CONF-890555--6

CONF-890555--6

DE89 008918

# APPROACH TO PLANT AUTOMATION WITH EVOLVING TECHNOLOGY*

J. D. White

Oak Ridge National Laboratory
Oak Ridge, Tennessee 37831-6010

Presented at

7th Power Plant Dynamics, Control, and Testing Symposium

Knoxville, Tennessee, May 15 - 17, 1989



---

*Research sponsored by the Office of Technology Support Programs, U.S. Department of Energy, under contract DE-AC05-84OR21400 for Martin Marietta Energy Systems, Inc.

# APPROACH TO PLANT AUTOMATION WITH EVOLVING TECHNOLOGY

James D. White
Oak Ridge National Laboratory
Oak Ridge, TN 37831-6009

## ABSTRACT

The U.S. Department of Energy has provided support to Oak Ridge National Laboratory in order to pursue research leading to advanced, automated control of new innovative liquid-metal-cooled nuclear power plants. The purpose of this effort is to conduct research that will help to ensure improved operability, reliability, and safety for advanced LMRs. The plan adopted to achieve these program goals in an efficient and timely manner consists of utilizing, and advancing where required, state-of-the-art controls technology through close interaction with other national laboratories, universities, industry and utilities. A broad range of applications for the control systems strategies and the design environment developed in the course of this program is likely. A natural evolution of automated control in nuclear power plants is envisioned by ORNL to be a phased transition from today's situation of some analog control at the subsystem level with significant operator interaction to the future capability for completely automated digital control with operator supervision. The technical accomplishments provided by this program will assist the industry to accelerate this transition and provide greater economy and safety. The development of this transition to advanced, automated control system designs is expected to have extensive benefits in reduced operating costs, fewer outages, enhanced safety, improved licensability, and improved public acceptance for commercial nuclear power plants.

## BACKGROUND

In 1985, the U.S. Department of Energy (DOE) established a task team to determine the need for, assess the feasibility of, and recommend an approach to the introduction of automation and advanced control into the nuclear power industry. The task team report[1], published in September 1985, recommended an Advanced Controls program with a centralized, multi-user capability. As a result of this task team report, the DOE has provided support to Oak Ridge National Laboratory (ORNL) to pursue research leading to advanced, automated control of new, innovative liquid metal reactor power plants (LMRs). The goal is to provide a national center of excellence in research, development, and testing of nuclear control systems employing the latest advances in automation, artificial intelligence, expert systems, hierarchical computer architectures, and optimal control. The Advanced Controls program established at ORNL will provide an integrated environment to support the rapid and confident design and testing of advanced control systems providing improved operability, reliability and safety for advanced LMRs.

Advanced, automated control systems will exploit the versatility of digital signal processing, analysis, and communication. These systems will accomplish in an orderly, comprehensive way all of the routine activities of an experienced human operator. In addition, sophisticated diagnostics will alert the operator as to plant status and any special actions which the operator should take. Automated control systems can perform most functions more rapidly, manage more complex systems, and consider more aspects of the situation in a shorter time interval than can a human operator without the aid of automation. The traditional role of the "hands-on" operator will be elevated by the use of automated systems to that of supervisor, planner, and strategist. Using techniques of artificial intelligence, automated systems will learn from operational experience and from the operator.

The automated control system can incorporate systematically the consideration of 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, centralized 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.

Although U.S. nuclear power plants currently exhibit some automation at the individual or subsystem level, automated 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. Examination of the operating experience of U.S. light water reactor plants (LWRs) since 1976 reveals a low average availability of only approximately 58%.[2] Advanced, automated control systems have the potential for improving plant availability and reducing operator error.

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 should also employ automation in plant operation, control systems, maintenance, and construction to compete with domestic alternative power sources and foreign nuclear plant designs. The advantages of automated plant control systems include reduced staff manpower requirements, elimination of routine operator tasks, minimization of human errors in operating plants and their consequences, improvement of plant availability, ability to manage multimodular plants, reduction of challenges to plant protection systems and to inherent safety features, and reduced risk to plant investment. These benefits, however, may be realized only if an intelligent plan of phased automation is pursued. Included in an automation plan should be consideration of the integration of all control system elements (hardware, software, human).

## BENEFITS OF AUTOMATION

The major areas of benefit predicted from the use of advanced control systems are (1) enhanced safety, (2) increased reliability and availability, and (3) reducted operating staff, (4) increased competitiveness, and (5) improved human-machine interface. Each of these benefits contribute to improved economics for the advanced reactor concepts employing the advanced controls technology.

Safety

The use of fault-tolerant automation can reduce the probability of a major accident through its impact on operator performance and through its ability to keep complex operating systems within a prescribed operating envelope. Assuming, for example, such probability is reduced from $10^{-4}$ to $10^{-5}$,[ref. 3] the direct benefit in plant investment and protection alone is at least $36 million per plant per year, (assuming $1 million per day cost for replacement power cost), or a total potential benefit in the order of $3.6 billion/year if 100 nuclear units were eventually automated. Although these predictions are for LWRs, the argument is applicable to advanced reactors also.

Reliability & Availability

Analog subsystem controllers, which constitute 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. 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 architecture 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.

While these subsystem improvements are possible, the development work to accomplish them is still in beginning stages, and much remains to be done. EPRI sponsored demonstration developments of selected subsystems in operating plants [the Monticello BWR-3 owned by Northern States Power and the Sequoyah plant owned by the Tennessee Valley Authority]. Planned availability improvements from the feedwater control system retrofits can save $500,000 per plant per year.[4-7] Manufacturers are developing product lines of digital instruments and controllers intended both for new plants and to replace 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. Improvements in sensor and support system performance are required to make the best use of improved digital techniques.

In the years 1982-1986, the average availability for all U.S. plants (very little automation) was about 63%.[8] The lifetime average availability of the highly automated CANDU plants is approximately 84%.[9]. Clearly, a 21% increase in availability of U.S. plants would be extremely beneficial to the nation.

Reduction in Operating Staff

Previous 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, or a total benefit on the order of $400 million/year if the benefits were eventually applied across 100 or so nuclear units.[10]

Competitiveness

Dual computer control systems are used for direct digital control of reactivity and other major process parameters in 27 full-size commercial CANDU nuclear units, 16 of which are in service. CANDU performance has been excellent, achieving over 84% availability, due in part to automation. Furthermore, planning studies indicate that the use of a distributed control approach to replace most of the control signal wiring and relay logic results in a large reduction of the construction work to be done on site. The planned construction schedule is shortened by 6 to 10 months for the new CANDU 300.[11-13] The Japanese have apparently taken the lead in the design of high-level hierarchical control systems. They have completed the design of a plant-wide, hierarchical, fault tolerant, distributed microprocessor control system and have validated the design on a simulator. The design is being implemented in ten new plants scheduled to become operational in the early 1990s.[14,15] To remain competitive in the worldwide market for advanced nuclear units, the U.S. must develop advanced, automated systems as well.

Human-Machine Interface

In 1980, NRC sponsored a project to examine the direct and deliberate allocation of functions between man and machine in the designs of nuclear facilities in the U.S. and to propose a methodology for its resolution. One of the results was a rule-based, iterative procedure based on a hypothetical-deductive model. In operational form, the model provided a practical, step-by-step, reproducible method by which allocations can be made.[16,17] Although no follow-on development or application of the method has been reported, more nearly automated plants will demand a deliberate approach to the allocation of functions. Such demands require that predictive models of the cognitive activities and performance of the human operator be developed for detailed evaluation of operator roles and candidate allocation configurations. In particular, knowledge-intensive operator models can be used to help define efficient and effective symbiotic interfaces between the operator and safety-related controls and protection systems.

Fault-tolerant designs of microprocessor systems promise to provide essential hardware reliability. Continuing development is needed to ensure cost-effective designs and to provide operating systems and software techniques compatible with the hardware designs. More highly automated plants will further separate the human operator from interaction with individual processes, therefore, built-in and automatic fault diagnosis and recovery techniques are needed so that maintenance can be performed and functions restored rapidly.

## PLANT AUTOMATION WITH EVOLVING TECHNOLOGY

The transition from today's nuclear control systems with some analog control at the subsystem level and significant operator integration to the future designs for complete automation under human supervision is envisioned to occur in phases. The transition may be described in terms of 4 levels as shown in Figure 1. Level 1 includes automated data management at a plant. This is actually occurring to a limited extent now in U.S. LWRs and is planned for U.S. LMRs. Also in this level will be some replacement of today's analog controllers with more reliable digital controllers performing basic proportional-integral-differential (PID) control. As mentioned previously, EPRI is already sponsoring some of this work at existing LWR sites.

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.

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 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. The Advanced LMR concept being studied fits within this phase.

Level 4 is total automation of the plant, an intelligent control system aware of all operational status and in interactive communication with the operator to keep him apprised concerning 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 an integral part of 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.

## R&D ISSUES WHICH NEED TO BE RESOLVED

Many of these benefits of automation, however, will not be available without well-planned R&D. There are several questions yet to be answered. How much automation is appropriate in the next and later phases? The answer to this question is dependent upon what advanced technologies will be deemed to be proven and acceptable by the industry and the regulatory bodies, which in turn depends on successfully demonstrating advanced control concepts through simulation and testing. Companion questions deal with determining the kinds of control strategies that are best for each system and which mathematical algorithms offer the best performance, reliablity, and flexibility. In addition, the appropriate role of the operator in relation to automated plant or component control under a variety of operating conditions must be addressed.

How to improve the relationship between man and reactor power plants is an important question even today for LWRs. This is being addressed by EPRI in the ALWR requirements document development efforts. Basic questions here are: How much automation is desirable? How many operators are needed? What are their responsibilities? How can lessons learned be accommodated?

Several tasks need to be completed to ensure that advanced reactors are designed to meet their objectives of high availability and improved operability. In order to meet this need and address the R&D questions raised concerning automation and the application of advanced control concepts in nuclear power systems, the Advanced Controls program at ORNL has initiated several projects that cover many issues raised about this emerging technology. Some of these tasks are listed below:

- Evaluation of control strategies and algorithms to meet the requirements of advanced systems;
- Demonstrations of prototype advanced digital control systems for nuclear plants including fault tolerant hierarchical distributed architectures with signal validation and smart sensors;
- Establishment of a suite of methodologies, tools and guidelines including rapid simulation capabilities, varied plant models, and man-machine models and interfaces; and
- Formulation of methods for development, verification and validation of software and for testing and validation of control designs.

It is the goal of ORNL that advances in these areas will provide an impetus for acceleration of the transition by the nuclear industry to advanced controls automation described above.

## ADVANCED CONTROLS PROGRAM

Oak Ridge National Laboratory plans to integrate emerging technologies in control theory, software engineering methodologies, very high level languages, advanced computer architectures, artificial intelligence, man-machine modeling, and plant-wide design database management into an environment in which a control systems designer can quickly develop and test control strategies and models. Collaboration with other national DOE LMR program participants will assure an integrated balance in control system design and analysis for advanced reactor concepts.

The Advanced Controls Program will conduct research to support the evolution of controls technology, provide a test bed for technology development, establish a real-time, engineering simulation capability for test and validation of software and equipment, and lead the development of appropriate industrial standards for automation of nuclear power systems. Progress of work by the team members toward the common goal will be shown during the program through demonstration projects. For some demonstrations, models and other software developed by program participants will be assembled to demonstrate tasks of increasing complexity as the program progresses. To the extent possible, the technology developments will be demonstrated in DOE reactors, including the Experimental Breeder Reactor-II in Idaho, the Fast Flux Test Facility in Washington and in-house reactors at ORNL, as appropriate.

To achieve a valid, accepted automated control system, the control system design process must start early in the plant design activity and follow through the final detailed design phase. The control system designer must be provided with the tools, models, facilities, and resources to successfully complete the entire design process. This process starts with (a) plant concepts, requirements, and constraints; (b) a control system concept and approach; and (c) considerations of the human interface requirements. It then proceeds through an iterative process of design, simulation, and validation to produce a final control system design and the validated, error-free software that will be installed in the plant automation equipment.

The support needed by the designer can be grouped into separate but interrelated "environments," each of which includes appropriate tools (software programs), information (data bases), models (mathematical descriptions), and facilities (computers, test environments). Lacking these fully developed, coordinated, and integrated environments, it would require an investment by each plant designer of $200 million to produce the estimated 2 million lines of software needed for a fully automated nuclear plant control system at today's rates of approximately $100/line of software (Current generation boiling water reactors (BWRs) use 1.3 to 1.4 million lines of code in computers associated with the control room alone)[18]. With the environments that the Advanced Controls Program will provide to the plant designer, the cost and time to complete the design will be reduced significantly. For example, the use of computer aided software engineering tools alone is predicted to reduce software generation cost by factors of two to twenty.[19]

To support the transition towards advanced automated control of nuclear plants, this program will conduct four major kinds of activities:

Demonstrations of advanced control system design;

Establishment of an integrated user-friendly design environment;

Testing and validation of advanced control system designs; and

Guidance in control software and hardware specifications.

These activities are discussed in more detail in the remainder of this paper.

<u>Demonstrations of Advanced Automated Control System Designs</u>

The purpose of this group of activities is to provide timely demonstrations of prototypic designs for control systems for selected aspects of the Advanced LMR concept. These demonstrations will be designed to show how state-of-the-art research can be used to help accelerate the transition to fully automated control. 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 controllers. Where possible, later demonstrations will be made on existing DOE reactor systems. These demonstrations will show how the most appropriate state-of-the-art developments in advanced control technology can be integrated into viable control system designs. These prototypic designs will be used as examples by Advanced LMR designers in the DOE Programs. These demonstrated designs will be a reasonable advance in the Evolution of Automation diagram shown in Figure 1.

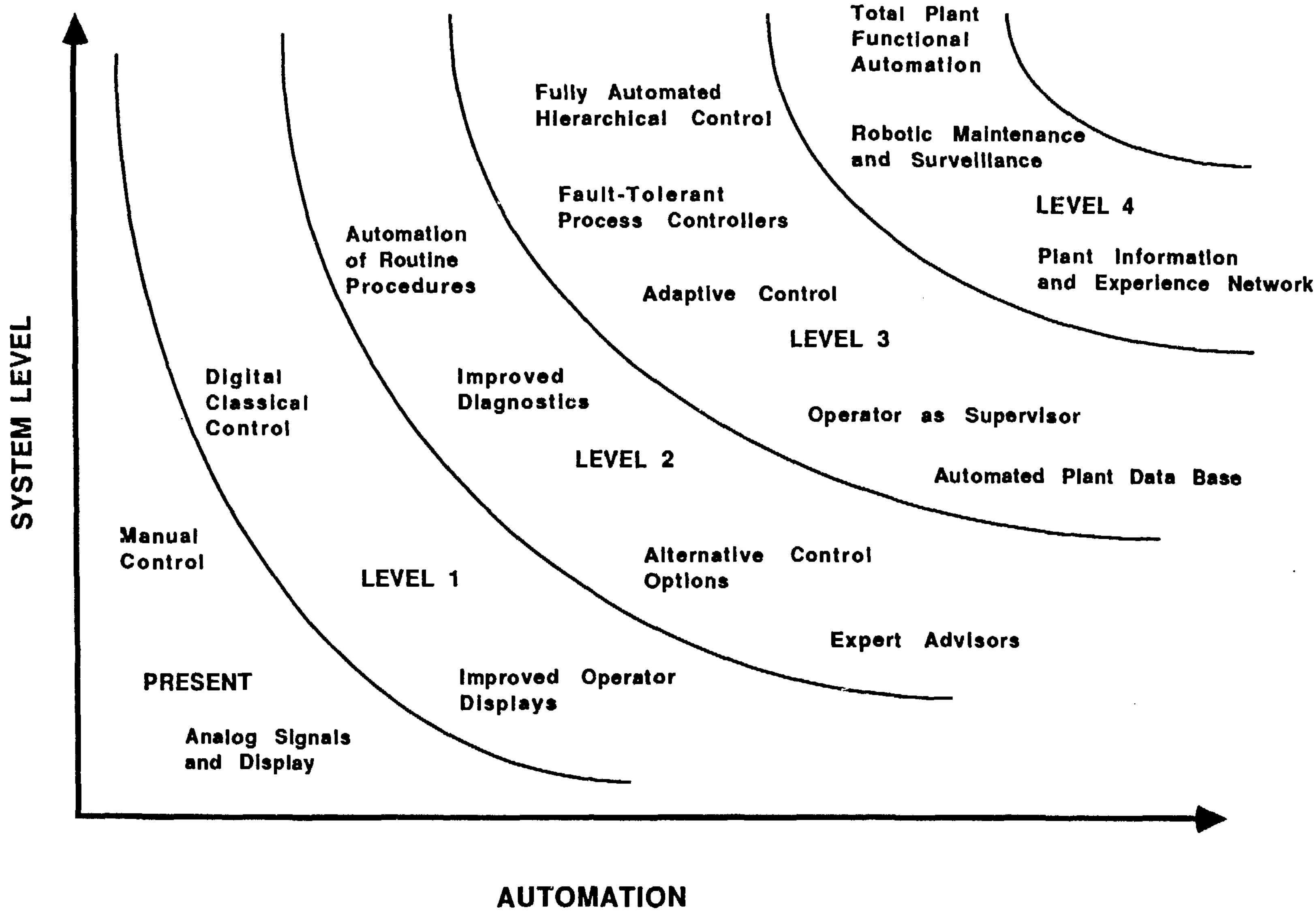


Fig. 1 Evolution of automation in nuclear power plants

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 (in some designs more than one), 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 already 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 proportional-integral-differential (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 better strategies offer control of several parameters at the same time 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. Furthermore, research at ORNL in improved man-machine interfaces and artificial intelligence will lead to more efficient utilization of the operators. ORNL will incorporate research and development advances in these areas to demonstrate simpler, fault tolerant, robust, flexible designs for the feedwater systems of an Advanced LMR. 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, like MHTGR and LWRs.

A first demonstration prototype was completed in late 1988. This completed work is described in another paper in this Symposium[20]. A model of a prototypical feedwater system was built and special features were added to simulate sensor noise, component failures, etc. Smart sensor algorithms were developed and demonstrated for processing raw sensor data samples and generating validated data. The algorithms are able to identify a failed sensor and lock it out of the control system. The operator interface to this system notifies the operator of the failure and the test results on which the failure was detected. The Smart Sensor standard modules will be applied to measured (simulated in the demonstration) variables in the feedwater system. The control system are able to operate with any single failure in the plant instrumentation. For this demonstration, Smart Sensor standard modules were be developed for liquid level, flow, temperature and pressure measurements.

In this demonstration project, ORNL designed continuous closed loop control algorithms for the feedwater plant using classical and modern design tools in Matrix-x. An advanced digital closed loop controller was developed that is multivariate optimal. The 1988 demonstration was of a controller using a state estimator and linear-quadratic-Gaussian (LQG) compensator with a Loop Transfer Recovery (LTR) technique. The control loops for the feedwater plant include the level controls for the feedwater heaters, steam generator, condenser, and deaerator and flow controls for pump recirculation valves. A Performance Monitor monitors plant readings and trends in readings to identify failures and deteriorating performance in components of the feedwater plant pumps, valves, and heat exchangers. An Expert Advisor analyzes the information and supplies to the operator the most likely causes for anomalies, advise proper corrective actions, and provide information about the feedwater system status. This capability provides the operator with the kind of assistance that an expert on the component might give on continued operation of a slowly degrading component or the operational alternatives that might allow continued operation with a particular component out of service. A Mode Selector recognizes changes in mode in the plant and carries out discrete actions or sequences of actions that are required to stabilize the plant after a change of mode. The User Interface displays the results of the demonstration on interactive screens.

In 1989, this work is continuing to include the other components making up the balance of plant.

Supervisory Control

Some designs for advanced LMRs (and other types of reactors) incorporate multiple modules which together produce power to meet grid demand. Some designs carry the idea further to have multiple reactor cores in each module. In such designs 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. 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. In 1988, ORNL demonstrated an example of such a hierarchical control strategy for an advanced multimodular LMR[21]. At the top level of control is a supervisory controller which determines how grid demand will be met, if possible, by the modules. The level of control under the plant supervisory controller will consist of module controllers. Each module controller will try to meet the power demand of the plant supervisory controller by coordinating multiple reactor cores and a single turbine generator. This hierarchy will continue to the level of component control. Any controller unable to fulfill the goal set by its supervisor will communicate back up the hierarchy. The supervisor will then try to meet its goal by another method. At the subsystem appropriate level, a nonlinear, multivariate, optimal controller strategy is used. The strategy used has been 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. 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, the parameters change over the life of a plant. The nonlinear control strategy developed has the ability to track changing parameters and continue to optimally control the reactor or reactors.

The demonstration completed in 1988 involved primarily a mathematical treatment of hierarchical control. Control systems of the future should be able to communicate goals in forms other than numerical values. Future demonstrations based on inclusion of non-numeric information in the control system will be done.

Another area of research that will be pursued over the next few years is control of uncertain nonlinear systems. A recurring problem of simulation and control is the inability to model the system to the lowest detail. The more detailed the model is, the slower the simulation. Furthermore, the control algorithms are based on mathematical descriptions of the plant dynamics which are often approximate and which may not describe the behavior of a plant undergoing changes during an operating transient. It is possible with some advanced control strategies to control some processes although the model that is being used is not complete. In the 1989 demonstration, models developed for the 1988 demonstration will be used along with less sophisticated models to demonstrate this capability.

Automated Start-Up

The scope of this work at ORNL is to develop control system philosophies control strategies software programs, control, and for automated start-up of advanced reactors. In a collaborative effort, Argonne National Laboratory/Experimental Breeder Reactor-II (ANL/EBR-II) will provide the necessary reactor facility for demonstrating the advanced control and diagnostics concepts where practical.

There are several areas in which work must be accomplished to fully implement a totally computer controlled start-up philosophy on EBR-II. The first task is to implement a computer graphics aide in the control room that requires the reactor operator to be an integral part of the control loop with the computer. The collaborative 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 much needed service to the operator.

This work entails the conversion of the start-up procedure with its manual checksheets into computer prompts to the operator and the automatic verification of plant signal values used during start-up. Reactor start-up will be performed by manual control actions with the aide of the computer prompts for each step. The computer will perform the data reduction and plotting now performed by the operator during approach to critical. It will issue prompts for hold points while the operator reviews data, takes manual data or makes decisions to proceed.

ORNL will develop the initial 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 other algorithms and software to perform advanced optimal start-up control. ANL will provide the necessary engineering and manpower to get the new required 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.

ORNL and ANL will work closely on the computer displays for the reactor operator during all phases of the work. The displays should provide the operator with required information in a format that is easy to understand and that is consistent from screen to screen. Diagnostics and sensor validation should eventually be incorporated into the computer software and into the displays.

Planned Demonstrations in other areas

These and other demonstrations in following years will help transfer to the reactor industry the benefits of the latest proven advances in control systems technology strategy. These further demonstrations will include: 1) advanced control with maintenance planning; 2) fault tolerant architectures; 3) control systems transparent to the human operator; and others as required.

The information processing and monitoring capabilities of the control system in the advanced reactor designs suggest expanding the role of the control system to include maintenance activities. A planned Maintenance Database and Expert Advisor demonstration project will illustrate what can be done with a central computer system to automate the information handling in nuclear power plant maintenance. Some of the main features which are planned for the demonstration project are:

- Computerized maintenance procedures - tag-outs (necessary for plant safety for the highly automated plant), work order preparation, testing procedures, all tied together in a integrated, computerized database package.
- Preventive/predictive maintenance - Schedules for preventive maintenance based on the health of the component as monitored by the Performance Monitor function of the control system.
- Service and repair records for the operating and engineering staff purposes. The records of failure and repair automatically recorded in the computerized maintenance procedures can be formatted so that operations and engineering can readily search the maintenance data for their respective information needs.
- Tie-in to national database of failure and servicing data. Some national databases for component failure data already exist for liquid metal reactors. The purpose of this task is to design interfaces in the Maintenance Database to share information with a national network.

A planned fault tolerant control system demonstration project will investigate architectures for the communications networks and digital processing units, and algorithms such as the component "heart beat" to detect and reconfigure for hardware failures. The study will use PRA methodologies to compare different strategies and will establish acceptable limits for mean-time-to-failure for the control system. To detect software failures, the possibilities for independent algorithms to verify the control system outputs will be investigated. (Example: A LQG/LTR controller might be compared to a simple PID.) A secondary algorithm to validate a control system output is a relatively new concept.

Another planned demonstration project will provide an example of a control system design that is transparent to the human operator. Frequently, the human operators in a nuclear plant have to manually integrate the control of various subsystems which are under analog control. These analog controllers are hard-wired and, except for failures or degradations in performance of components, do not change. In advanced digital control systems, however, the controllers will have software options and adaptive features to provide robustness, fault tolerance, and flexibility. A logical concern, then, is that the operators would be even more unaware of the future plant actions and conditions than they are now in existing LWRs. For example, a temperature sensor in the plant may fail resulting in the control system switching to a redundant measurement or a calculated temperature. If the operator is not aware of this change, he may inadvertently make a poor decision during some upset condition. As another example, the control logic could require a rebalancing of the coefficients in an adaptive optimal algorithm under certain operating conditions - as designed. (In a multimodular plant, burnup in one or more reactors may need to be accelerated relative to others). If the operators are unaware of this change, they may find themselves in a position of fighting the control logic without realizing it. Research at ORNL will be performed to investigate how to keep the operators informed about not only the current state of the plant, but also what the control system is trying to do and the probable future results of the control system actions. An operator interface to the control system will be designed to inform the operator about: the validity and faulted state of each of the sensor signals interrogated by the data acquisition system; the purpose and the relative weights of the objectives of each of the controllers; the faulted state and backup of any failed controllers; and the expected state of the system as a function of time.

Man-machine interface models and human cognitive models will be used to determine how much information concerning plant status and control system actions the operators will be able to utilize. The amount and type of information needed by the operators will be dependent upon whether the plant is in start-up, load-following, upset, shut-down, or other conditions. Research using interactive simulation with man-machine models and Advanced LMR models will determine how information needs will change with plant conditions.

## Design Environment

The 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. There will be a central physical location for this environment at ORNL with electronic linkage to other participating universities and institutions. All information will be in electronic form for easy accessibility. ORNL professional staff members also will be available to assist in the transfer of technology to the users.

## Intelligent Controls Analysis and Design Workstations Environment

The Advanced Controls Program is developing a controls analysis workstation environment for efficient engineering of control systems, especially for advanced power reactors such as modular liquid-metal reactors. The concept of a workstation is one of 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 push for safe, reliable, and efficient operation, as well as increased component lifetime, efficient maintenance, and improved human-machine interaction, forces the development of intelligent control systems, which of necessity, requires high-level decision-making capability and the coordinating capability to integrate all facets of plant operation and maintenance. The engineering of such intelligent control systems requires an improved tool set and environment.

The controls analysis workstation environment will be used to automate, document, and test all aspects of the design, analysis, and specification. The advantages of the workstation will be

- Productivity Enhancement through Improved Tools and Design Environment Error Reduction
- Project Management
- Automatic Record Keeping
- Standardization of Controls Analysis Methods
- Communications between Design Teams

These phases of control system development will require the control workstation to support all of the Advanced Controls Program analysis and design activities. Three areas related to control system design are considered in this project: (1) design methods for control systems, (2) computer programs to increase productivity of designers and analysts, and (3) computer hardware to support the design and analysis software. Improved design methods are needed to reduce engineering effort and simultaneously decrease errors. Such methods will be usable with software-based development tools, data-bases, and computer workstations. In addition to simplifying the effort to functionally specify the control system, the method must also document the specification so that computer programs can be written to implement the specification on real-time process computers.

Software packages are needed to perform mathematical and logical analyses, design trade-off and selection, simulation, database management, report generation and graphical representation, and inter-team communications. Commercial software packages are available that fulfill some of these needs. However, many are not integrated (i.e., one company's package cannot call on another for data, to invoke a function, or to effect coordination towards a common goal). Computer hardware and peripheral equipment are needed to execute the software tools indicated above. The hardware must run at sufficient throughput so as not to hinder the design effort and meet specific compatibility requirements.

The workstation will include a graphically-based software package that provides a means of assembling models of the power plant and its subsystems. 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. A prototype demonstration of this capability was completed in 1988 and is reported in another paper at this symposium.[22]

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 control design workstation will be developed as an integrated group of modules, the:

Control System Analysis Package. This software package will provide analysis tools for the development of modern (state-space) linear and non-linear control systems. The package will have many self-contained general and specific equation solvers. In addition, it can make reference to other commercial packages for continuous and discrete-control tools.

Control System Database. This software package will provide a centralized repository for all information relevant to those control system methods supported by the analysis package. Categories include: (1) control system design data from vendors, (2) logbooks for users of the workstation, (3) input/output files of analysis software, (4) help file and documentation for analysis software, and (5) current bibliography related to control system methods supported by the analysis package.

Interactive Simulation Package. This software package will provide a user-friendly modeling environment for testing control systems at various stages during the development cycle. Some of its features will include:
(1) Interactive. The package will allow for instant feedback on changes made to the system (either model or control). This encourages experimentation and shortens development time. It also provides an excellent means of demonstrating control concepts to others outside the controls development portion of the project.
(2) Hierarchical. The package will allow detailed and course-grained models of the plant to mixed and interchanged as required to obtain simulation speed and performance.
(3) Graphical Interface. The package will provide a graphically-based display of the plant, control system, operating conditions and variables, and other parameters and features as required. The premise is that most engineers and analysts are visually-oriented. The display is hierarchically-based so that as a user needs to see more information he may proceed into deeper layers of the system.

Plant Model Database. This software package will provide a centralized repository for all information relevant to plant modeling work. For example, specific design information (e.g., PRISM, SAFR) may be made available. Also output from simulation runs can be filed for later analysis by other users.

## Strategies for Advanced Control

The push for safe, reliable, and efficient operation, as well as 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 control (which include multivariate, optimal, model algorithmic, hierarchical coordination, disturbance accommodating, discrete event, operations planning, and system-wide automation) are being examined for their potential benefits in actual reactor control and operations.[23]

Continuous Control Strategies

Modern multivariate, optimal, and adaptive control techniques are relatively new to nuclear power reactor design. Their advantages and disadvantages are now being explored as a part of this program. One area being investigated is adaptive control. 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.

Strategies for Inherent Robustness

The loop transfer recover technique (LTR) 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.

Discrete-Event Control

Automation of large-scale systems will necessarily require control and coordination of discontinuous-variable type systems. These are systems distinguished by the discrete nature of their outputs or internal states. Examples of discrete-event systems are those which are either off or on or those which take on specific modes of operation such as startup, run, and shutdown. Control of discrete-event systems is notably different than continuous-variable type systems. Traditionally, ladder-logic models and diagramming techniques have been employed to represent and perform this type of control. However, this technique has limitations: there exists no inherent sense of the plant's state, understandability of the ladder diagram by newcomers is difficult, and flexibility of the technique for future additions and modifications is limited. 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 for discrete event control. The combination of state and object methods will yield a more powerful tool than we presently have. This will be pursued in subsequent years.

<u>Decision-Making for Degraded Conditions</u>

The modes and effects of equipment failure must be considered in the design of control systems. Current practice is to rely substantially on the plant operator's diagnostic and decision-making capability to mitigate degraded conditions. Human decision-making can be improved by providing refined, pertinent information. Additionally, many decisions can be entrusted to the computer-based control system. A distributed, intelligent control system would have capability for decision-making allocated from the lowest-level controllers to the highest level of supervisory control.

There are several strategies for improving decision-making when equipment are malfunctioning or conditions are off-normal. One of these is the plant-state projection. A faster-than-real-time simulator is used to estimate the future state (status) of the plant based on current conditions and planned control actions. This will be explored in subsequent years.

Another control strategy under development by the program involves the treatment of the interaction between the rest of the plant and failed subsystems (and components) as unknown perturbations to a reduced model of the system dynamics using nonlinear control techniques. The incorporation of these techniques into the supervisory controller will permit control of critical plant systems under degraded conditions. This work will be shown in a supervisory control demonstration.

Distributed Intelligent Control

The integration of discrete event controllers and continuous controllers under the supervision of an optimal schedule planner is going to be a major task. One necessity will be the proper distribution of intelligence throughout the elements of the control system - from sensors and controllers to operator monitoring/control consoles. An integrated scheme will be developed that achieves a distribution of intelligence for normal steady-state and dynamic plant operation and degraded plant conditions.

**Advanced Controls Human-Machine Integration R&D**

To a considerable degree, the design of reactor systems in the past has been viewed (and carried out) primarily as a "hardware design" problem. From this traditional viewpoint, a control system is essentially instrumentation and control hardware, and its design is effectively an instrumentation and control engineer's problem. Similarly, elements such as software, staff and support facilities tend to be considered as ancillary system elements that will be addressed by someone else. This approach depends on the assumption that input from other disciplines can be obtained, when needed, from specialists in those areas. In effect, designers in different disciplines traditionally tend to be "compartmentalized" and have relatively limited interaction/communication until there is a need, much later in the overall design process, to merge all of the independent efforts into a final design. The Advanced Controls Program at ORNL, in contrast, will provide an integrated environment that is supportive of the entire life cycle of a control system design.[24] 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 good approach to higher levels of automation.

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. Specific program details are provided below.

Preliminary Design Phase. During this phase of the life-cycle, control system designers have relatively high-level notions or design philosophies related to an envisioned control system. Expert, high-level advice to designers will aid their formulation of feasible objectives, performance specifications, and functions. Specific cognitive engineering support will be in the form of expert high-level cognitive engineering design guidelines. These will be provided through an expert system developed for this purpose. Such a tool will aid in the specification of system design objectives, system performance specifications and functional identifications that specifically consider the role of the operator in the system design.

Design Phase. During this phase of the life-cycle, the functional descriptions of the system are elaborated into a set of potentially feasible design alternatives. In general, the design alternatives will include various means of achieving the overall objectives of the system. This may include various types of hardware, software, interfaces, and levels of automation (allocation of function). During the design phase, a number of alternative designs may be generated, and each will be tested and evaluated with respect to the quality with which they meet overall system objectives. It is an iterative process that will eventually lead to a first approximation to a well-engineered control system.

Multi-disciplinary efforts must be integrated in order to allow feasible design alternatives to be subjected to simultaneous constraint evaluation. The cognitive engineering support for this phase will include the development, testing, and evaluation/validation of a human operator model [the Integrated Reactor Operator/System (INTEROPS)]. 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.

The INTEROPS model is being developed in a framework combining the capabilities of network simulation and knowledge-based simulation. This framework has been successfully employed to develop a prototype version of INTEROPS, and is currently being employed to develop the full-scale version of the model. INTEROPS prototype development was completed during FY-1987, and successful completion demonstrated 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 evaluation/validation of a full-scale, single operator/single LMR module version of the INTEROPS model.

Testing and Evaluation Phase. Once a final design alternative has been selected, detailed characteristics of its operation need to be assessed. The program will provide the capability for real-time, full-scoped, full-plant simulation of the final design concept. During this 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. Interface design will be supported through the development of requirements which emphasize: a) transparency, b) model-based integration, c) hierarchial integration and data abstraction, d) usefulness and reduction of redundancy, and e) supportiveness of the operator's mental model of system structure and function.

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 "fully-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.

Surveys and investigations of computer hardware and software capabilities for satisfying the full-plant simulator requirements have been initiated, and will continue through the periods in which the hardware and software are acquired. Discussions are being held with vendors of the various types of computer hardware and software systems (e.g. workstations, parallel processors, etc.) regarding current and projected future capabilities. The potential benefits of various architectures (local and shared memory for the parallel processors), processor types (vector and scaler), operating systems, programming languages, and other features are being considered. Special attention will be given to evaluating the applicability of current and projected availability of expert system tools, object-oriented programming systems, CASE tools, database management systems, and graphics capabilities to the program requirements. Because of the rapid development of both hardware and software technologies, the capabilities for upgrading systems and transporting (and reusing) software are major concerns in order to ensure high quality output and certifiable controller designs. At this time, several computer based workstations and a parallel processor have been acquired, installed and used for development and testing of designs generated within the program.

Methods are being developed to ensure that the Advanced Controls Program software development conforms with industry standards (ANSI, IEEE, NRC Regulatory Guides, etc.).

Simulator validation and verification work will be a continuing effort, and again will depend on the availability of pertinent data and corroborating runs from independent codes. We expect to be able to use EBR-II and FFTF data in support of the LMR simulations, as well as comparisons with simulations by codes used by other LMR researchers. In the long term, we plan to initiate cooperative tasks for model verification and testing with the French, German, and Japanese LMR programs.

Additional testing demonstrations will be accomplished with the proposed EBR-II automated startup activities. The possibilities for tying in prototype controller designs to operator training simulators have also been investigated for two specific LWR simulators which are available, part time, for R&D activities.

Control Software and Hardware R&D

The 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.

Software for Advanced Controls will reflect a new set of demanding expectations. Utilization of modern database management tools and techniques ensures that procedural code is insulated from changes in the underlying data structures; modern database management (DBMS) systems are making significant strides towards offering "truly distributed" data. Because of the critical nature of the operator interfaces, graphics and icon-based programming will be important ingredients. As already seen this year, object-oriented programming systems (OOPS) offer many advantages over traditional procedural language environments; as object-oriented database systems mature, these could replace the (SQL-based) relational database systems currently available. ORNL will evaluate technological improvements currently under development.

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 controlling 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 ACTO prototypical control systems and for control systems designed by others.

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.

SUMMARY

Control system designs for nuclear power plants are evolving from analog, inflexible single input single output concepts toward completely automated digital multivariate optimal concepts. This evolution is occurring because of a number of reasons including the need to improve plant availability and operability and also the technological advances in low-cost digital hardware and software. Advanced reactor concepts rely upon the integration of these advances in control system technologies to accomplish their goals. The Advanced Controls Program at ORNL is funded by DOE to determine how this technological evolution will occur and which of the advances are appropriate for the proposed ALMR. This program is organized to provide: 1) demonstrations of advanced control system concepts that will enable the ALMR to achieve its goals; 2) an advanced user-friendly environment including rapid simulation capabilities, plant models, human-machine interface models , and advanced control strategies; 3) testing and validation of advanced strategies; and 4) guidelines and standards for control hardware and software.

REFERENCES

1. A. D. Alley et al, "Advanced Control Test Operation-Task Team Report", GEFR-00771, September, 1985.
2. L. C. Oakes, J. E. Jones, "Proposed New Initiatives in Advanced Reactor Technology", Oak Ridge National Laboratory, March 15, 1985.
3. Federal Register, Thursday, August 21, 1986, Vol. 51, #162, Rules and Regulations, Amendment to 10 CFR Part 50.
4. M. Divakaruni et al, "BWR Feedwater Control System Replacement in Monticello Plant", Proceedings: EPRI NP-4769-SR, September, 1986.
5. N. P. Mueller and F. M. Siler, "PWR Feedwater System Failure Data as a Basis for Design Improvements", Proceedings: EPRI NP-4769-SR, September, 1986.
6. K. A. Gaydos et al, "An Optimal Control Strategy in the Design of a PWR Feedwater Controller", Proceedings: EPRI NP-4769-SR, September, 1986.
7. K. F. Graham and S. M. Divakaruni, "EPRI Digital Feedwater Control Project: System Verification Plans in an Operating Plant", Proceedings: EPRI NP-4769-SR, September, 1986.
8. "Generating Availability Reports, 1982-1986", North American Electric Reliability Council, Princeton, N.J.
9. D. Chan et al, "Large-Scale Implementation of Computerized Plant Control and Monitoring in CANDU Power Plants," Proceedings: EPRI NP-4769-SR, September, 1986.
10. A. D. Alley and W. R. Daniel, "A Systematic Approach to the Design of a Nuclear Power Plant Hierarchical Distributed Digital Control and Protection System", Proceedings: EPRI NP-4769-SR, September, 1986.
11. W. R. Whittall and G. A. Hepburn, AECL, "Canadian Nuclear Power Plant Computer Control and the Application of Microprocessors", Proceedings: 1985 Seminar on Power Plant Digital Control and Fault-Tolerant Microcomputers, EPRI NP-4769-SR, September, 1986.
12. R. M. Lepp, L. M. Watkins, "Control and Instrumentation Systems for the 600 MW(e) CANDU Nuclear Power Plants", AECL-7519, February, 1982.
13. F. J. Kee, J. E. Smith, "Development of a Reliable Single-Channel Direct-Digital Reactor Control System", IAEA-SM-226/103, April, 1978.

14. S. Kawakami et al, "Operating Experience in Using Computerized Plant Automatic Start-up Control System", Proceedings: 1985 Seminar on Power Plant Digital Control and Fault-Tolerant Microcomputers, EPRI NP-4769-SR, September, 1986.
15. S. Taguchi et al, "Application of Digital Control in Japanese PWR Plants", Proceedings: 1985 Seminar on Power Plant Digital Control and Fault-Tolerant Microcomputers, EPRI NP-4769-SR, September, 1986.
16. H. E. Price et al, "The Allocation of Functions in Man-Machine Systems: A Perspective and Literature Review", NUREG/CR-2623, June, 1982.
17. R. Pulliman et al, "A Methodology for Allocating Nuclear Power Plant Control Functions to Human or Automatic Control", NUREG/CR-3331, August, 1983.
18. Personal communication: A. D. Alley, General Electric, San Jose, CA to R. A. Kisner, Oak Ridge National Laboratory, January 12, 1988.
19. C. McClure, "Software Automation," Business Software, September, 1987.
20. T. L. Wilson, "Balance of Plant Control for the PRISM", these proceedings.
21. P. J. Otaduy, C. R. Brittain, and L. A. Rovere, "Supervisory, Hierarchical Control for a Multimodular ALMR", these proceedings.
22. J. T. Robinson, "An Intelligent Simulation Environment for Control System Design", these proceedings.
23. R. A. Kisner, B. R. Upadhyaya, and R. C. Berkan, "Performance Characteristics for Advanced Control Systems", these proceedings.
24. H. E. Knee and J. C. Schryver, "Human Role Definition and Human-machine Interface", these proceedings.