as calculated from the learned states and the observed state. 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 depends heavily on the analysis of variance. It 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. To

accomplish this, the test inspects the signals and mathematically predicts their mutual divergence. A limitation of the SPRT is that it does not guarantee that either signal represents a desired signal. The two signals, originally correct, could depart together from the true physical process value at some time point, and hence both become incorrect. 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. It is also very useful where it is desired to have another, diverse means to provide an important measurement. In the case of failed or failing instruments, the robustness of the analytic redundant approach can be shown to be high. 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 & diagnostics

It is now becoming known that one of the shortcomings of the nuclear industry is that there has been no model or paradigm for the presentation of plant data to the human operator. 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. This approach adheres to the paradigm of conservation of energy, as the production and utilization of energy is fully depicted. Additional "page-down" displays are created that adhere to the conservation of mass paradigm, thus covering the requirement that the operator know that there is a coolant inventory sufficient to remove the heat generated in the system.

To allow the development of advanced graphical displays, diagnostics, and other applications, it is necessary to have access to the real-time data in a convenient fashion. At EBR-II, the method used is to extract the plant information from the plant Data Acquisition System (DAS) computer at one-second intervals and provide the data to an ethernet. The ethernet is connected to file servers and "client" computers. The file server gathers data from the DAS, and redistributes to the client computers according to their requests. In this way, a very flexible system is available to develop and test new ideas/concepts.

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. As it is possible to provide separate pattern recognition systems in a hierarchical fashion, deduction of plant status from a high, supervisory level, down to the component level is possible based on instrumentation availability.

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

Networking technology is advancing rapidly for office automation. It is, however, moving a bit slower for real time applications such as process control. Much of the development of network hardware and software, however, has some application in real-time work. For example, fibre optics allows transmission of large amounts of data because of the high bandwidth, and the fact that a fibre optic network is not affected by electromagnetic fields is a definite advantage for process control. Networking is being examined as a means to accomplish distributed control for the next generation power plant and for backfitting existing plants.

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. The advantages of a networked approach include flexibility, cost, and operability.

An additional area of development taking advantage of distributed controllers is that of diagnostics. The ability to distribute diagnostic software in local controllers allows diagnostics to be used at the component and sometimes sensor levels; this would be almost impossible with a monolithic diagnostic approach. Work is progressing at EBR-II in this area.

5.4 Plant testing of passive safety features

To ensure that advanced control and diagnostic techniques do not obviate 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. A simple example to illustrate is the situation where a poorly designed power control system would attempt to increase reactivity to compensate for power reduction when the system was in a loss of pumps situation. This work has pointed out that a close interface with systems designers (in the case of new plants) is not only desirable, but mandatory.

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.

5.6 Faster than real time simulation

It has long been hypothesized that the use of real-time simulation, reset by real plant signals would be of value as a prognostic tool. Prediction of the plant state at some future time could help operators to determine the effect of control actions before deleterious events occurred. Faster than real-time simulation could, if successful, also provide a feedback to automatic control to modify the control commands in the event that the system would be put at risk.

A test has been conducted using real-time signals from the EBR-II plant fed to a CRAY supercomputer which ran a faster than real-time simulation of the EBR-II process.[19] A comparison, via an expert system, was made between the actual plant signals and the simulation. The tests were successful to the level anticipated. As better means are developed to "reset" the simulation based on new plant input, additional tests will be run and the predictive potential of faster than real-time simulation explored further.

6. DESCRIPTION OF RESULTS OF GE WORK

GE's PRISM plant concept was recently selected by the DOE as the basis for design of the Advanced Liquid Metal Reactor (ALMR) plant in the United States. It is a 1395 MWe power plant, made up of nine 155 MWe modules, organized into three power blocks of three modules, each power block supplying its own 465 MWe turbine/generator. The plant is proposed to be controlled by an advanced state-of-the-art control system especially designed to facilitate plant operation, optimize availability, and protect plant investment[20]. The control system will be distributed, hierarchical, and model based with extensive on-line diagnostics and operator aids. Sufficient automation will be built in to support a design goal of one operator running an entire power block under both normal and faulted conditions. All normal plant operations (such as startup, shutdown, load following, etc.) will be automated. The simplicity of the PRISM plant configuration (no control valves in the primary and secondary systems, constant speed feedwater pumps and intermediate pumps), and the inherently simple operability of the modules (large negative reactivity feedback built in, saturated steam cycle) will allow increased automation to be introduced at a reasonable cost.

Fundamental to the control philosophy of the PRISM design is the separation of the Plant Control System (PCS) from that of the Reactor Protection System (RPS). The RPS is a highly reliable Class 1E system which is implemented on a per module basis (no interaction of one module RPS action on any other module) and whose purpose is to automatically scram the reactor module whenever safety setpoints are exceeded. The RPS is cleanly separated from the PCS, as it uses separate sensors, electronics, and actuators. The RPS design is backed up by fundamental

physics, inherent to the module design, which will shut the reactor module down even if the RPS were to take no action. Thus, the RPS does not rely on the PCS to mitigate any event, and no fault in the PCS can prevent the RPS from performing its safety function. The PCS can be designed as an integrated, plant-wide control system and optimized for economic operation without being burdened by safety actions.

The PCS will be organized hierarchically, with local closed loop control on module systems (reactivity, primary and secondary pumping systems, steam generators) and power block systems (turbine/generator, feedwater, BOP), and with supervisory controllers at the module, power block, and plant levels. The figure illustrates this integrated network of computationally powerful controllers. Plant data highways will be designed to provide fault tolerant data handling and transmission.

Local, model based control of the PRISM design has been demonstrated on key lead systems at GE and ORNL[21]. One of the powerful features of this design is the ability to run on line validation and diagnostics. Early fault detection has been demonstrated on a limited basis in simulation. This is made possible by the fact that the controllers are not only running their assigned control algorithms, but also simulations of the processes being controlled. Comparisons of measured data to model predictions running in the controller allow the system to diagnose trouble in its process (leaks, stuck valves, etc.), and alert the operator before the situation deteriorates.

Development of the PRISM PCS and RPS designs calls for integration of the ideas and results of R&D work at the national labs with the design application experience of GE. Simulation and testing will play a key role in this effort. Initial concepts are being demonstrated in interactive design simulation. This kind of simulation is valuable in "proof of concept". As the project moves from the advanced conceptual stage, through design, and on to application, a variety of test beds are planned which will assure that the PCS and RPS will perform as expected. Cooperative efforts between GE, ORNL, and ANL will make this possible. Key feature demonstrations of "PRISM type" PCS and RPS controllers are being planned at EBR-II. Concepts for real time simulation with ports to support interfacing with prototype local and supervisory controllers are

being evaluated at ORNL. This type of simulation will be used in staging prior to application. These activities will culminate in the construction and certification testing of a full scale PRISM reactor module with its PCS and RPS.

7. RELATIONSHIP TO COMMERCIAL INDUSTRY

The commercial 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 discussing with DOE and ORNL 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. As new techniques are developed, they are tested under simulation with prerecorded plant data from EBR-II, and then 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 may impact the LWR community as well.

The nuclear industry stands to reap enormous benefits in power plant

availability and reliability from the incorporation of automated control technology. Futhermore, by eliminating most of the contributing causes to the world's reactor accidents and frequent operational upsets, these advanced, automated techniques could also help restore public confidence in the nuclear option. To realize these potential benefits, an intelligent research and development plan and an up-front investment in tools, methods, and supporting staff is required. This investment will be extremely cost effective in performance improvement and in the nth unit cost of control systems for future reactors.

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", Proceedings: 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", Proceedings: EPRI NP-4769-SR, September, 1986.

[4] GAYDOS, K. A., et al, "An Optimal Control Strategy in the Design of a PWR Feedwater Controller", Proceedings: 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", Proceedings: 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", 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, Vol. 1 pp. 35.01-35.16 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, Vol. 2, Knoxville, May 1989, pp. 67.01-67.09.
[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," 7th DASC Digital Avionics Conference, Oct 13-16, 1986, Fort Worth-EEE, AIAA.
[19] LARSON, H. A., DEAN, E. M., LEHTO, W. K., "Faster Than Real-Time Simulation for Plant Control", (ibid #7) Vol. 1 pp. 34.01-34.10,
[20] DAYAL, Y., "Advanced PRISM Plant Control System", Proceedings, 7th Power Plant Dynamics Control and Testing Symposium, May 15-17, 1989, University of Tennessee and IEEE Control Systems.
[21] WILSON, T. L., and WAGNER, W. K., "Multivariable Control for the PRISM", Proceedings, 7th Power Plant Dynamics Control and Testing Symposium, May 15-17, 1989, University of Tennessee and IEEE Control Systems.

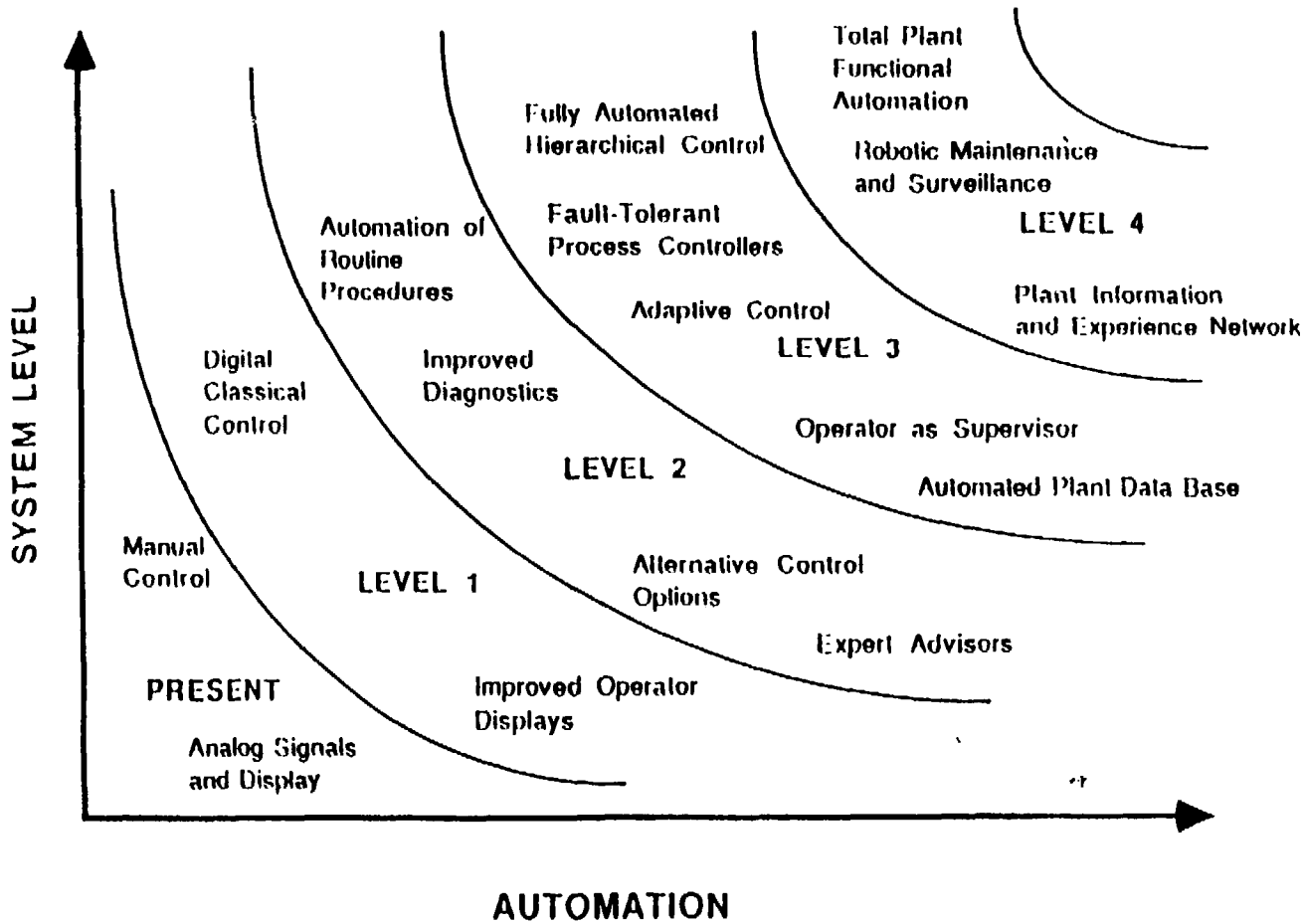

Fig. 1 Evolution of automation in nuclear power plants

PRISM HIERARCHICAL CONTROL AND PLANT INTERFACES